CBV COLLECTION SERVICES LTD.

Your source for accounts receivable recovery since 1921

CBV Collection Services Ltd

Service Organization Control Report

(SOC 2® Type II)

Report on the Suitability of the design and operating effectiveness of Controls to meet the Trust Services Criteria for Security and Availability

For the period July 1, 2021, to June 30, 2022

Threat IQ

Committed to keep you secure. ALWAYS.

www.threatiq.io 1 (866) 837-0773

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations ™

Contents

Section I: Independent Service Auditor’s Report

To: Management of CBV

Scope

We have examined CBV Collection Services, LTD’s (“CBV”, or “the Company”) description of controls for its information technology and collections processing system, and related transactions throughout the period July 1, 2021, through June 30, 2022, based on the criteria for a description of a service organization’s system in DC Section 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report (AICPA, Description Criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 1, 2021, through June 30, 2022, to provide reasonable assurance that CBV’s service commitments and system requirements were achieved based on the trust service criteria for security and availability outlined in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at CBV, to achieve CBV’s service commitments and system requirements based on the applicable trust services criteria. The description presents CBV’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of CBV’s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization’s Responsibilities

CBV is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that CBV’s service commitments and system requirements were achieved. CBV has provided the accompanying assertion titled "Assertion of CBV Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. CBV is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion on the description and the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description
- Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in Section IV

Opinion

In our opinion, in all material respects, based on the description criteria identified in CBV's assertion and the applicable trust services criteria:

(a) The description fairly presents the system that was designed and implemented for the period July 1, 2021, to June 30, 2022.

(b) The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period and user entities applied the complementary user-entity controls contemplated in the design of CBV's controls throughout the period; and

(c) The controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the Security and Availability trust services criteria were met for the period July 1, 2021, to June 30, 2022.

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of CBV, user entities of CBV's Platform during some or all of the period July 1, 2021, to June 30, 2022, business partners of CBV, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, and other parties
- Internal control and its limitations
- Complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Sudheendran Cheenikkal
ThreatIQ - Chartered Professional Accountants
www.threatiq.io 1 (866) 837-0773

Section II: Management's Assertion

We have prepared the description of CBV's information technology and collections processing system ("system" or "the system") throughout the period July 1, 2021, through June 30, 2022, ("the description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization System in a SOC 2 Report* (AICPA, Description Criteria). The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with CBV Service Organization's system, particularly information about system controls that CBV has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability outlined in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA Trust Services Criteria).

We confirm, to the best of our knowledge and belief, that:

a. The description presents CBV's system that was designed and implemented throughout the period of July 1, 2021, to June 30, 2022, per the description criteria.

i. The description contains the following information:

(1) The types of services provided.

(2) The components of the system used to provide the services, which are the following:

- *Infrastructure* – The physical and hardware components of a system (facilities, equipment, and networks).
- *Software* – The programs and operating software of a system (systems, applications, and utilities).
- *People* – The personnel involved in the operation and use of a system (developers, operators, users, and managers).
- *Procedures* – The automated and manual procedures involved in the operation of a system.
- *Data* – The information used and supported by a system (transaction streams, files, databases, and tables).

(3) The boundaries or aspects of the system covered by the description.

(4) How the system captures and addresses significant events and conditions.

(5) The process used to prepare and deliver reports and other information to user entities and other parties.

(6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization and other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(7) For each category being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the Company's system.

(8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the Company, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria; and for privacy, the types of activities that the subservice organization would need to perform to comply with privacy commitments.

(9) Any applicable trust services criteria that are not addressed by a control at the Company or a subservice organization and the reasons, therefore.

(10) Other aspects of the Company's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(11) Relevant details of changes to the Company's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the Company's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each user may consider important to his or her own needs.

b. The controls stated in the description were suitably designed throughout the period July 1, 2021, through June 30, 2022, to provide reasonable assurance that CBV's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period.

c. The controls stated in the description operated effectively throughout the period July 1, 2021, through June 30, 2022, to provide reasonable assurance that CBV's service commitments and system requirements were achieved based on the applicable trust services criteria.

Isak Jon Benjaminsson
Director Information Technology
October 17, 2022

Isak Ben

Section III: DESCRIPTION OF CBV COLLECTION SERVICES, LTD'S INFORMATION TECHNOLOGY AND COLLECTIONS PROCESSING SYSTEM

Overview of Operations

CBV was originally founded in 1921 and has operated continuously since then. CBV operates four (4) contact centers in Canada in addition to operating back-office facilities in India and Chile. During that time CBV has grown to be one of the largest business process outsourcings (BPO) and contact center companies in Canada. CBV's current clients include all levels of government in Canada, leading banks and credit providers in Canada, public and private utilities, commercial companies, and others.

Products and Services Overview

CBV's core businesses are:

- 3rd party collection of accounts at all placement levels
- 1st party customer care, contact center, and business process outsourcing
- Debt purchasing

CBV established FrontLine Group as a separate division dedicated to Business Process Outsource Solutions catering to their growing BPO portfolio. Services include inbound and outbound customer care, level 1 technical support, sales, and back-office solutions.

Description of the Environment

Principal Services Provided

CBV's primary service is to provide accounts receivable management services. The Company contacts delinquent debtors and manages the end-to-end collections process for creditors. CBV leverages technology and almost one hundred (100) years of experience to ensure claims are processed accurately, securely, and confidentially.

Principal Service Commitments and System Requirements

CBV's principal service commitments and system requirements, as they relate to the system description and the applicable trust services categories of security and availability, are to provide collections services securely, with a focus on each client's performance, privacy, and reputational requirements.

Components of the System

The SOC 2 examination covers the CBV Collection Services Infrastructure Environment ("IT Environment" or "System") including operations, database administration, storage management, server administration, change management, system backup, and disaster recovery processes, as well as network operations, system monitoring tools and processes, system security (both logical and physical), and common support processes, applicable to all lines of business.

The System is comprised of the following components:

- Infrastructure (facilities, equipment, and networks)

- Software (systems, applications, and utilities)
- People (developers, operators, users, and managers)
- Procedures (automated and manual)
- Data (transaction streams, files, databases, and tables)

The following sections of this description define each of these five components comprising the System.

Infrastructure

The CBV Collection Services Technology (IT) environment includes two data centers located in Markham, Ontario, and Burnaby, BC. Housed within these data centers are the supporting operating system platforms (AS/400 and Windows-based), networking components (routers, switches, firewalls), and data storage devices. The data centers are inter-connected to several designated CBV office locations by an Internet protocol (IP)-based MPLS connection. The IT personnel that support these data centers are primarily based at the Company's corporate office facilities in Burnaby and Markham.

The accompanying SOC 2 examination report covers the IT infrastructure supporting the following technology solutions, which are developed and managed by the CBV IT group:

- Network and Data Centre Operations
- Collections Management System
- Predictive Dialer system

IT is presently responsible for supporting more than one hundred (100) servers supporting the in-scope technology solutions. These servers are summarized below by operating system and the various purposes served.

Operating System	Server Purpose
Windows Server AS/400 Various Unix variants	Monitoring Tools Collections Application and Database Client file transfer systems Backup Domain File and Print Email

Software

Software utilized by IT to manage and support the CBV IT Environment includes:

- Back up management
- System monitoring
- Job scheduling, processing, and monitoring
- Network monitoring
- Security monitoring
- Change management
- Help desk support

The CBV IT Environment described herein does not include application software supporting the technology solutions provided by CBV to individual clients or CBV business unit applications.

People

IT personnel provide the following core support services over the CBV IT Environment components above:

- Systems and Network Monitoring
- Security
- Database Administration
- Backup Operations
- Network Management
- Application Change Management
- Infrastructure Change Management

In order to provide these services, IT is divided into several functional areas: Network Services, Development, Support, and Dialer Operations. Below is a brief description of each of these functional areas:

- **Network Management Services:** The team deals with Fault, Configuration, Accounting, Performance and Security (FCAPS) - It keeps the network up and running smoothly, and monitors the network to spot problems as soon as possible, ideally before users are affected, keeping track of resources on the network and how they are assigned.
- **AS/400 Development:** The team oversees new product developments, client customizations, new releases, and updates for client software.
- **Support:** The team deals with maintenance, repairs, and upgrades attending to client support.
- **Dialer Operations:** Maintains and manages the Company's predictive dialer systems.

Procedures

CBV has documented policies and procedures to support the operations and controls over its IT Environment.

Specific examples of the relevant policies and procedures include the following:

- Policy management and communication
- System security administration
- Server security configuration
- Computer operations
- Network operations
- Disaster recovery planning
- Change management
- Incident/Problem management
- Physical security
- Backup and secured storage

Data

AS/400 Development manages the Company's collections management system within the IT Environment. Access to data is limited to authorized personnel per the Company's system security administration policies.

IT is also responsible for the overall availability of data, including system backups, monitoring of data processing, and file transmissions as well as identifying and resolving problems.

Disclosures

For the period under review, there were no reported incidents that originated from CBV. There were no material changes committed during the period that were within the boundaries of the System Description.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, MONITORING, AND INFORMATION AND COMMUNICATION

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The control environment has a pervasive influence on the structure of business activities, establishment of objectives, and assessment of risks. It influences control activities, information and communication systems, and monitoring procedures. The control environment is influenced by an entity's history and managerial culture. Effectively controlled entities strive to have competent personnel, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive corporate direction. These entities establish appropriate controls that foster shared values and teamwork in the pursuit of the organization's objectives.

Control environment elements include the following, and the extent to which each element is addressed at CBV is described below:

- Management Controls, Philosophy, and Operating Style
- Integrity and Ethical Values
- Organizational Structure
- Assignment of Authority and Responsibility
- Standard Operating Controls
- Audit
- Risk Assessment
- Monitoring

Management Controls, Philosophy, and Operating Style

Management is responsible for directing and controlling operations; establishing, communicating, and monitoring control policies and procedures; and setting the tone for the organization. Importance is placed on accuracy and integrity, maintaining written and updated procedures, security and privacy, and establishing and maintaining sound internal controls over all functional aspects of operations.

Management's philosophy and operating style affect the way the entity is managed, including the kinds of business risks accepted. CBV places a great deal of importance on working to ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in daily operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in customer support and transaction processing.

Formal job descriptions and regular departmental meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operates under Company policies and procedures, including confidentiality agreements and security policies. Periodic training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring the customer base for trends, changes, and anomalies.

Competence should reflect the knowledge and skills needed to accomplish tasks that define an individual's job. Through consideration of an entity's objectives and the strategies and plans for the achievement of those objectives, management must determine how well these tasks need to be accomplished. Management identified the competence levels for particular jobs and translated those levels into requisite knowledge and skills.

