CBAI SECURED SOLUTIONS FOR COMMUNITY BANKS
WEB SITE HOSTING SERVICES
Business Resumption Contingency Plan
Table of Contents

SECTION I – OVERVIEW ......................................................................................................................... 1
Definition .................................................................................................................................................. 1
Goals of the Plan ........................................................................................................................................ 1
Scope of the Plan ........................................................................................................................................ 2
Overall Policies/Procedures ...................................................................................................................... 2

SECTION II - ORGANIZATIONAL PLANNING ....................................................................................... 3
Project Workgroup ................................................................................................................................. 3
Timeline for Development and Implementation ....................................................................................... 4
Risk Management Process and Reporting .............................................................................................. 4
Integration of Existing Business Contingency Plans ............................................................................... 5
The Recovery Process ............................................................................................................................. 5
Levels of Disasters .................................................................................................................................... 6
Alternative Site Backup Processing ......................................................................................................... 6
Distribution of the Plan ............................................................................................................................ 6
Maintenance of the Plan ............................................................................................................................ 7
Testing of the Plan ...................................................................................................................................... 7

SECTION III – BUSINESS RESUMPTION SCENARIOS ......................................................................... 8
Company Wide Scenarios: Web Site Hosting Service Fails ................................................................. 8
Company Wide Scenarios: Building is destroyed or damaged ............................................................ 10
Company Wide Scenarios: Utility Company Fails to Deliver Electricity ........................................... 11

SECTION IV – KEY NAMES AND NUMBERS ....................................................................................... 12

Section V – NETWORK MAPS ............................................................................................................... 13
CBAI Mail Flow. ........................................................................................................................................ 13
Network Diagram. ................................................................................................................................. 14
CBAI Virtual Servers ............................................................................................................................. 15
CBAI Virtual Server Roles ...................................................................................................................... 16
CBAI Chicago Traffic Flow and Lightower Fiber Networks’a .............................................................. 17

Addendum A – Redundancy Plan Process and Procedures ................................................................. 18
(This page left blank intentionally)
SECTION I – OVERVIEW

Management of Community Bankers Association of Illinois (CBAI), with the support of its Board of Directors, fully intends for all mission critical systems to remain at 99.9% functionality. We recognize that events could occur that are beyond management’s control, which could affect system functionality. The contingency plan is designed to minimize the overall effects of any systems which become non-operational. The project work group (defined later in this document) intends to continually update this document as new information is brought to management’s attention.

Definition

This plan is designed to allow for continuous processing of the CBAI Web Site Services with minimal disruptions to our bank’s web sites. The plan will provide a mechanism to educate our employees on the potential effects of system failure and also provide them with appropriate guidance and tools to implement re-establishment in the event a system failure occurs.

Per the Federal Financial Institutions Examination Council (FFIEC), the definition of a Business Resumption Contingency Plan (BRCP) is as follows:

“Contingency planning is the process of identifying critical information systems and business functions and developing plans to enable those systems and functions to be resumed in the event of a disruption. The process includes testing of the recovery plans to ensure they are effective.”

Goals of the Plan

“The goal of an effective Contingency Plan and recovery process is to facilitate and expedite the resumption of business after a disruption of vital information systems and operations. The principal objectives are to:

- Ensure timely resumption of operations.
- Minimize disruptions of service to member institutions’ web sites and their customers.
- Limit losses to financial institutions’ web site content. (DOES NOT INCLUDE INTERNET BANKING CONTENT...THIS WOULD BE THE RESPONSIBILITY OF THE BANK’S INTERNET BANKING PROVIDER.)

CBAI will accomplish these objectives by implementing the following:

- Overall responsibility of the contingency plan is assigned to Operations Management.
- Operations Management will be assigned specific areas to monitor.
- The plan will be reviewed at least annually and be revised as significant or major changes are implemented.
Community Bankers Association of Illinois
Web Site Business Resumption Contingency Plan

Scope of the Plan

The focus of this plan is also to provide continuous processing in the event of a system failure or other disaster.

