CU*ANSWERS
A Credit Union Service Organization

6000 28TH STREET S.E. • GRAND RAPIDS, MI 49546
phone: 616.285.5711 • 800.327.3478 • fax: 616.285.5735
visit us on the web: www.cuanswers.com

SECURIKEY

CBX

Including Risk/Threat Assessment

VERSION 1.2 October, 2025

Contents

SecuriKey

CBX

LEGAL DISCLAIMER

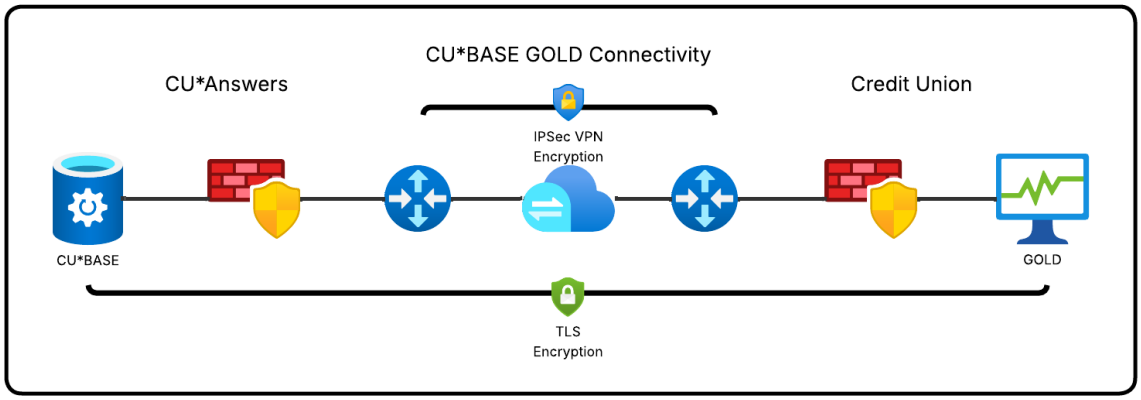
The information contained in this Assessment does not constitute legal advice. We make no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this Assessment. You should retain and rely on your own legal counsel, and nothing herein should be considered a substitute for the advice of competent legal counsel. These materials are intended, but not promised or guaranteed to be current, complete, or up-to-date and should in no way be taken as an indication of future results. All information is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will CU*Answers, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information provided or for any consequential, special or similar damages, even if advised of the possibility of such damages.

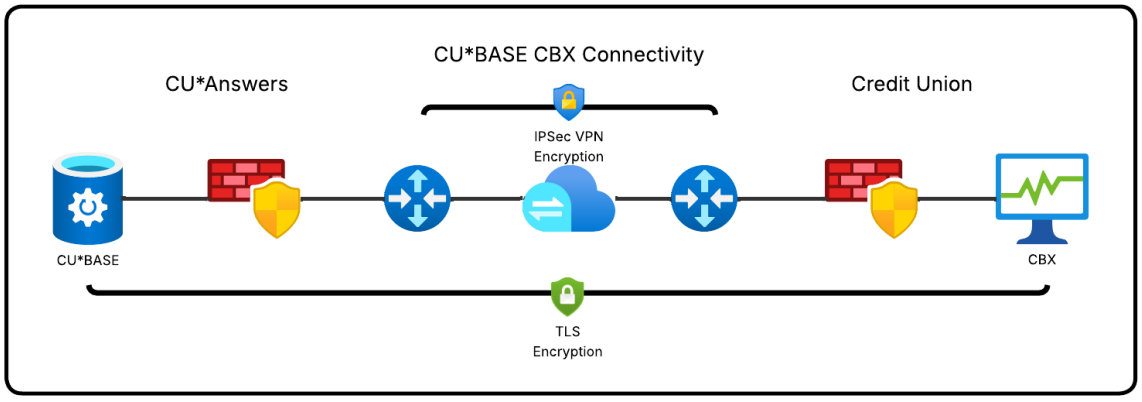
Quick Reference Guide: CBX Design and Controls

Simply put, CBX is a browser-based version of CU*BASE. The purpose of CBX is to improve the readability and usability of the application, keeping the infrastructure the same while providing a sleek User Interface presented right in your browser window. CBX is presented via a browser that instead of using multiple pages, uses a single page that is updated by the server when a user interacts with it.