Integrity and Ethical Values

Maintaining a climate that demands integrity and ethical values is critical to the establishment and maintenance of an effectively controlled organization. The effectiveness of internal controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. CBV has programs and policies designed to promote and ensure integrity and ethical values in its environment.

CBV desires to maintain a safe, pleasant, and cooperative working environment and expects employees to have high standards of performance, integrity, productivity, and professionalism. CBV developed professional conduct policies that set forth policies of importance to all employees relating to ethics, values, and conduct. All employees are expected to know and adhere to these standards, as well as to generally accepted norms of conduct and courtesy at all times. While managers are responsible for understanding, communicating, and enforcing Company policies, this does not override or diminish an employee's responsibility to be aware of and adhere to these policies. Violations of these policies or other forms of misconduct may lead to disciplinary or corrective action up to and including dismissal.

Standards of Conduct

The Company implemented standards of conduct to guide all employee and contractor behavior. Management monitors behavior closely, and exceptions to these standards lead to immediate corrective action as defined by Human Resources (HR) policies and procedures. Additionally, all employees must sign confidentiality agreements before employment. Any employee found to have violated the Company's ethics policy may be subject to disciplinary action, up to and including termination of employment.

Commitment to Competence

The Company has formal job descriptions that define roles and responsibilities and the experience and background required to perform jobs professionally and competently. The Company determines the knowledge and skills needed to perform job duties and responsibilities and hires for that skill set and job requirement. Management monitors and formally evaluates employee and contractor performance periodically to determine that performance meets or exceeds CBV standards.

Organizational Structure

An entity's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Significant aspects of establishing a relevant organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. Significant cross-training between Management positions and between staff positions exists to help ensure smooth operations and maintenance of controls during staff or Management absence.

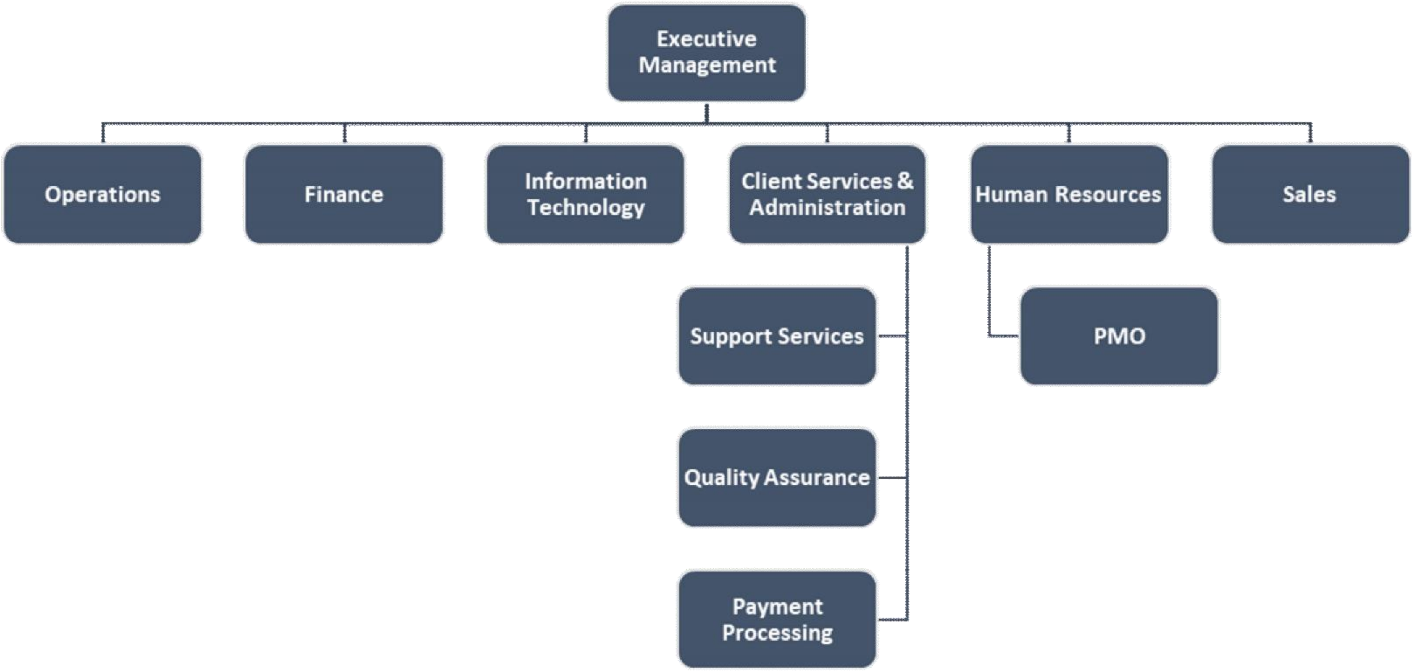
Assignment of Authority and Responsibility

The extent to which individuals recognize that they are held accountable influences the control environment. This holds true for everyone who has ultimate responsibility for activities within an entity, including the internal control system. This includes the assignment of authority and responsibility for operating activities and the establishment of reporting relationships and authorization protocols. CBV's Management encourages individuals and teams to use initiative in addressing issues and resolving problems. Policies describing appropriate business practices, knowledge and experience of key personnel, and available resources are provided to employees to assist them in carrying out their duties.

The Company is led by a team of Senior Executives that assigns authority and responsibility to key Management personnel with the skills and experience necessary to carry out their assignments. Such assignments commonly relate to achieving corporate objectives, oversight of operating functions, and any compliance with applicable regulatory requirements. Open dialogue and individual initiative are encouraged as fundamental parts of the Company's goal to deliver client service.

Roles and Responsibilities

The following organizational chart depicts CBV's corporate structure.



Executive Management is responsible for developing and establishing organizational goals, strategic vision, organizational direction, client strategy, client acquisition, market positioning, and company growth.

CBV is segregated into the following six (6) distinct and separate departments:

Operations – The Operations Department is responsible for collections activities. It operates call centers across Canada to manage CBV client needs.

Finance – The Finance Department is responsible for accounting processes, including managing debt settlement.

Information Technology – The Information Technology Department manages CBV's technology infrastructure, including the Collections Management System, predictive dialer, and telephony systems.

Client Services & Administration – This department consists of Support Services, Quality Assurance, and Payment Processing. A brief description of these teams is as follows.

Support Services – The Support Services Team is responsible for the support of CBV's clients.

Quality Assurance – The Quality Assurance Team is responsible for ensuring collections operations are held to high standards for quality and meet regulatory and client requirements.

Payment Processing – The Payment Processing Team is responsible for managing credit card payments in compliance with the Payment Card Industry Data Security Standard (PCI-DSS).

Human Resources – The Human Resources Department is responsible for the Company's most valuable asset – its people. HR manages the recruiting, onboarding, training, recognition, and improvement processes for all staff including the Project Management Office.

Project Management Office (PMO) – The PMO Team is responsible for the independent management of projects across CBV.

Sales – The Sales Department is responsible for sales and business development.

Standard Operating Controls

CBV Management sends guidance to employees regarding expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluation, counseling, promotion, compensation, and remedial actions.

CBV has hiring practices that are designed to help ensure that new employees are qualified for their job responsibilities. All applicants pass through an interview process that assesses their qualifications related to the expected responsibility level of the individual. CBV conducts pre-employment reference checks from information provided on the employment application. HR conducts pre-hire background investigations relating to past employment history, credit history, and criminal activity per the Fair Credit Reporting Act (FCRA).

CBV invests significant resources in employee development by providing on-the-job training and other learning opportunities. New employees participate in an orientation program that acquaints them with the Company's organization, its affiliated companies, functions, values, products, and selected policies. Thereafter, development activities include providing more challenging assignments, job rotation, training programs, seminars, and continuing education programs. Additionally, employees are provided with measurable objectives and are subject to periodic performance reviews to help ensure competence.

Security Awareness

CBV conducts security training programs for all employees in the areas of physical safety and security. Each member of CBV is made aware of the security implications that revolve around their functions and actions. Approaching security as an organization has a more profound effect than relying solely on a single group. This process begins with providing individuals with the understanding and knowledge needed to help secure them and their data within established policies. Security awareness programs include the message that individual users can have a significant impact on the overall security of an organization.

Human Resources oversees the training and awareness of the topics contained in the Employee Handbook and the Client Security Policy:

- Computer and Email Usage
- Use of Telephones
- Use of Equipment
- Internet Usage Summary Policy
- Computer Software
- Personal Use of Company Property
- Property and Equipment Care
- Restricted Areas
- Return of Company Property
- Safety Rules
- Security Violations of Policies

Audit

CBV Management performs periodic audits of procedures and holds scheduled compliance meetings with staff to review current and new procedures.

Risk Assessment

CBV has a cross-functional risk assessment process that utilizes Management, as well as staff, to identify risks that could affect the Company's ability to meet its contractual obligations. Risk assessment efforts include analyses of threats, probabilities of occurrence, potential business impacts, and associated mitigation plans. Risk mitigation strategies include prevention and elimination through the implementation of internal controls and transference through commercial general and umbrella policies. Management maintains risk plans and updates them at least annually.

Team leaders are required to identify significant risks related to their areas of responsibility and implement measures to mitigate those risks. The Management Team meets regularly to identify any risks and develop corrective steps to minimize the impact of these risks. The Company employs numerous methods to assess and manage risk, including policies, procedures, team structure, recurring meetings, and automated error detection controls. The Company strives to identify and prevent risks at an early stage through policy and procedure adherence in addition to mitigating relevant risks as discovered either through team structure, meetings, or notifications. The Company placed into operation the following teams that facilitate the identification of relevant risks to the achievement of objectives.

The Company maintains security policies and communicates them to staff to ensure that individuals utilizing Company resources understand their responsibility in reducing the risk of compromise and exercise appropriate security measures to protect systems and data.

Monitoring

Management monitors internal controls as part of normal business operations. CBV uses a series of Management reports and processes to monitor the results of the various business processes. The Management Team regularly reviews the reports and logs, and records, and resolves all exceptions to normal processing activities.

The Company uses software to track user and customer requests, which are maintained in a system and tracked until completion. Management performs regular reviews of tasks assigned to their departments/divisions units. Tasks that are not addressed on time are manually escalated and resolved.

The Company's Information Technology Team regularly monitors the network for capacity, performance, and hardware failure. Overall system health and capacity planning are monitored daily to ensure the system will meet the needs of the Company's clients. Administrators monitor security access violations, including server logs and reports.