Definition: For purposes of this plan, a “failure” is defined as a system or service being incapacitated to such an extent that it is effectively rendered non-operational for an extended period of time.

Overall Policies/Procedures

All CBAI employees must recognize that they serve the community banking profession that is important to our society. If computer problems exist or services are impaired, member inquiries and requests will be significant during the period of recovery. Therefore, no employees will be permitted to take vacation during a recovery time period. The President of CBAI must approve any exceptions to this policy.

CBAI has security procedures in place which protect CBAI headquarters and hardware/software items necessary to conduct web site business. Even in the event of a power failure, for example, these security procedures are always in effect. These procedures provide a safe environment for CBAI staff to ensure prompt resumption of web site business in the event of a system failure.
SECTION II - ORGANIZATIONAL PLANNING

CBAI Operations Management is directly involved in the BRCP planning process and has the responsibility of overseeing the process to the Project Workgroup identified in paragraph A that follows. The Project Workgroup identifies the persons who are responsible for the areas identified below and will periodically update the CBAI Board, Technology Committee, and hosted financial institutions on the status of the contingency plan. The plan developed by Operations Management is subject to the Board of Directors approval and will be presented to the Board after each significant proposed update. The Board will also be informed on the results of testing the contingency plan. Ultimately, the Board of Directors and Operations Management are responsible for the overall process and are committed to make sufficient resources available to ensure the success of the business resumption contingency plan.

Project Workgroup

The project workgroup is responsible for developing and monitoring the business resumption contingency plan. CBAI Operations Management will also request others to participate on an “as needed” basis. The Workgroup consists of the following components:

<table>
<thead>
<tr>
<th>Members</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CBAI</strong></td>
<td></td>
</tr>
<tr>
<td>1) Jenny Dial, CBAI Senior Vice President of Operations</td>
<td>Project Leader</td>
</tr>
<tr>
<td>2) Mike Kelley, CBSC President</td>
<td>Public Relations</td>
</tr>
<tr>
<td>3) Bob Wingert, CBAI President</td>
<td>Servers</td>
</tr>
<tr>
<td></td>
<td>Client Servers</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Troy Rodriguez, DBS Services President/Sr. Tech</td>
<td>Servers</td>
</tr>
<tr>
<td>2) Jason Keck, DBS VP of Hosting Operations/Sr. Tech</td>
<td>Client Servers</td>
</tr>
<tr>
<td>3) Jim Rodriguez, DBS Services COO</td>
<td></td>
</tr>
</tbody>
</table>


**Timeline for Development and Implementation**

The BRCP will be reviewed and revised periodically. The BRCP will be presented to the Board of Directors at least annually for reaffirmation.

**Risk Management Process and Reporting**

Each core business process will have its own minimum acceptable level of service. However, SQL, and Web Hosting software must function at 99.9% to meet customer needs as well as those of CBAI.

Some mission critical systems are “more critical” than others and demand a more rapid response in case of failure. The on-line services are most critical and will require a contingency plan that can be implemented within hours rather than days or weeks.

This section of the BRCP focuses on assessing the potential impact of the mission-critical system failures on the core web site business processes. CBAI has assessed which processes are critical in day-to-day web site operations. The results of this analysis provided the basis for the BRCP.

Efforts will be focused on the core web site hosting business processes that, should they be compromised, create the greatest risk to the institutions. The core web site business processes will continually be re-evaluated to determine priority and importance of each identified item. Operations Management will review the core processes periodically. Any changes in the plan will be approved at the operations management level and then submitted to the Technology Committee for action. The status and progress of the contingency plan will be included in the periodic report to the Board of Directors.

The BRCP for each core business process will include one or more of the following methods of repair.