CBX is not a Web-Based or Internet Application

CBX is not available on the internet. CBX is a private network application delivered via an encrypted browser connection via the same network infrastructure as CU*BASE GOLD. This is an important distinction for your compliance team, auditors, and examiners. CBX is not a publicly available or distributed application, and therefore does not require security measures such as Web Application Firewalls. Browser-based applications are very common in the financial tech services world, and our software remains as secure as CU*BASE GOLD was previously.





Dedicated Network with Highly Available Replication

The same hardware and network infrastructure is used to deliver CBX securely to your credit union or organization. Whitelisted VPN connections from credit union sites connect to the primary data center, itself protected through firewalls, intrusion detection, and a third-party SEIM system. In turn, a redundant

fiber core network connects the primary data center with the High Availability data center. This network provides the backbone for real-time data replication. In the event of a data communications disruption at either the primary or High Availability data centers, access to/from client credit union networks is backhauled through the surviving site.

Application Security

The same application security for CU*BASE GOLD applies to CBX, and is set by the individual organization using the software. Please refer to the reference materials on cuanswers.com for more information on how to configure CBX securely for your users.

Risks Threat Assessment Specific to CBX

This Assessment is designed to assist clients of CBX in assessing the risk of using the software. The Assessment can be used by clients to develop their own Assessments and assist in explaining to their stakeholders the risks and controls associated with CBX, and developing their own compensating controls where feasible to assist with minimizing risk.

The following risk or threat types were considered in the development of this assessment. The types listed are solely for CBX-related threats and does not include controls related to credit union use or items otherwise related to CU*Answers' operations.

Physical (Datacenter)

Flooding	Includes as the result of natural flooding (heavy rains) and human-created (damage to water infrastructure).
Natural and Elemental	Includes severe winds/tornado, lightning strikes, severe winter, and severe heat.
Fire	Can include large fires (e.g., those that trigger the fire suppression system, if the site is so equipped, or require the involvement of trained firefighters) and small fires (e.g., those extinguishable with a hand-held extinguisher).
Transportation	Includes airport, train, truck or other systems used to transport hazardous materials.

Internet and Utility

Internet/Data Outages	Loss or disruption of data communication capabilities.
Voice Communication	Loss or disruption of voice communication capabilities.
Power Outages	Long-term power failure associated with power outages.
Water/Sewer Outages	Disruption to the function of water and/or sewer.

Equipment

Server/Hosting Equipment Failure	Sudden or chronic failures with an IT system used to host CBX.
HVAC Failure	Failure of environmental controls, causing increased temperature and humidity, which can damage sensitive computer equipment and storage media.
Network Equipment Failure	Sudden or chronic failures with an IT system used to transmit CBX.

Cybersecurity

Network Compromise	Disruption of a computer network and its connected systems, resulting in the loss of confidentiality, integrity, or availability of sensitive data and resources.
Device Compromise	Disruption of a device and its connected systems, resulting in the loss of confidentiality, integrity, or availability of sensitive data and resources.
Malware	Viruses, worms, trojans, and other software used to disrupt networks and devices.
System Vulnerabilities	Exploitable code that can be used to disrupt networks and devices.
Social Engineering	External adversarial actions intended to persuading individuals within organizations into revealing critical/sensitive information.
Denial of Service (DoS)	Internet services are targeted to deny access to systems and resources.

Unauthorized Access	Access is gained to data a party is not authorized to receive, or where access granted exceeds authority.
Supply Chain	Supply chain services are disrupted, resulting in the loss of confidentiality, integrity, or availability of sensitive data and resources.