Monitoring policies and procedures are utilized for addressing issues relating to outages of critical services or other issues needing immediate action. These procedures vary based on the defined severity level of the problem. Company administrators use several monitoring tools to identify and provide alerts to the following conditions:

- A managed system has exceeded a predefined performance or load threshold.
- A managed system has suffered an error condition.
- A managed system has detected a hardware element that is expected to fail soon.
- A managed system is no longer in communication with the monitoring infrastructure.
- A managed system has entered a condition previously specified by Company administrators as operating outside of a threshold.

The IT Department utilizes a third-party resource for performing external vulnerability testing. The assessment includes testing for current and recent known threats against the Company's external-facing Internet firewalls. The testing verifies the configuration of the security policy on the firewall. Detailed reports are delivered upon completion for administrators to act upon if a vulnerability is discovered.

Information and Communication Systems

CBV uses a variety of communication methods to ensure that significant events and issues are conveyed on time and that staff understands their role and responsibility over service and controls. These methods include the following: new hire training, ongoing training, policy and process updates, weekly departmental meetings summarizing events and changes, the use of email to communicate time-sensitive information, and the documentation and storage of historical data in internal repositories for business and support activities. The Company maintains systems that manage the flow of information and facilitate communication with its customers.

Information Flow from Senior Management to Operations Staff

CBV has implemented various methods of communication to help ensure that employees understand their roles and responsibilities over processing and controls and communicate significant events on time. Employee manuals are provided upon hire that communicates policies and procedures concerning employee conduct. Security of the physical premises and logical security of systems is reinforced by training and awareness programs. The communication system between Senior Management and Operations staff includes the use of the office email system, written memos when appropriate, and weekly meetings. Managers hold departmental meetings with personnel to discuss new Company policies and procedures and other business issues.

Monthly staff and training meetings are utilized to inform staff of new policy and technology updates.
Communication is encouraged at all levels to promote the operating efficiency of CBV.

Trust Services Criteria and Related Controls

The Company's trust services criteria and related control activities are included in Section III of this report to eliminate the redundancy that would result from listing them here in Section II and repeating them in Section III.

Although the trust services criteria and related control activities are included in Section III, they are, nevertheless, an integral part of the Company's description of controls.

User Control Considerations

The Company’s applications are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve the control objectives included in this report.

This section describes additional controls that should be in operation at user organizations to complement the controls at the Company. User auditors should consider whether or not the following controls are implemented at user organizations:

- Controls are in place for user organizations to ensure compliance with contractual requirements.
- Controls are in place to ensure that user organizations adopt strong operating system and application password management procedures, including using passwords that cannot be easily compromised and require change regularly.
- Controls are in place to provide reasonable assurance of the compatibility of software not provided by the
    - Company.
- Controls to provide reasonable assurance that the customer has procedures in place for developing, maintaining, and testing their business continuity plans (BCP).
- Controls to provide reasonable assurance that Company IT is notified in advance of any equipment or other shipments they will be sending or receiving.
- Controls to provide reasonable assurance of the transmission and receipt of information not provided by the
    - Company.
- Controls for approving the telecommunications infrastructure between itself and the Company.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Providing data center colocation and managed services for customers by CBV covers only a portion of the overall internal control structure of each customer. The Company's products and services were not designed to be the only control component in the internal control environment. Additional control procedures require implementation at the customer level. It is not feasible for all of the control objectives relating to providing data center colocation and managed services to be fully achieved by CBV. Therefore, each customer’s system of internal controls must be evaluated in conjunction with the internal control structure described in this report

Section IV: Trust Services Criteria and Independent Auditor’s Testing

Procedures

The tests that we performed included the following procedures to the extent they were considered necessary:

Test	Description
Inquiry	Made inquiries of appropriate personnel and corroborated responses using other test procedures (including Observation, Inspection, and/or Re-Performance) to ascertain the existence or operating effectiveness of the control activity.
Observation	Observed application of the control activity.
Inspection	Inspected documents and reports indicating the performance of the control activity.
Re-performance	Re-performed operation of the control activity.

Trust Services Criteria and Related Controls for Systems and Applications

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of CBV. The “Independent Auditor’s Testing Procedures” and the “Results of Tests” are the responsibility of the service auditor

Nr.	Points of focus specified in the COSO Framework	The test applied by the Service Auditor	Test results
CC1.0 - CONTROL ENVIRONMENT			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1	Sets the Tone at the Top—The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.	A) Inspected CC1.1a - 2.1 Code of Conduct Policy.pdf as the most current code of conduct and ethics policy. No issues noted B) Inspected CC1.1b - Complaint Summary new Jun - May 22. pptx which confirms that CBV monitors and upholds its commitments to integrity and ethical values. As inquired, Th Complaint Summary would only be discussed within the monthly meeting if there were concerns, otherwise, all executives review it independently. No issues noted C) Inspected CC1.1c - CBV Confidentiality and Non-Disclosure Agreement 2020.doc as the most current employee confidentiality/nondisclosure policy or agreement. No issues noted.	No relevant exceptions noted
	Establishes Standards of Conduct—The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.	D) Inspected CC1.1a - 2.1 Code of Conduct Policy.pdf as the most current code of conduct and ethics policy. No issues noted E) Inspected CC1.1e - ARC - COLLECTION AGENCY AGREEMENT.pdf, CC1.1e - Provana Master Solution Agmt - CBV Collection Services 062421.pdf and CC1.1e Sample Contract Templates as a sample (2) of executed service agreements for vendors used in the scope of this engagement concerning standards of conduct expected. No issues noted F) Inspected CC1.1c - CBV Confidentiality and Non-Disclosure Agreement 2020.doc as the most current employee confidentiality/nondisclosure policy or agreement. No issues noted.	No relevant exceptions noted

	Evaluates Adherence to Standards of Conduct—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.	G & H) Inspected 5.2 PERFORMANCE STANDARDS & APPRAISALPOLICY which confirms that every employee goes through a review and feedback process. It also, states that employees who are measured against a monthly or a quarterly target may not receive annual reviews based on the fact that they receive regular feedback, direction, and coaching from their Manager. No issues noted	No relevant exceptions noted
	Addresses Deviations promptly—Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.	I) Inspected 5.3 Progressive Improvement Policy.pdf and CC1.1j - Disciplinary Action.xlsx as the most current employee disciplinary policy and procedures. No issues noted. J) Inspected CC1.1j - Disciplinary Action.xlsx as the summary of employee sanctions concerning actions taken. No issues noted.	No relevant exceptions noted
	An additional point of focus specifically related to all engagements using the trust services criteria:		
	Considers Contractors and Vendor Employees in Demonstrating Its Commitment—Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations promptly.	K) Inspected CC1.1k - CS Policy - Vendor Management v3.8.pdf as the most current policy and procedures for contractor and vendor employee onboarding, standards of conduct, and work termination. No issues noted	No relevant exceptions noted
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2	Establishes Oversight Responsibilities—The board of directors identifies and accepts its oversight responsibilities concerning established requirements and expectations.	A) Inspected I1 - CBV New Shareholders Agreement.pdf and CC1.2a - K5 - Certificate of Amalgamation.pdf as the supporting evidence. No issues noted B) Inspected CC1.2b - EMC Minutes 2021-09-13_Redacted.pdf and CC1.2b - EMC Minutes 2021-10-13_Redacted.pdf as a sample of board meeting minutes concerning Senior management oversight responsibilities and established requirements and expectations. No issues noted	No relevant exceptions noted

	Applies Relevant Expertise—The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action.	C) As inquired with CBV, CBV Collections maintains an informal Board of Directors, consisting of Dave Demerchant Chief Operating Officer, and two other owners. Dave leads and manages all day-to-day activities at CBV Collections. As there is no formal BoD, marking this control NA D) Inspected CC1.2b - EMC Minutes 2021-09-13_Redacted.pdf and CC1.2b - EMC Minutes 2021-10-13_Redacted.pdf as a sample of Senior management meeting minutes held during the period under review. No issues noted	No relevant exceptions noted
	Operates Independently—The board of directors has sufficient members who are independent of management and objective in evaluations and decision-making.	E) As inquired with CBV, CBV Collections maintains an informal Board of Directors, consisting of Dave Demerchant Chief Operating Officer, and two other owners. Dave leads and manages all day-to-day activities at CBV Collections. As there is no formal BoD, marking this control NA	No relevant exceptions noted
	An additional point of focus specifically related to all engagements using the trust services criteria:		
	Supplements Board Expertise—The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, through the use of a subcommittee or consultants.	E) As inquired with CBV, CBV Collections maintains an informal Board of Directors, consisting of Dave Demerchant Chief Operating Officer, and two other owners. Dave leads and manages all day-to-day activities at CBV Collections. As there is no formal BoD, marking this control NA	No relevant exceptions noted
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3	Considers All Structures of the Entity—Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.	A) Inspected CC1.3a - CBV Budget F.Y. 2021-22.msg as a sample of budgetary information for the entity concerning consideration for multiple structures used during the period under review. No issues noted	No relevant exceptions noted

	Establishes Reporting Lines — Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.	B) Inspected CC1.3b - CBV FLG Corporate Org Chart.pdf as the most current high-level organizational chart. No issues noted C) Inspected CC1.3c - Re Please choose - updated Org Chart. msg as evidence concerning the organizational reporting structure reviewed. No issues noted.	No relevant exceptions noted
	Defines, Assigns, and Limits Authorities and Responsibilities— Management and the board of directors delegate authority, define responsibilities and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.	D) Inspected CC1.3b - CBV FLG Corporate Org Chart.pdf as the most current high-level organizational chart. No issues noted E) Inspected CC1.3c - Re Please choose - updated Org Chart. msg as evidence concerning the organizational reporting structure reviewed. No issues noted.	No relevant exceptions noted
	Additional points of focus specifically related to all engagements using the trust services criteria:		
	Addresses Specific Requirements When Defining Authorities and Responsibilities— Management and the board of directors consider requirements relevant to **security and availability** when defining authorities and responsibilities.	F) Inspected SecCom Minutes 20220112.pdf and SecCom Minutes 20220420.pdf as a sample of recurring Management meeting minutes OR calendared events concerning organizations, business, and IT requirements objectives. No issues noted G) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted	No relevant exceptions noted