- Quick fix – Desktop, servers, etc., that fail can quickly be replaced with new equipment from DBS Services or local vendors.
- Failover – (Offsite ‘hot-spare’ services) Servers will be required to failover in the event of a single server failure. If a physical server fails to respond for 1 hour, Secondary servers will assume the role of the source servers. (*Refer to Addendum A Redundancy Plan Process and Procedures.*)

CBAI has inventoried web site business processes and designated each process as core vs. non-core. The processes were assigned to the lists taking into consideration the following:

- Business Risk priorities
- Regulatory Impact
Integration of Existing Business Contingency Plans

CBAI utilizes DBS Services (DBS) Disaster/Collocation Facilities for multiple production services.

- CBAI provides clustered name server resolution for all domains hosted with CBAI at DBS Disaster/Collocation Facilities. In the event the clustered name servers on the Primary DBS Servers fail, DNS resolution will seamlessly failover to Secondary DBS Servers.
- DBS provides offsite hosting of 8 production web servers (Windows and Linux) for CBAI. These servers keep real-time synchronization of the critical services hosted (Web, DNS, Email, SQL) with DBS’s Backup Servers located at DBS’s Disaster/Collocation Facility.

The Recovery Process

In the event of a failure, the recovery process will be initiated as follows:

- DBS Operations Management team will perform an initial assessment of the disruption.
- DBS Operations Management will be assigned to project workgroups. Group leaders are defined in the “Project Workgroup” section of this document.
- Each project work group will be responsible for a category as defined below:
- Vendor liaison. The team will be responsible for communicating with the responsible vendor to determine the recovery time and the steps necessary to return to on-line status. Decisions relating to costs and time required to return to on-line status will be communicated to other members of the management team.

The following personnel are also authorized to initiate the BRCP:

Troy Rodriguez, DBS CIO
Jason Keck, DBS VP of Hosting Operations
Jenny Dial, CBAI Senior Vice President of Operations
Melissa Roberts, CBAI Operations Administrative Assistant

The personnel implementing the plan will work with the Project Workgroup. The personnel will also notify any additional personnel needed to assist in:

- Notifying CBAI employees/customers that the Contingency Plan is in effect
- Assisting members of the Project Workgroup to notify respective key employees
Levels of Disasters

The main effort in any disaster or incident is to keep our banks’ web sites and email in operation. These procedures should be considered:

1. Emergency situations are categorized as:
   a. Natural Disaster – flood, earthquake, tornado, storm
   b. Utility Emergency – gas leak, water main break, phone outage, power outage
   c. Medical Emergency – heart attack, stroke, poisoning, accident
   d. Violent Crimes – company robbery, bomb threat, extortion, employee violence, assault
   e. Special Emergencies – fire, civil unrest, national crisis, war, terrorist attack

2. Levels of disasters are categorized as:
   a. Hardware failure – one component or small components of the CBAI’s Collocated systems are in need of necessary maintenance, repairs, and/or malfunctioning.
      Expected downtime: none (all components are redundant) or less than 30 minutes
   b. Software failure – One or more of CBAI’s Collocated production services are down; for example, IIS, Apache, ColdFusion, and etc. software.
      Expected downtime: less than 30 minutes
   c. Network failure – X software/hardware are down and CBAI Collocated production services are not available. Contingency plans will be implemented.
      Expected downtime: less than 1 hour

Alternative Site Backup Processing

CBAI has entered into an agreement with DBS Services, of Chatham, IL, to provide production equipment/facility/hosting. The agreement provides that, depending on the severity of the failure; DBS Services will either:

- Troubleshoot and repair the hardware/software problem at the Disaster/Collocation Facility, or
- Restore an image of all systems to an Alternative Collocation Facility

Expected time frame: 4 – 8 hours

Distribution of the Plan

Copies of the plan will be distributed as follows:

1. One copy to each Technology Committee member.
2. A copy maintained with each Project Workgroup member, both CBAI, and DBS Services. Each copy will be maintained in a location that is accessible to authorized employees. The location will not be locked to ensure access at all times.
3. A copy will also be kept at the homes of each member of the Project Workgroup.
Community Bankers Association of Illinois
Web Site Business Resumption Contingency Plan

As the contingency plan is revised, updates or new copies will be provided to the distribution list.