Software Development/Enhancement

Security Vulnerabilities	Vulnerabilities are introduced into CBX.
Data Integrity	Errors generated as a result of the CBX coding.

Using the Assessment

This Assessment is used to determine the likely probability of a risk/threat to CBX, as well as the severity of that risk/threat. The Assessment regards probability in five grades: Very Low, Low, Medium, High, and Very High. Severity is graded, using the same ranking. RTOs (Real Time Objectives) are the maximum acceptable time that a business process or system can be unavailable before significant consequences occur. Point values are assigned to each level of probability and severity. A heat map value has also been created to reflect the weight of the respective total probability and severity. A five-point qualitative range of controls effectiveness (Fully, Mostly, Moderately, Partially, Mildly) is included before a residual risk score is generated.

Probability and Severity

Impact probability is rated using this list of perceived probabilities:

Almost Certain (5)	86-100% chance
Occasional/Likely (4)	61-85% chance
Uncommon (3)	31-60% chance
Rare (2)	11-30% chance
Improbable (1)	1-10% chance

Threat Impact Severity is rated using this key:

Major (E)	Service outages likely to last more than 48 hours
Significant (D)	Service outages likely to last more than 24 hours
Moderate (C)	Affects RTOs in terms of service outages
Minor (B)	May stress RTOs
Insignificant (A)	RTOs not likely to be affected

Matrices/Methodology

Use this qualification matrix to help determine risk scoring.

Probability	**Severity**				
	Insignificant (A)	**Minor (B)**	**Moderate (C)**	**Significant (D)**	**Major (E)**
Almost Certain (5)	5A	5B	5C	5D	5E
Occasional/Likely (4)	4A	4B	4C	4D	4E
Uncommon (3)	3A	3B	3C	3D	3E
Rare (2)	2A	2B	2C	2D	2E
Improbable (1)	1A	1B	1C	1D	1E

This heat map matrix is used to quantify the probability and severity levels of each threat within the previous matrix.

Probability	Severity				
	Very Low (A)	Low (B)	Medium (C)	High (D)	Very High (E)
Very High (5)	Medium	High	Very High	Very High	Very High
High (4)	Low	Medium	High	High	High
Medium (3)	Very Low	Low	Medium	Medium	Medium
Low (2)	Very Low	Very Low	Low	Low	Low
Very Low (1)	Very Low	Very Low	Very Low	Very Low	Very Low

Sources

*Note: CU*BASE/CBX may be used interchangeably in source materials, unless otherwise described.*

Sources used to generate the Assessment matrix include the following:

- SSAE-18 SOC Reports
- External Testing
- Internal Testing
- Disaster Recovery/Business Resumption Testing
- Policies and Procedures

For security reasons, CU*Answers does not publish or make available its vulnerability or other highly sensitive testing. CU*Answers does make all of its SOC, ACH, and other due diligence materials available on its website at: https://www.cuanswers.com/about/due-diligence-materials/.

Up to date Disaster Recovery/Business Resumption materials can be found at CU*Answers website at the following link: https://www.cuanswers.com/solutions/business-continuity/auditing-and-testing/.

System uptime and downtime is published online at our website at the following link: https://www.cuanswers.com/resources/system-availability/.

Up to date CBX information and resources is available on our website at: https://www.cuanswers.com/products/core-software/cbx/.

Assessment with Controls

*Note: The following Assessment is specific to CBX and is not indicative or representative of all threats, risks, and controls related to CU*Answers and its operations.*

Physical (Datacenter)

Risk/Threat	Initial Threat/Risk Scoring			Controls/Mitigation Measures	Controls Effectiveness	Residual Risk Score
Flooding	Probability	3	Medium	Sump pump; moisture sensors; HA system	Moderately Effective	Low
	Severity	D				
Natural and Elemental	Probability	2	Low	Low risk environmental zone; large scale absence policy; HA system	Mostly Effective	Very Low
	Severity	D				
Fire	Probability	2	Low	Building equipped with extinguishers; two nearby bodies of water for FD to use; hydrant less than 50 feet from building; datacenter equipped with fire suppression system; HA system	Mostly Effective	Very Low
	Severity	E				
Transportation	Probability	2	Low	Large scale absence policy, HA system	Mostly Effective	Very Low
	Severity	D				