<table>
<tr><td></td><td><u>Considers Interactions With External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities</u>—Management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.</td><td>H) Inspected CC1.1e - ARC - COLLECTION AGENCY AGREEMENT.pdf, CC1.1e - Provana Master Solution Agmt - CBV Collection Services 062421.pdf and CC1.1e Sample Contract Templates as a sample (2) of executed service agreements for vendors used in the scope of this engagement. No issues noted</td><td>No relevant exceptions noted</td></tr>
<tr><td colspan="4"><b>CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives.</b></td></tr>
<tr><td><b>CC1.4</b></td><td><u>Establishes Policies and Practices</u> —Policies and practices reflect expectations of competence necessary to support the achievement of objectives.</td><td>A) Inspected CC1.4a - New Hire Paperwork Package.pdf as the most current AND reviewed Employee Handbook. No issues noted
B1) Inspected CC1.4b1 - 4.1 Recruitment and Selection Policy.pdf as the documented process for evaluating new hire candidates and selecting successful candidates. No issues noted.
B2) Inspected CC1.4b2 - New Hire Process - Flowchart.pdf and CC1.4b2 - CBV New Hire Paperwork Guide.docx as the documented new hire onboarding process. No issues noted
B3) Inspected CC1.4b3 - Departure Checklist.pdf as the documented terminated employee offboarding process (e.g., termination checklist). No issues noted.
C) Inspected CC1.4c CBV Training Program.pdf as the Company's employee training posture. No issues noted.</td><td>No relevant exceptions noted</td></tr>
</table>

	Evaluates Competence and Address Shortcomings—The board of directors and management evaluate competence across the entity and in outsourced service providers concerning established policies and practices and act as necessary to address shortcomings.	D) Inspected CC1.4d - HR Policies - 2022 Master Document Control.xlsx as the Management acknowledgment concerning Employee Handbook, HR, and training policies and procedures reviewed. No issues noted E) Inspected CC1.4e - CS Policy - Vendor Management v3.8.pdf as the most recent vendor management policy and procedures. No issues noted F) Inspected CC1.1e - ARC - COLLECTION AGENCY AGREEMENT.pdf, CC1.1e - Provana Master Solution Agmt - CBV Collection Services 062421.pdf and CC1.1e Sample Contract Templates as a sample (2) of executed service agreements for vendors used in the scope of this engagement. No issues noted	No relevant exceptions noted
	Attracts, Develops, and Retains Individuals — The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.	G) Inspected CC1.4g - Individual Course Results 2021.xlsx as the most current training completion records. No issues noted	No relevant exceptions noted
	Plans and Prepares for Succession —Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control.	H & I) Inspected CC1.4j - SOP - Business Continuity Plan v5.9.pdf as the most current disaster recovery plan and business continuity plan. No issues noted	No relevant exceptions noted
	An additional point of focus specifically related to all engagements using the trust services criteria:		
	Considers the Background of Individuals—The entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.	J & K) Inspected completed background check confirmations for a selection of new hires (CIC363, BRI661, MAH926, MAH081, ADE161, MAU060, SPI178). No issues noted	No relevant exceptions noted

	Considers the Technical Competency of Individuals—The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.	L) Inspected job descriptions AND associated resumes for a selection of new hires. No issues noted	No relevant exceptions noted
	Provides Training to Maintain Technical Competencies — The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.	M) Inspected CC1.4g - Individual Course Results 2021.xlsx as the most current training completion records. No issues noted	No relevant exceptions noted
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5	Enforces Accountability Through Structures, Authorities, and Responsibilities—Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for the performance of internal control responsibilities across the entity and implement corrective action as necessary.	A) Inspected signed acknowledgment of the Employee Handbook for a selection of new hires (CIC363, BRI661, MAH926, MAH081, ADE161, MAU060, SPI178). No issues noted B) Inspected signed NDAs/Confidentiality agreements for a selection of new hires (CIC363, BRI661, MAH926, MAH081, ADE161, MAU060, SPI178). No issues noted C) Inspected signed acknowledgment of the Code of Conduct for a selection of new hires (CIC363, BRI661, MAH926, MAH081, ADE161, MAU060, SPI178). No issues noted D) Inspected Director of IT and CSO 20100119.doc as the job description for the Company's Security Officer. No issues noted	No relevant exceptions noted

	Establishes Performance Measures, Incentives, and Rewards— Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.	E) Inspected CC1.5e - National Contingency - Revised Commission Structure - V.2 Effective January 1, 2022 - ammended.docx as the sample of most current employee performance measures. No issues noted.	No relevant exceptions noted
	Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance— Management and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.	F) Inspected 5.2 PERFORMANCE STANDARDS & APPRAISALPOLICY which confirms that every employee goes through a review and feedback process. It also, states that employees who are measured against a monthly or a quarterly target may not receive annual reviews based on the fact that they receive regular feedback, direction, and coaching from their Manager. No issues noted	No relevant exceptions noted
	Considers Excessive Pressures —Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.	G) Inspected CC1.5e - National Contingency - Revised Commission Structure - V.2 Effective January 1, 2022 - ammended.docx as the sample of most current employee performance measures. No issues noted.	No relevant exceptions noted

	Evaluates Performance and Rewards or Disciplines Individuals—Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and provide rewards or exercise disciplinary action, as appropriate.	H) Inspected CC1.5e - National Contingency - Revised Commission Structure - V.2 Effective January 1, 2022 - ammended.docx as the sample of most current employee performance measures. No issues noted. I) Inspected 5.3 Progressive Improvement Policy.pdf and CC1.1j - Disciplinary Action.xlsx as the most current employee disciplinary policy and procedures. No issues noted.	No relevant exceptions noted

CC2.0 - COMMUNICATION AND INFORMATION

CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

CC2.1	Identifies Information Requirements —A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.	A) Inspected CC2.1a - CBV System Description.docx as the most current system description. No issues noted B) Inspected CC2.1b - CBV Intranet - Policies.docx as a screenshot of the location of your policies, procedures, and organizational structure for internal users. No issues noted C) Inspected CC2.1c - Terms of Service.png as a screenshot of the location of the terms of service for users of your system. No issues noted D) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted E) Inspected global address list (GAL) as a screenshot of the Wiki-based (or online) staff listing or directory. No issues noted	No relevant exceptions noted

	Captures Internal and External Sources of Data — Information systems capture internal and external sources of data.	F) Inspected COINFINC_AC1X0000_QPQUPRFIL_73_QPADEV004X_618228_083122070011, ET-NRGUERE_20220831_091146.pdf, ETPNRGUE01_20220831_091144.pdf, INBOUND FILE LOGS TO AS400.zip, MTNPLEDT_AC1X0000_REPORT_79_QPADEV004X_618228_083122070127.pdf, MTRCLEDT_AC1X0000_QPQUPRFIL_89_QPADEV004X_618228_083122070443.pdf as a sample (6) of system generated logs of critical data received AND transmitted, by the System at either the application or service layer. No issues noted	No relevant exceptions noted
	Processes Relevant Data Into Information — Information systems process and transform relevant data into information.	G) Inspected CC2.11-BLXPMTB_AC1X0000_REPORT_33_QPADEV004X_432641_070422160515.pdf, CC2.11-BODAYBALC_AC1X0000_20220705090127.pdf, and CC2.11-DRNPMTB_AC1X0000_REPORT_66_QPADEV001 as samples (3) of system generated data output files (e.g., reports, communications, notifications) captured and processed using CC2.1F sources of data. No issues noted	No relevant exceptions noted
	Maintains Quality Throughout Processing — Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.	I) Inspected BLXPMTB_AC1X0000_REPORT_33_QPADEV004X_432641_070422160515.pdf, BODAYBALC_AC1X0000_20220705090127.pdf, and DRNPMTB_AC1X0000_REPORT_66_QPADEV001Q_443573_070522084021.pdf in a form of edit listings which is automatically generated after the loading process has completed. These files evidence the samples (3) of error logging or exception reporting. No issues noted J) As inquired, Data Operations provides a loading summary notification and edit listing if necessary to CSR. CSR will then communicate with the client as to how to move forward with the exceptions. If anything processed runs into an error, a ticket will be opened to AS400, so that a programmer will take a further look and fix the data or program as needed. Inspected RE CAP ONE LOADED WITH REJECTIONS (1).msg, RE CAP ONE LOADED WITH REJECTIONS.msg which evidences the above procedure. Control is compliant as it is operating effectively. No issues noted **Suggestion:** To fulfill the design effectiveness of the control, please create detailed Standard Operating Procedures on Errors and Exceptions handling	No relevant exceptions noted

CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

CC2.2	Communicates Internal Control Information—A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.	A) Inspected CC2.2a - Policy - Security v4.1.pdf as the most current information security policy. No issues noted B) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted C) Inspected CC2.1b - CBV Intranet - Policies.docx as a screenshot of the location of your policies, procedures, and organizational structure for internal users. No issues noted	No relevant exceptions noted
	Communicates With the Board of Directors—Communication exists between management and the board of directors so that both have the information needed to fulfill their roles concerning the entity's objectives.	D) As inquired with CBV, CBV Collections maintains an informal Board of Directors, consisting of Dave Demerchant Chief Operating Officer, and two other owners. Dave leads and manages all day-to-day activities at CBV Collections. As there is no formal BoD, marking this control NA E) As inquired, there have been no incidents within this audit period where a formal notification would be sent out to Senior Management. No issues noted	No relevant exceptions noted
	Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	F) Inspected CC2.2f - Whistleblower Screenshot.pdf as a screenshot of the secure channel input interface. No issues noted	No relevant exceptions noted
	Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the information.	G) Inspected CC2.2g - Annual VIP training modules - Part 1 Module annuels de formation VIP - Partie 1. msg, CC2.2g - New Feature in VIP Send your payslips by email! Nouvelle Fonctionnalité en VIP Envoyez vos fiches de paie par email!.msg and CC2.2g - New Policy - Covid19 Vaccine. msg as a sample (3) of internal communications concerning Company objectives OR changes to objectives (such as schedules, rollout plans, new compliance requirements, or changes to operations or staff) for the period under review.	No relevant exceptions noted

	Communicates Responsibilities—Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.	H) Inspected Director of IT and CSO 20100119.doc and Network Manager 2008.doc as the sample was written job descriptions for IT security AND system admin personnel within the organization. No issues noted I) Inspected CC2.2i Promotion Announcement - Felipe Sequeira.pdf as a sample of employee responsibility change notifications concerning IT and/or system admin personnel. No issues noted	No relevant exceptions noted
	Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters—Entity personnel are provided with information on how to report systems failures, incidents, concerns, and other complaints to personnel.	J) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted	No relevant exceptions noted
	Communicates Objectives and Changes to Objectives—The entity communicates its objectives and changes to those objectives to personnel promptly.	K) Inspected CC2.2g - Annual VIP training modules - Part 1 Module annuels de formation VIP - Partie 1. msg, CC2.2g - New Feature in VIP Send your payslips by email! Nouvelle Fonctionnalité en VIP Envoyez vos fiches de paie par email!.msg and CC2.2g - New Policy - Covid19 Vaccine. msg as a sample (3) of internal communications for Company objectives OR changes to objectives (such as schedules, rollout plans, new compliance requirements, or changes to operations or staff) for the period under review.	No relevant exceptions noted
	Communicates Information to Improve Security Knowledge and Awareness—The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.	L) Inspected security awareness training completion records/confirmations. for a selection of active employees (MAC563,CHI381,JIA640,DJA101,BHA085,PAN511,LEP185, GAI201,LAF259,CIC363). No issues noted	No relevant exceptions noted
	Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level:		

	Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation.	M) Inspected CC2.1a - CBV System Description.docx as the most current system description. No issues noted N) Inspected CC2.1b - CBV Intranet - Policies.docx as a screenshot of the location of your policies, procedures, and organizational structure for internal users. No issues noted	No relevant exceptions noted
	Communicates System Objectives—The entity communicates its objectives to personnel to enable them to carry out their responsibilities.	O) Inspected CC2.1a - CBV System Description.docx as the most current system description. No issues noted P) Inspected CC2.1b - CBV Intranet - Policies.docx as a screenshot of the location of your policies, procedures, and organizational structure for internal users. No issues noted	No relevant exceptions noted
	Communicates System Changes—System changes that affect responsibilities or the achievement of the entity's objectives are communicated on time.	Q) Inspected CC2.2g - Annual VIP training modules - Part 1 Module annuels de formation VIP - Partie 1. msg, CC2.2g - New Feature in VIP Send your pay slips by email! Nouvelle Fonctionnalité en VIP Envoyez vos fiches de paie par email!.msg and CC2.2g - New Policy - Covid19 Vaccine. msg as a sample (3) of internal communications concerning Company objectives OR changes to objectives (such as schedules, rollout plans, new compliance requirements, or changes to operations or staff) for the period under review.	No relevant exceptions noted

CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

CC2.3	Communicates to External Parties—Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.	A) Inspected CC2.3a - Letter of Attestation - Dec 2021.pdf as a screenshot of the mode of communication to external parties concerning system description/system operations/internal controls (e.g., terms of service, system description, etc.). As inquired, this communication is provided at the time of client audits and upon request from our clients. No issues noted B) Inspected CC2.3a - Letter of Attestation - Dec 2021.pdf as a sample of notifications to external parties concerning system operations/internal controls. No issues noted	No relevant exceptions noted
	Enables Inbound Communications—Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.	C) As inspected, https://www.cbvcollections.com/contact/ is the path for customers/business partner entry points to create a ticket, fax, email, or ftp, their needs, and expectations to the entity. No issues noted	No relevant exceptions noted
	Communicates With the Board of Directors—Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.	D) Inspected SecCom Minutes 20210712.pdf as evidence that external assessments, concerning security and availability, are communicated to the Sr. Mgmt. No issues noted	No relevant exceptions noted
	Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	E) Inspected CC2.3e External Parties Communication.docx as a screenshot of the externally facing hotline user interface OR secure method to receive secure, anonymous/confidential communications (from external users). No issues noted	No relevant exceptions noted

	Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.	F) Inspected New Brunswick- CBV Collection Services Ltd-Signed FS FY June 30'21.msg, Newfoundland#01-15-CB110-1 CBV Collection Services Ltd-Signed FS FY June 30'21.msg and PEI # 3576 CBV Collection Services Ltd-Signed FS FY June 30'21.msg as a sample (3) of external communications concerning changes of schedules, rollouts, new compliance requirements, or changes to operations for the period under review. No issues noted	No relevant exceptions noted
	An additional point of focus that applies only to an engagement using the trust services criteria for confidentiality:		
	Communicates Objectives Related to Confidentiality and Changes to Objectives—The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives, and changes to objectives related to confidentiality.	G) Inspected https://www.cbvcollections.com/company/privacy/ as the most current externally facing documentation concerning objectives and changes to objectives related to confidentiality. No issues noted	No relevant exceptions noted
	An additional point of focus that applies only to an engagement using the trust services criteria for privacy:		
	Communicates Objectives Related to Privacy and Changes to Objectives—The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives related to privacy, and changes to those objectives.	H) Inspected https://www.cbvcollections.com/company/privacy/ as the most current externally facing documentation concerning objectives and changes to objectives related to privacy. No issues noted	No relevant exceptions noted
	Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level:		

	Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the system and the results of system operation.	I) Inspected CC2.3a - Letter of Attestation - Dec 2021.pdf as a screenshot of the mode of communication to external parties concerning system description/system operations/internal controls (e.g., terms of service, system description, etc.). As inquired, this communication is provided at the time of client audits and upon request from our clients. No issues noted	No relevant exceptions noted
	Communicates System Objectives—The entity communicates its system objectives to appropriate external users.	J) Inspected CC1.1e - ARC - COLLECTION AGENCY AGREEMENT.pdf, CC1.1e - Provana Master Solution Agmt - CBV Collection Services 062421.pdf and CC1.1e Sample Contract Templates as a sample (2) of executed service agreements for vendors used in the scope of this engagement. No issues noted	No relevant exceptions noted
	Communicates System Responsibilities—External users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive communications about their responsibilities and have the information necessary to carry out those responsibilities.	K) Inspected CC1.1e - ARC - COLLECTION AGENCY AGREEMENT.pdf, CC1.1e - Provana Master Solution Agmt - CBV Collection Services 062421.pdf and CC1.1e Sample Contract Templates as a sample (2) of executed service agreements for vendors used in the scope of this engagement. No issues noted	No relevant exceptions noted
	Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters—External users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.	L) As inquired, "CBV's Incident Response Policy is available upon request for clients". Any critical incident impacting the client will be communicated. There were no critical incidents logged for the audit period. No issues noted. M) As inspected, https://www.cbvcollections.com/contact/ is the path for customers/business partner entry points to create a ticket, fax, email, or ftp, their needs, and expectations to the entity. No issues noted	No relevant exceptions noted

CC3.0 - RISK ASSESSMENT

CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

CC3.1	Operations Objectives Reflects Management's Choices—Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.	A) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted B) Inspected CC3.1b - SecCom Minutes 20220112.pdf as a sample of risk management review meeting minutes. No issues noted.	No relevant exceptions noted
	Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives.	C) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted	No relevant exceptions noted
	Includes Operations and Financial Performance Goals—The organization reflects the desired level of operations and financial performance for the entity within operations objectives.	D) Inspected CC1.3a - CBV Budget F.Y. 2021-22.msg as a sample of budgetary information for the entity concerning operational and budgetary objectives. No issues noted	No relevant exceptions noted
	Forms a Basis for Committing of Resources—Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.	E) Inspected CC1.3a - CBV Budget F.Y. 2021-22.msg as a sample of budgetary information for the entity concerning operational and budgetary objectives. No issues noted	No relevant exceptions noted
	External Financial Reporting Objectives Complies With Applicable Accounting Standards—Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate for the circumstances.	F) Inspected CC1.3a - CBV Budget F.Y. 2021-22.msg as a sample of budgetary information for the entity concerning financial reporting objectives consistent with accepted accounting principles. No issues noted	No relevant exceptions noted

	Considers Materiality—Management considers materiality in financial statement presentation.	G) Inspected CC3.1g1 - CBV Collection Services Ltd. Final FS - June 30, 2021-signed.pdf as the most current and approved financial presentation(s). No issues noted	No relevant exceptions noted
	External Nonfinancial Reporting Objectives Complies With Externally Established Frameworks—Management establishes objectives consistent with laws and regulations or standards and frameworks of recognized external organizations.	H) Inspected CC1.1e - ARC - COLLECTION AGENCY AGREEMENT.pdf, CC1.1e - Provana Master Solution Agmt - CBV Collection Services 062421.pdf and CC1.1e Sample Contract Templates as a sample (2) of executed service agreements for vendors used in the scope of this engagement. No issues noted	No relevant exceptions noted
	Reflects Entity Activities—External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.	I) Inspected ISMS Register - Risk Analysis_2022.xlsx as a sample of identified risks and their associated rating and part of the risk assessment process reviewed by Management. No issues noted	
	Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting.	J) Inspected CC3.1g3 - TransUnion Canada 2021 SOC2.pdf and CC3.1g3 - IT SOC 2 Type 2 Report Final.pdf as the most current SOC 1 Type 2 and/or SOC 2 Type 2 reports for sub-service organizations. No issues noted K) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed. pdf as the most current PCI report. No issues noted. L) Inspected CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf and CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed. pdf as a sample of (2) third-party vulnerability assessments. No issues noted	No relevant exceptions noted

	Reflects Entity Activities—External reporting reflects the underlying transactions and events within a range of acceptable limits.	M) Inspected CC3.1g3 - TransUnion Canada 2021 SOC2.pdf and CC3.1g3 - IT SOC 2 Type 2 Report Final.pdf as the most current SOC 1 Type 2 and/or SOC 2 Type 2 reports for sub-service organizations. No issues noted N) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed. pdf as the most current PCI report. No issues noted. O) Inspected CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf and CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed. pdf as a sample of (2) third-party vulnerability assessments. No issues noted	No relevant exceptions noted
	Internal Reporting Objectives Reflects External Laws and Regulations—Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.	P) Inspected CC1.1a - 2.1 Code of Conduct Policy.pdf as the most current code of conduct and ethics policy. No issues noted	No relevant exceptions noted
	Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.	Q) Inspected CC3.1g3 - TransUnion Canada 2021 SOC2.pdf and CC3.1g3 - IT SOC 2 Type 2 Report Final.pdf as the most current SOC 1 Type 2 and/or SOC 2 Type 2 reports for sub-service organizations. No issues noted Inspected CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, and Internal Penetration Test.pdf. No issues noted	

	Reflects Entity Activities—Internal reporting reflects the underlying transactions and events within a range of acceptable limits.	R) Inspected CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_Websites_June2022.csv and CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed. pdf as the most recent internal or external vulnerability assessment completed within the period under review. No issues noted	
	Compliance Objectives Reflects External Laws and Regulations—Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.	S) Inspected I1 - CBV New Shareholders Agreement.pdf and CC1.2a - K5 - Certificate of Amalgamation.pdf as the supporting evidence. No issues noted	
	Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives.	T) Inspected ISMS Register - Risk Analysis_2022.xlsx as a sample of identified risks and their associated rating and part of the risk assessment process reviewed by Management. No issues noted	