**Maintenance of the Plan**

The BRCP will be updated periodically. Any significant revisions will be forwarded to the Technology Committee for its approval. Consideration will also be given to issues and suggestions raised by regulatory authorities. This plan will be approved at a minimum on an annual basis.

**Testing of the Plan**

The BRCP is tested on a quarterly basis. Test results will be documented and logged. The Operations Management will review the test results, summarize and present them to the Board of Directors. Certain components of the plan may be tested more frequently, such as the backups for the network (tested weekly). The testing plan includes the following by significant system:

**Power Supply** – The primary web servers at DBS’s Disaster/Collocation Facility is equipped with two power feeds from the local power company on separate grids. If both power company feeds fail, an Uninterrupted Power Supply (UPS) will keep the system powered until generators resumes power distribution.

**Web Site Services/Hardware** – Where practical all hardware/software is duplicated (redundant). Hardware is also covered by manufacturer’s warranty and maintenance contracts, where applicable. In addition, DBS Disaster/Collocation Facility practices a daily software backup routine that is kept for one day, one week and one month for all servers.

Hardware/software sufficient to provide Web Services is kept on standby at DBS and will go into production in the event of a catastrophic hardware/software failure at the Disaster/Collocation Facility.
SECTION III – BUSINESS RESUMPTION SCENARIOS

Contingency Plan and Implementation

Company Wide Scenarios: Web Site Hosting Service Fails

(Note: Scenario considers the telecommunication links, hardware, file servers, software, etc.)

Trigger Date: Immediately

Responsible Party: DBS Services, CBAI Senior Vice President of Operations

Methodology: The CBAI Web Hosting System is accessed through redundant Firewalls located at the DBS Collocation Facility. This plan and methodology will be implemented only if the CBAI Web Hosting System and associated redundant systems fail at DBS’s Collocation Facility.

In the unlikely event the CBAI Web Hosting System fails at DBS’s Collocation Facility, DBS will perform a series of diagnostic checks in order to establish the nature of the failure and attempt to immediately bring redundant systems online. DBS will then inform the CBAI Senior Vice President of Operations of the critical nature of the failure.

If it is determined the Primary system cannot be brought back online within its relative time frame, DBS Services and CBAI will fail-over the CBAI Web Hosting System to the Redundant Systems in place.

After the Redundant System is in production DBS personnel, in conjunction with any necessary vendors, will continue to troubleshoot and repair any problems with the Primary System.

When the Primary Facility is repaired and tested DBS and CBAI will schedule a time after hours to fail-back CBAI’s Web Hosting System to DBS’s Primary Collocation Facility.

Implementation of the contingency plan is immediate. (Refer to Addendum A – Redundancy Plan Process and Procedures.)

DBS Collocation Facility – uses redundant Cisco routers, redundant Barracuda Spam Firewall Vx and SonicWALL™ Network Security Appliance 2600 Next-Generation Firewall(s) and multiple bandwidth feeds from various backbone providers. Additionally, this Collocation Facility is equipped with multiple power feeds, battery backups and onsite generators to insure 99.9% uptime.

Data in the Collocation Facility is also protected against individual disk failure by an EqualLogic SAN Array using a proprietary RAID and daily system snapshots. In addition regular backups are performed daily, weekly and monthly.
Hardware – Servers and/or other redundant hardware are protected by manufacturer’s warranties and can be easily replaced. If a critical hardware fails, backup hardware will be used until hardware can be provided.

Software – DBS Services maintains all software necessary to provide CBAI’s Web Hosting Services, including but not limited to, periodic security updates and security configurations. DBS also provide current and active Antivirus/Spyware protection.