Internet and Utility

Risk/Threat	Initial Threat/Risk Scoring			Controls/Mitigation Measures	Controls Effectiveness	Residual Risk Score
Internet/Data Outages	Probability	3	Medium	Redundant network connections; HA system	Mostly Effective	Low
	Severity	D				
Voice Communication	Probability	2	Low	Redundant connectivity	Moderately Effective	Low
	Severity	D				
Power Outages	Probability	3	Medium	Backup generators; HA system	Moderately Effective	Low
	Severity	D				
Water/Sewer Outages	Probability	3	Medium	Sump pump, moisture sensors,	Moderately Effective	Low
	Severity	D				

Equipment

Risk/Threat	Initial Threat/Risk Scoring			Controls/Mitigation Measures	Controls Effectiveness	Residual Risk Score
Server/Hosting Equipment Failure	Probability	3	Medium	Redundant servers; warranties including hardware replacement on key systems; HA system	Mostly Effective	Low
	Severity	D				
HVAC Failure	Probability	3	Medium	Temporary HVAC systems available; HA system	Moderately Effective	Low
	Severity	D				
Network Equipment Failure	Probability	3	Medium	Redundant equipment; warranties including hardware replacement on key systems; HA system	Mostly Effective	Low
	Severity	D				

Cybersecurity

Risk/Threat	Initial Threat/Risk Scoring			Controls/Mitigation Measures	Controls Effectiveness	Residual Risk Score
Network Compromise	Probability	3	Medium	Dedicated network connections; VPN; Intrusion detection; firewall management; SEIM services; data encryption; vulnerability management	Mostly Effective	Low
	Severity	D				
Device Compromise	Probability	3	Medium	Data encryption; vulnerability management	Mostly Effective	Low
	Severity	D				
Malware	Probability	2	Low	Anti-malware system; vulnerability management; limited administrator access	Mostly Effective	Very Low
	Severity	D				
System Vulnerabilities	Probability	3	Medium	Vulnerability management; regular patching; notification of critical vulnerabilities	Mostly Effective	Low
	Severity	D				
Social Engineering	Probability	3	High	Employee training; limited admin access;	Moderately Effective	Medium
	Severity	D				
Denial of Service (DoS)	Probability	2	Medium	ISP controls; SEIM system; instruction prevention	Mostly Effective	Very Low
	Severity	D				
Unauthorized Access	Probability	3	Medium	Password protection; limited administrator access	Moderately Effective	Low
	Severity	D				
Supply Chain	Probability	1	Very Low	Vendor management; IP owned in-house; development in-house	Mostly Effective	Very Low
	Severity	D				

Software Development/Enhancement

Risk/Threat	Initial Threat/Risk Scoring			Controls/Mitigation Measures	Controls Effectiveness	Residual Risk Score
Security Vulnerabilities	Probability	2	Low	SDLC; QA Testing prior to production	Moderately Effective	Low
	Severity	D				
Data Integrity	Probability	2	Low	SDLC; QA Testing prior to production	Moderately Effective	Low
	Severity	D				

Other Security Considerations

If an auditor or examiner asks what steps your institution is doing to secure your CBX users, please refer them to the security settings in CBX. Your organization may also wish to consider additional compensating controls for security purposes. Such controls might include content and malicious website filtering for internet browsing, having the browser not save usernames and passwords, limiting the installation of browser plugins, and reviewing business configuration recommendations for the browser(s) used by your organization.

Document Version Control

Version	Update	Date
1.0	First Published	August 22, 2025
1.1	Added Introduction and Other Security Considerations	October 15, 2025
1.2	Added Diagram	October 27, 2025