	An additional point of focus specifically related to all engagements using the trust services criteria:		
	Establishes Sub-objectives to Support Objectives—Management identifies sub-objectives related to security and availability to support the achievement of the entity's objectives related to reporting, operations, and compliance.	U) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted	No relevant exceptions noted
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2	Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels—The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.	A) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted B) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted	No relevant exceptions noted
	Analyzes Internal and External Factors—Risk identification considers both internal and external factors and their impact on the achievement of objectives.	C) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted D) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted	No relevant exceptions noted

	Involves Appropriate Levels of Management—The entity puts into place effective risk assessment mechanisms that involve appropriate levels of management.	E) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted	No relevant exceptions noted
	Estimates Significance of Risks Identified—Identified risks are analyzed through a process that includes estimating the potential significance of the risk.	F) Inspected ISMS Register - Risk Analysis_2022.xlsx as a sample of identified risks and their associated rating and part of the risk assessment process reviewed by Management. No issues noted	No relevant exceptions noted
	Determines How to Respond to Risks—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.	G) Inspected ISMS Register - Risk Analysis_2022.xlsx as a sample of identified risks and their associated rating and part of the risk assessment process reviewed by Management. No issues noted	No relevant exceptions noted
	An additional point of focus specifically related to all engagements using the trust services criteria:		
	Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities—The entity's risk identification and assessment process include: (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; (4) identifying the vulnerabilities of the identified assets.	H) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted I) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted J) Inspected "CC3.2 J Provide the most current IT asset inventory concerning asset owners.docx, CC3.2. J-1, CC3.2. J-2, CC3.3c - Asset Inventory 2022(Portable Devices).pdf and CC3.3c - Asset Inventory 2022.pdf" as the most current IT asset inventory concerning asset owners. No issues noted	No relevant exceptions noted

	Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties—The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.	K) Inspected CC1.4e - CS Policy - Vendor Management v3.8.pdf as the most recent vendor management policy and procedures. No issues noted	No relevant exceptions noted
	Considers the Significance of the Risk—The entity's consideration of the potential significance of the identified risks includes : (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.	L) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted M) Inspected "CC3.2 J Provide the most current IT asset inventory concerning asset owners.docx, CC3.2. J-1, CC3.2.J-2, CC3.3c - Asset Inventory 2022(Portable Devices).pdf and CC3.3c - Asset Inventory 2022.pdf" as the most current IT asset inventory concerning asset owners. No issues noted	No relevant exceptions noted
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3	Considers Various Types of Fraud—The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.	A) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted B) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted C) Inspected "CC3.2 J Provide the most current IT asset inventory concerning asset owners.docx, CC3.2. J-1, CC3.2. J-2, CC3.3c - Asset Inventory 2022(Portable Devices).pdf and CC3.3c - Asset Inventory 2022.pdf" as the most current IT asset inventory concerning asset owners. No issues noted	No relevant exceptions noted

	Assesses Incentives and Pressures—The assessment of fraud risks considers incentives and pressures.	D) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted	No relevant exceptions noted
	Assesses Opportunities—The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts.	E) Inspected CC3.3e - IT Policy - Data and Media Destruction v3.2.pdf as the most current policy and procedures for the disposal of assets or firmware. No issues noted	No relevant exceptions noted
	Assesses Attitudes and Rationalizations—The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.	F) Inspected CC3.3g - Policy - Acceptable Use v4.0.pdf as the most current acceptable use policy. No issues noted	No relevant exceptions noted
	An additional point of focus specifically related to all engagements using the trust services criteria:		
	Considers the Risks Related to the Use of IT and Access to Information—The assessment of fraud risks includes consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information.	G) Inspected "CC3.2 J Provide the most current IT asset inventory concerning asset owners.docx, CC3.2. J-1, CC3.2.J-2, CC3.3c - Asset Inventory 2022(Portable Devices).pdf and CC3.3c - Asset Inventory 2022.pdf" as the most current IT asset inventory concerning asset owners. No issues noted H) Inspected CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf and CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed. pdf as a sample of (2) third-party vulnerability assessments. No issues noted	No relevant exceptions noted
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4	Assesses Changes in the External Environment—The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.	A) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted B) Inspected CC2.2a - Policy - Security v4.1.pdf as the most current physical security policy and procedures (pg. 4). No issues noted	No relevant exceptions noted

	Assesses Changes in the Business Model—The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.	C) Inspected CC1.3a - CBV Budget F.Y. 2021-22.msg as a sample of budgetary information for the entity concerning operational and budgetary objectives. No issues noted D) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted	No relevant exceptions noted
	Assesses Changes in Leadership—The entity considers changes in management and respective attitudes and philosophies on the system of internal control.	E) Inspected a sample email communication concerning changes in leadership and system control objectives. No issues noted F) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted	No relevant exceptions noted
	An additional point of focus specifically related to all engagements using the trust services criteria:		
	Assess Changes in Systems and Technology—The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.	G) Inspected Change Management Policy as the most current, documented change management policy and procedures. No issues noted	No relevant exceptions noted

	Assess Changes in Vendor and Business Partner Relationships—The risk identification process considers changes in vendor and business partner relationships.	H) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted I) Inspected CC1.4e - CS Policy - Vendor Management v3.8.pdf as the most recent vendor management policy and procedures. No issues noted	No relevant exceptions noted
CC4.0 - MONITORING ACTIVITIES			
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1	Considers a Mix of Ongoing and Separate Evaluations—Management includes a balance of ongoing and separate evaluations.	A) Inspected CC4.1a - network server monitoring software management console.jpg as a screenshot of the network/ server monitoring software management console. No issues noted B) Inspected CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf and CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed. pdf as a sample of (2) third-party vulnerability assessments. No issues noted	No relevant exceptions noted
	Considers Rate of Change—Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.	C) Inspected CC4.1a - network server monitoring software management console.jpg as a screenshot of the network/ server monitoring software management console. No issues noted D) Inspected Change Management Policy as the most current, documented change management policy and procedures. No issues noted	No relevant exceptions noted

	Establishes Baseline Understanding—The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.	E) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted F) Inspected CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf and CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed. pdf as a sample of (2) third-party vulnerability assessments. No issues noted	No relevant exceptions noted
	Uses Knowledgeable Personnel—Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.	G) Inspected Director of IT and CSO 20100119.doc and Network Manager 2008.doc as the sample was written job descriptions for IT security AND system admin personnel within the organization. No issues noted	No relevant exceptions noted
	Integrates With Business Processes—Ongoing evaluations are built into the business processes and adjust to changing conditions.	H) Inspected CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf and CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed. pdf as a sample of (2) third-party vulnerability assessments. No issues noted I) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted	No relevant exceptions noted
	Adjusts Scope and Frequency—Management varies the scope and frequency of separate evaluations depending on risk.	J) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted	No relevant exceptions noted

	Objectively Evaluates—Separate evaluations are performed periodically to provide objective feedback.	K) Inspected CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf and CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed. pdf as a sample of (2) third-party vulnerability assessments. No issues noted	No relevant exceptions noted
	An additional point of focus specifically related to all engagements using the trust services criteria:		
	Considers Different Types of Ongoing and Separate Evaluations—Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.	L) Inspected CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf and CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed. pdf as a sample of (2) third-party vulnerability assessments. No issues noted M) Inspected External Penetration Test.pdf and Internal Penetration Test.pdf as the most current penetration testing results. No issues noted N) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted	No relevant exceptions noted
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies promptly to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2	Assesses Results—Management and the board of directors, as appropriate, assess the results of ongoing and separate evaluations.	A) Inspected SecCom Minutes 20210712.pdf, SecCom Minutes 20220112.pdf, and SecCom Minutes 20220420.pdf as a sample (3) of risk assessment and security review meeting minutes. No issues noted	No relevant exceptions noted
	Communicates Deficiencies—Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.	B) Inspected Ticket 835388.pdf, Ticket 839434.pdf, and Ticket 840678.pdf as a sample of completed change requests concerning change communication to affected parties AND Management. No issues noted.	No relevant exceptions noted

	Monitors Corrective Action—Management tracks whether deficiencies are remedied on a timely basis.	c) Inspected CC4.2C infrastructure change ticketing system--.jpg, CC4.2C infrastructure change ticketing system.pdf, and CC4.2C infrastructure change ticketing system_.pdf as a screenshot of the infrastructure change ticketing system. No issues noted D) Inspected CC4.2d - software development ticketing system.jpg as a screenshot of the software development ticketing system. No issues noted E) Inspected CC4.2E infrastructure change ticketing system.pdf, CC4.2E infrastructure change ticketing system_ (2).pdf and CC4.2E infrastructure change ticketing system_.pdf as a sample (3) of completed deficiency tickets (change requests). No issues noted	No relevant exceptions noted
CC5.0 - CONTROL ACTIVITIES			
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1	Integrates With Risk Assessment—Control activities help ensure that risk responses that address and mitigate risks are carried out.	A) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted B) Inspected DR Run Book_Nov 2021.pdf, DR testing evidence_IT_20211119.pdf, and Letter of Attestation - Dec 2021.pdf as the most current disaster recovery testing results. No issues noted C) Inspected CC3.4g - IT Policy - Server and Security System Standards v3.9.pdf (Pg 6,7 & 9) as the most current, documented server build and hardening procedures. No issues noted	No relevant exceptions noted

	Considers Entity-Specific Factors—Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.	D) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted E) Inspected SecCom Minutes 20210712.pdf, SecCom Minutes 20220112.pdf, and SecCom Minutes 20220420.pdf as a sample (3) of risk assessment and security review meeting minutes. No issues noted	No relevant exceptions noted
	Determines Relevant Business Processes—Management determines which relevant business processes require control activities.	F) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted G) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted	No relevant exceptions noted

	Evaluates a Mix of Control Activity Types—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.	H) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted I) Inspected CC1.4e - CS Policy - Vendor Management v3.8.pdf as the most recent vendor management policy and procedures. No issues noted J) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted	No relevant exceptions noted
	Considers at What Level Activities Are Applied—Management considers control activities at various levels in the entity.	K) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted	No relevant exceptions noted
	Addresses Segregation of Duties—Management segregates incompatible duties, and where such segregation is not practical, management selects and develops alternative control activities.	L & M) Inspected the communication from HR to IT for network access and provide completed network access requests for a selection of new hires (CIC363, BRI661, MAH926, MAH081, ADE161, MAU060, SPI178). No issues noted	No relevant exceptions noted
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2	Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls—Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.	A) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted B) Inspected CC1.3a - CBV Budget F.Y. 2021-22.msg as a sample of budgetary information for the entity concerning operational and budgetary objectives. No issues noted	No relevant exceptions noted