CBAI and DBS Services use a third party vendor to conduct quarterly (or as deemed necessary) intrusion, penetration, and vulnerability testing on CBAI’s web servers. CBAI and DBS also monitor CBAI’s public and private networks. In the event of a disaster, CBAI maintains a relationship with a network support company for software replacement.

Other Network Components – Hubs, wiring and routers are easily replaced. DBS maintains spare parts in the event replacement is needed.

Validation/Training: Backups are tested weekly.
Community Bankers Association of Illinois
Web Site Business Resumption Contingency Plan

Company Wide Scenarios: Building is destroyed or damaged

(NOTE: The goal here is to document what CBAI will do to function during the recovery time.)

Trigger Date: Immediate

Responsible Party: DBS Services / CBAI Senior Vice President of Operations

Methodology: This scenario addresses how CBAI will operate in the event one of the facilities incurs damage, whether due to natural disaster, terrorism, or other damage.

The Project management team will meet immediately to discuss the impact of the damage and determine if the facility can remain open.

DBS Collocation Facility – If the Collocation Facility is destroyed or damaged DBS Services will initiate a full system restore onto similar/dissimilar hardware virtualized in a standby facility.

If the Primary Facility cannot be repaired in a reasonable time frame DBS Services will locate a new Primary Facility and rebuild the system as quickly as possible.

(See Section II – Organizational Planning G. Alternative Site Backup Processing.)

Validation/Testing: Emergency procedures will be reviewed quarterly.
Community Bankers Association of Illinois
Web Site Business Resumption Contingency Plan

**Company Wide Scenarios: Utility Company Fails to Deliver Electricity**

**Trigger Date:** Immediate

**Responsible Party:** DBS Services / CBAI Senior Vice President of Operations

**Methodology:** DBS will notify CBAI Senior Vice President of Operations of power outage if all grids are down to run the web server and significant systems during the power outage; The DBS Collocation Facility is equipped with two major power grids in the downtown Chicago loop area, with uninterrupted power supply and generators.

In addition, if there is a power failure and both power grid connections are down, the battery systems are depleted and the generator has failed, the Project Workgroup personnel will initiate the BRCP. *(Also see Section II – Organizational Planning G. Alternative Site Backup Processing.)* This resource would be used predominately to run the web servers and other significant systems during the power outage.

**Validation/Testing:** Emergency procedures will be reviewed semi-annually.
SECTION IV – KEY NAMES AND NUMBERS

CBAI Staff

Jenny Dial, CBAI Senior Vice President of Operations
Community Bankers Association of Illinois 901 Community Drive
Springfield, IL 62703
217.529.2265
217.553.7590 (24 hours)
217.697.8590 (24 hours )
www.cbaisupport.com
jennyd@cbai.com

DBS Services Contacts

Troy Rodriguez, DBS President and Senior Engineer
DBS Services
314 N Main Plaza
Chatham, IL 62629
217.697.8590 (24 hours)
troy@dbhosting.com

Jason Keck, DBS VP of Hosting Operations
DBS Services
314 N Main Plaza
Chatham, IL 62629
217.697.8590 (24 hours)
jason@dbhosting.com

Jim Rodriguez, DBS COO
DBS Services
314 N Main Plaza
Chatham, IL 62629
217.697.8590 (24 hours)
jim@dbhosting.com

CBAI Web Site Business Resumption Contingency Plan - (BRCP 12012005)

Revised 12/15/2005
Revised 12/21/2006
Revised 03/02/2007
Revised 06/15/2007
Revised 06/20/2008
Revised 10/31/2008
Revised 05/25/2011
Revised 04/26/2013
Revised 01/01/2014
Revised 06/01/2015
Revised 06/01/2016
Revised 09/09/2016
All VPS Servers are distributed across the vSphere Host cluster and on the SAN array. All VPS hosts are snapshotted on a 4 hour time frame and backed up on a daily, weekly, monthly schedule. Bandwidth and power are on redundant grids in the Chicago Loop.
## CBAI VPS Server Roles