	Establishes Relevant Technology Infrastructure Control Activities—Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.	C) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted D) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted E) Inspected SOP - Business Continuity Plan v5.9.pdf and DR Run Book_Nov 2021.pdf as the most current disaster recovery plan. No issues noted	No relevant exceptions noted
	Establishes Relevant Security Management Process Controls Activities—Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.	F) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted G) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted H) Inspected CC6.2e - CBV - Help Desk - ALL LOCATIONS - Internal Review - Monthly Elevated Privileges Checks (April 2022).pdf and CC6.2e - CBV - Help Desk - ALL LOCATIONS - Internal Review - Monthly Elevated Privileges Checks (March 2022).pdf as a sample (2) of completed network access rights reviews (e.g., quarterly access rights reviews). No issues noted	No relevant exceptions noted

	Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities—Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.	I) Inspected CC1.3a - CBV Budget F.Y. 2021-22.msg as the most current budget concerning IT procurement and maintenance. No issues noted	No relevant exceptions noted
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.			
CC5.3	Establishes Policies and Procedures to Support Deployment of Management 's Directives—Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.	A) Inspected CC2.2a - Policy - Security v4.1.pdf as the most current information security policy. No issues noted	No relevant exceptions noted
	Establishes Responsibility and Accountability for Executing Policies and Procedures—Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.	B) Inspected SecCom Minutes 20210712.pdf, SecCom Minutes 20220112.pdf, and SecCom Minutes 20220420.pdf as a sample (3) of risk assessment and security review meeting minutes. No issues noted	No relevant exceptions noted
	Performs on time—Responsible personnel perform control activities on time as defined by the policies and procedures.	C) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and ISMS Register - Risk Analysis_2022.xlsx as the most current internal audit program concerning actions taken & results. No issues noted	No relevant exceptions noted
	Takes Corrective Action—Responsible personnel investigates and acts on matters identified as a result of executing control activities.	D) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and ISMS Register - Risk Analysis_2022.xlsx as the most current internal audit program concerning actions taken & results. No issues noted	No relevant exceptions noted

	Performs Using Competent Personnel—Competent personnel with sufficient authority perform control activities with diligence and continuing focus.	E) Inspected Director of IT and CSO 20100119.doc and Network Manager 2008.doc as the sample was written job descriptions for IT security AND system admin personnel within the organization. No issues noted	No relevant exceptions noted
	Reassesses Policies and Procedures—Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.	G) Inspected SecCom Minutes 20210712.pdf, SecCom Minutes 20220112.pdf, and SecCom Minutes 20220420.pdf as a sample (3) of risk assessment and security review meeting minutes. No issues noted H) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted	No relevant exceptions noted
CC6.0 - LOGICAL AND PHYSICAL ACCESS CONTROLS			
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1	Identifies and Manages the Inventory of Information Assets—The entity identifies, inventories, classifies and manages information assets.	A) Inspected "CC3.2 J Provide the most current IT asset inventory concerning asset owners.docx, CC3.2. J-1, CC3.2. J-2, CC3.3c - Asset Inventory 2022(Portable Devices).pdf and CC3.3c - Asset Inventory 2022.pdf" as the most current IT asset inventory concerning asset owners. No issues noted	No relevant exceptions noted
	Restricts Logical Access—Logical access to information assets, including hardware, data (at rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.	B) Inspected CC6.1 B as a screenshot of the operating system security groups. No issues noted	No relevant exceptions noted

	Identifies and Authenticates Users—Persons, infrastructure, and software are identified and authenticated before accessing information assets, whether locally or remotely.	C) Inspected CC6.1 B as a screenshot of the operating system security groups. No issues noted	No relevant exceptions noted
	Considers Network Segmentation—Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.	D) Inspected CC6.1.D.pdf as the most current network topology diagram. No issues noted E) Inspected C6.1 E - System policy Sophos PC Block all.jpg and CC6.1.E.pdf as a screenshot of the DMZ configuration. No issues noted	No relevant exceptions noted
	Manages Points of Access—Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.	F) Inspected CC6.1.F.PNG and CC6.1.E.pdf as a screenshot of the firewall rules regulating access routes. No issues noted G) Inspected CC6.1.G.PNG as evidence that the firewall is configured to log certain events. No issues noted H) Inspected CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf and CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed. pdf as a sample of (2) third-party vulnerability assessments. No issues noted	No relevant exceptions noted
	Restricts Access to Information Assets—Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules for information assets.	I) Inspected IT07 - Security Policy as the data classification policy and procedures (Sec 10.1, pg. 9). No issues were noted J) Inspected CC6.1j - spool_QPQUPRFIL_796000.txt as access control list of database administrators. No issues noted K) Inspected CC6.7.D.PNG as a screenshot of the current SSL certificate(s). No issues noted.	No relevant exceptions noted

	Manages Identification and Authentication—Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure, and software.	L) Inspected CC6.1.L.PNG as a screenshot of the operating system password policy. No issues noted M) Inspected CC6.1m - Policy - Security v4.1.pdf (Sec 9.3 pg. 7) as the most current password policy. No issues noted	No relevant exceptions noted
	Manages Credentials for Infrastructure and Software—New internal and external infrastructure and software users are registered, authorized, and documented before being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required, or the infrastructure and software are no longer in use.	N & O) Inspected the communication from HR to IT for network access and provide completed network access requests for a selection of new hires (CIC363, BRI661, MAH926, MAH 081, ADE161, MAU060, SPI178). No issues noted P, Q, & R) Inspected completed network access revocation requests and of network access accounts disabled or removed for a selection of terminated employees (CAR888, CAM291, TAY596, NGK397, DES397, GIL456, AHM346, VER570, ROC066, CHA299, BOU689). No issues noted	No relevant exceptions noted
	Uses Encryption to Protect Data—The entity uses encryption to supplement other measures used to protect data-at-rest when such protections are deemed appropriate based on assessed risk.	S) Inspected v2.2_CC6.1s_EncryptionScreenShot as a screenshot(s) of production database(s) encryption confirmation. No issues noted T) Inspected CC6.1T as a screenshot of local/hard drive encryption settings. No issues noted	No relevant exceptions noted
	Protects Encryption Keys—Processes are in place to protect encryption keys during generation, storage, use, and destruction.	U) Inspected CC6.1.U.PNG as evidence that encryption keys are stored and protected. No issues noted	No relevant exceptions noted
CC6.2 - Before issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			

CC6.2	Controls Access Credentials to Protected Assets—Information asset access credentials are created based on authorization from the system's asset owner or authorized custodian.	A & B) Inspected the communication from HR to IT for network access and provide completed network access requests for a selection of new hires (CIC363, BRI661, MAH926, MAH081, ADE161, MAU060, SPI178). No issues noted	No relevant exceptions noted
	Removes Access to Protected Assets When Appropriate—Processes are in place to remove credential access when an individual no longer requires such access.	C & D) Inspected completed network access revocation requests and network access accounts disabled or removed for a selection of terminated employees (CAR888, CAM291, TAY596, NGK397, DES397, GIL456, AHM346, VER570, ROC066, CHA299, BOU689). No issues noted	No relevant exceptions noted
	Reviews Appropriateness of Access Credentials—The appropriateness of access credentials is reviewed periodically for unnecessary and inappropriate individuals with credentials.	E) Inspected CC6.2e - CBV - Help Desk - ALL LOCATIONS - Internal Review - Monthly Elevated Privileges Checks (April 2022).pdf and CC6.2e - CBV - Help Desk - ALL LOCATIONS - Internal Review - Monthly Elevated Privileges Checks (March 2022).pdf as a sample (2) of completed network access rights reviews (e.g., quarterly access rights reviews). No issues noted	No relevant exceptions noted
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3	Creates or Modifies Access to Protected Information Assets—Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.	A & B) Inspected the communication from HR to IT for network access and provide completed network access requests for a selection of new hires (CIC363, BRI661, MAH926, MAH081, ADE161, MAU060, SPI178). No issues noted	No relevant exceptions noted
	Removes Access to Protected Information Assets—Processes are in place to remove access to protected information assets when an individual no longer requires access.	C & D) Inspected completed network access revocation requests and network access accounts disabled or removed for a selection of terminated employees (CAR888, CAM291, TAY596, NGK397, DES397, GIL456, AHM346, VER570, ROC066, CHA299, BOU689). No issues noted	No relevant exceptions noted

	Uses Role-Based Access Controls—Role-based access control is utilized to support the segregation of incompatible functions.	E) Inspected CC6.1 B as a screenshot of the operating system security groups. No issues noted	No relevant exceptions noted
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4	Creates or Modifies Physical Access—Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas, based on an authorization from the system's asset owner.	A) Inspected CC2.2a - Policy - Security v4.1.pdf as the most current physical security policy and procedures (pg. 4). No issues noted B) Inspected the completed physical access requests for a selection of new hires (CIC363, BRI661, MAH926, MAH081, ADE161, MAU060, SPI178). No issues noted	No relevant exceptions noted
	Removes Physical Access—Processes are in place to remove access to physical resources when an individual no longer requires access.	C) Inspected completed physical access revocation requests for a selection of terminated employees (CAR888, CAM291, TAY596, NGK397, DES397, GIL456, AHM346, VER570, ROC066, CHA299, BOU689). No issues noted	No relevant exceptions noted
	Reviews Physical Access—Processes are in place to periodically review physical access to ensure consistency with job responsibilities.	D) Inspected CC6.4 D - Physical access rights review.pdf and Access Review Ticket - 830268 - Jan 2022.pdf as a sample (2) of completed physical access rights reviews. No issues noted E) Inspected SOC2 CC6.4e access control list to the data center.jpg as the current access control list to the data center(s). No issues noted.	No relevant exceptions noted
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			

CC6.5	Identifies Data and Software for Disposal—Procedures are in place to identify data and software stored on equipment to be disposed of and to render such data and software unreadable.	A) Inspected CC3.3e - IT Policy - Data and Media Destruction v3.2.pdf as the most current policy and procedures for the disposal of assets or firmware. No issues noted	No relevant exceptions noted
	Removes Data and Software From Entity Control—Procedures are in place to remove data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable.	B) Inspected CC3.3e - IT Policy - Data and Media Destruction v3.2.pdf as the most current policy and procedures for the disposal of assets or firmware. No issues noted	No relevant exceptions noted
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6	Restricts Access—The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.	A) Inspected CC6.6.A.PNG as a screenshot of the firewall management console. No issues noted B) Inspected CC6.1.F.PNG and CC6.1.E.pdf as a screenshot of the firewall rules regulating access routes. No issues noted	No relevant exceptions noted
	Protects Identification and Authentication Credentials—Identification and authentication credentials are protected during transmission outside its system boundaries.	C) Inspected CC6.6.C.PNG as the screenshot of the VPN, TLS, or SSL authentication configuration(s). No issues noted.	No relevant exceptions noted
	Requires Additional Authentication or Credentials—Additional authentication information or credentials are required when accessing the system from outside its boundaries.	D) Inspected CC6.6.D.PNG as a screenshot or evidence of multi-factor authentication concerning accessing systems from outside boundaries. No issues noted	No relevant exceptions noted