### CBAI VPS Servers

<table>
<thead>
<tr>
<th>Server</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1.cbai.com</td>
<td></td>
</tr>
<tr>
<td>S2.cbai.com</td>
<td></td>
</tr>
<tr>
<td>W1.cbai.com</td>
<td></td>
</tr>
<tr>
<td>DNS1.cbai.com</td>
<td></td>
</tr>
<tr>
<td>DNS2.cbai.com</td>
<td></td>
</tr>
<tr>
<td>DNS3.cbai.com</td>
<td></td>
</tr>
</tbody>
</table>

The S1 & S2 servers are Hardened cPanel VPS servers that are setup for Standard Web Hosting as provided by CBAI. This is to distribute the load of all websites using different versions of software on a single server. This has encapsulation so no single host can affect other hosts on the same server.

The W1 server is a Windows VPS server that is specifically tailored for running Windows designed websites. This server has been hardened for the Windows platform and is used to host Windows websites.

The DNS1, DNS2 & DNS3 servers will be the Primary DNS servers for all domains hosted with CBAI. When a new domain is added to CBAI’s hosting platform DNS entries will be added to these servers automatically from the cPanel hosting servers. During normal DNS operation this server will answer ALL DNS requests to CBAI hosted domains for resolution.

---

Vmware vSphere Cluster
Lightower Fiber Networks’ ("Lightower")

Lightower, best-in-class fiber operator delivering high-performance networks for the most demanding applications.

Lightower specializes in delivering high-performance, low-latency networks to serve the mission-critical applications of our large enterprise, carrier, and data center customers with a focus on how customers connect to cloud services and access or distribute content. Our Xtreme Ultra-Low Latency Network connects all of the major financial exchanges and data centers together to serve the needs of the financial services market and any other verticals with applications that demand high-performance. As proof, Lightower carries trillions of dollars of trades per day, more than any other provider. The company also focuses on diversely connecting to every data center within its footprint to provide customers with access to cloud services, backup and recovery, content distribution, and carrier interconnection.
Addendum A – Redundancy Plan Process and Procedures

For redundancy to work correctly DNS1.CBAI.COM, DNS2.CBAI.COM, and DNS3.CBAI.COM must be set as the DNS servers for the site(s) at the registrar level. In the case of a facility disaster all servers will be reimaged from the DBS Facility to an Alternate Facility and return to normal operation. By using CBAI DNS Servers the customer will eliminate the need for bank IT staffs to become involved during the process.

Redundancy of the Web Hosting servers is facilitated by DBS Services using custom scripts and VMware failover software for virtualized hosting environments.

Servers at the DBS Secondary Facility are set in a manual startup mode and are configured to come online and be placed in production only in the event a failover condition exists. This process must be initiated by DBS Technical Staff.

Cybersecurity Threats Mitigation Protection and Control

CBAI and DBS SonicWALL firewalls provide a comprehensive layer of defence against today’s Cybersecurity threats by combining gateway content filtering, anti-spam, anti-virus, anti-spyware, intrusion prevention (such as DDoS), and regain visibility into the network through application intelligence and visualization. Essential to an intelligent and highly adaptive security system, Dell SonicWALL Next-Generation Firewalls scan every byte of every packet for the deepest level of network protection and, unlike competitive offerings, massively scale to extend state-of-the-art security to growing and distributed enterprise networks.

Lightower Fiber Network monitors bandwidth utilization reports on all backbone links and ISP connections. If a security threat is suspected by either a link going above a set threshold, a customer report, an alarm, etc then Lightower looks at Netflow data to determine the destination of the attack. Once identified, then a null route is placed on the ISP routers connecting to Lightower’s transit providers. This step usually mitigates most issues. After the null route is in place Lightower contacts the upstream providers requesting they block traffic in question, which occurs at the ingress to their network. This will mitigate any bandwidth overloads on the ISP transit connections.