	Implements Boundary Protection Systems—Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.	E) Inspected CC6.6.A.PNG as a screenshot of the firewall management console. No issues noted F) Inspected C6.1 E - System policy Sophos PC Block all.jpg and CC6.1.E.pdf as a screenshot of the DMZ configuration. No issues noted G) Inspected CC6.6.G.PNG as a screenshot of the IDS/IPS management interface. No issues noted H) Inspected CC6.6.H.msg as a sample of IDS/IPS notifications for pre-determined events or unauthorized access attempts. No issues noted	No relevant exceptions noted
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7	Restricts the Ability to Perform Transmission—Data loss prevention processes and technologies are used to restrict the ability to authorize and execute transmission, movement, and removal of information.	A) Inspected CC6.7.A.PNG as a screenshot of the data loss prevention (DLP) management interface. No issues noted	No relevant exceptions noted

	<u>Uses Encryption Technologies or Secure Communication Channels to Protect Data</u>—Encryption technologies or secured communication channels are used to protect the transmission of data and other communications beyond connectivity access points.	B) Inspected CC6.7.B-1.PNG and CC6.7.B-2.PNG as a screenshot of the remote access VPN encryption methodology. No issues noted C) Inspected CC6.7.C.PNG as a screenshot of the site-to-site (gateway) VPN encryption settings. No issues noted D) Inspected CC6.7.D.PNG as a screenshot of the current SSL certificate(s). No issues noted.	No relevant exceptions noted
	<u>Protects Removal Media</u>—Encryption technologies and physical asset protections are used for removable media (such as USB drives and backup tapes), as appropriate.	E) Inspected IT07 - Security Policy (Sec 8.3, pg. 6) as the most current policy concerning removable media. No issues noted F) Inspected C6.1 B System policy Block removable disks.jpg as a GPO configuration screenshot related to removable media status (disabled). No issues noted	No relevant exceptions noted
	<u>Protects Mobile Devices</u>—Processes are in place to protect mobile devices (such as laptops, smartphones, and tablets) that serve as information assets.	G) Inspected CC6.1T as a screenshot of local/hard drive encryption settings. No issues noted	No relevant exceptions noted
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8	<u>Restricts Application and Software Installation</u>—The ability to install applications and software is restricted to authorized individuals.	A) Inspected CC6.8 A (ACL) of personnel with elevated access to make system changes.pdf as the access control list (ACL) of personnel with elevated access to make system changes. No issues noted. B) Inspected CC3.3g - Policy - Acceptable Use v4.0.pdf as the most current acceptable use policy. No issues noted	No relevant exceptions noted
	<u>Detects Unauthorized Changes to Software and Configuration Parameters</u>—Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software.	C) Inspected CC7.1.D.msg as a sample of notifications sent, concerning the detection of unauthorized modifications of critical system files, configuration files, or content files. No issues noted	No relevant exceptions noted

	Uses a Defined Change Control Process—A management-defined change control process is used for the implementation of software.	D) Inspected Change Management Policy as the most current, documented change management policy and procedures. No issues noted	No relevant exceptions noted
	Uses Anti-virus and Anti-Malware Software—Anti-virus and anti-malware software is implemented and maintained to provide for the interception or detection and remediation of malware.	E) Inspected CC6.8 E Sophos Client on Domain server.jpg and CC6.8.E.PNG as a screenshot of the anti-virus client on the Domain server and the application database(s). No issues noted F) Inspected CC6.8f F - Antivirus update frequency - BBYSophos01.PNG as a screenshot of the polling interval for new definitions. No issues noted	No relevant exceptions noted
	Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software—Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected before its implementation on the network.	G) Inspected CC6.8G Sophos malware scanning evidence.jpg as evidence that malware scanning is in place for incoming communications or incoming file receipts. No issues noted	No relevant exceptions noted
CC7.0 - SYSTEM OPERATIONS			
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1	Uses Defined Configuration Standards—Management has defined configuration standards.	A) Inspected CC3.4g - IT Policy - Server and Security System Standards v3.9.pdf (Pg 6,7 & 9) as the most current, documented server build and hardening procedures. No issues noted B) Inspected CC7.1b PA Firewall Configuration Hardening Guidelines v2.pdf as the most current, documented firewall hardening procedures. No issues noted	No relevant exceptions noted

	Monitors Infrastructure and Software—The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.	C) Inspected CC4.1a - network server monitoring software management console.jpg as a screenshot of the network/ server monitoring software management console. No issues noted	No relevant exceptions noted
	Implements Change-Detection Mechanisms—The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.	D) Inspected CC7.1.D.msg as a sample of notifications sent, concerning the detection of unauthorized modifications of critical system files, configuration files, or content files. No issues noted	No relevant exceptions noted
	Detects Unknown or Unauthorized Components—Procedures are in place to detect the introduction of unknown or unauthorized components.	E) Inspected EXTERNAL bbypa01 - Daily Palo Alto Networks Reports for Saturday, Aug 27. msg as a sample of notifications sent, concerning the detection of unknown or unauthorized components. No issues noted	No relevant exceptions noted
	Conducts Vulnerability Scans—The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations periodically and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.	F) Inspected CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf and CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed. pdf as a sample of (2) third-party vulnerability assessments. No issues noted G) Inspected External Penetration Test.pdf and Internal Penetration Test.pdf as the most current penetration testing results. No issues noted	No relevant exceptions noted

CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2	Implements Detection Policies, Procedures, and Tools—Detection policies and procedures are defined and implemented, and detection tools are implemented on Infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include: (1) a defined governance process for security event detection and management that includes the provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; (3) logging of unusual system activities.	A) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted B) Inspected CC7.2b - IDS-IPS and Application and Threat Profile as a sample (3) of IDS/IPS notifications for pre-determined events or unauthorized access attempts. No issues noted C) Inspected CC7.2c - Siem.docx as a screenshot of the Syslog or SEIM utility interface. No issues noted	No relevant exceptions noted
	Designs Detection Measures—Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; (6) implementation or connection of unauthorized hardware and software.	D) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted E) Inspected CC7.2b - IDS-IPS and Application and Threat Profile as a sample (3) of IDS/IPS notifications for pre-determined events or unauthorized access attempts. No issues noted F) Inspected CC7.2c - Siem.docx as a screenshot of the Syslog or SEIM utility interface. No issues noted	No relevant exceptions noted

	<u>Implements Filters to Analyze Anomalies</u>—Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.	G) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted H) Inspected CC7.2h - Incidents.pdf and CC7.2h - ManageEngine ServiceDesk Plus.pdf as a screenshot of the infrastructure software ticketing system concerning logged security events. No issues noted	No relevant exceptions noted
	<u>Monitors Detection Tools for Effective Operation</u>—Management has implemented processes to monitor the effectiveness of detection tools.	I) Inspected CC7.2b - IDS-IPS and Application and Threat Profile as a sample (3) of IDS/IPS notifications for pre-determined events or unauthorized access attempts. No issues noted J) Inspected CC7.2c - Siem.docx as a screenshot of the Syslog or SEIM utility interface. No issues noted K) Inspected CC6.1.G.PNG as evidence that the firewall is configured to log certain events. No issues noted	No relevant exceptions noted
CC7.3 - The entity evaluates security events to determine whether they could or have failed the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3	<u>Responds to Security Incidents</u>—Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures periodically.	A) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted B) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted	No relevant exceptions noted

	Communicates and Reviews Detected Security Events—Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.	C) Inspected SecCom Minutes 20210712.pdf, SecCom Minutes 20220112.pdf, and SecCom Minutes 20220420.pdf as a sample (3) of risk assessment and security review meeting minutes. No issues noted	No relevant exceptions noted
	Develops and Implements Procedures to Analyze Security Incidents—Procedures are in place to analyze security incidents and determine system impact.	D) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted E) Inspected SecCom Minutes 20210712.pdf, SecCom Minutes 20220112.pdf, and SecCom Minutes 20220420.pdf as a sample (3) of risk assessment and security review meeting minutes. No issues noted F) Inspected CC7.3f - Incident - Closed.pdf as a sample of resolved incidents which includes root cause analysis, Corrective actions, and Preventative measures. No issues noted.	No relevant exceptions noted

CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

CC7.4	Assigns Roles and Responsibilities—Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary.	A) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted	No relevant exceptions noted
	Contains Security Incidents—Procedures are in place to contain security incidents that actively threaten entity objectives.	B) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted	No relevant exceptions noted

	Mitigates Ongoing Security Incidents—Procedures are in place to mitigate the effects of ongoing security incidents.	C) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted	No relevant exceptions noted
	Ends Threats Posed by Security Incidents—Procedures are in place to end the threats posed by security incidents through the closure of the vulnerability, removal of unauthorized access, and other remediation actions.	D) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted	No relevant exceptions noted
	Restores Operations—Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.	E) Inspected CC7.4.E.PNG as a screenshot of the backup system schedule(s). No issues noted F) Inspected CC7.4.F.PNG a sample of completed data restore request results. No issues noted	No relevant exceptions noted
	Develops and Implements Communication Protocols for Security Incidents—Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.	G) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted H) Inspected CC7.3f - Incident - Closed.pdf as a sample of resolved incidents which includes root cause analysis, Corrective actions, and Preventative measures. No issues noted.	No relevant exceptions noted
	Obtains Understanding of Nature of Incident and Determines Containment Strategy—An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.	I) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted J) Inspected CC7.3f - Incident - Closed.pdf as a sample of resolved incidents which includes root cause analysis, Corrective actions, and Preventative measures. No issues noted.	No relevant exceptions noted

	Remediates Identified Vulnerabilities—Identified vulnerabilities are remediated through the development and execution of remediation activities.	K) Inspected CC7.3f - Incident - Closed.pdf as a sample of resolved incidents which includes root cause analysis, Corrective actions, and Preventative measures. No issues noted.	No relevant exceptions noted
	Communicates Remediation Activities—Remediation activities are documented and communicated following the incident response program.	L) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted M) Inspected CC7.3f - Incident - Closed.pdf as a sample of resolved incidents which includes root cause analysis, Corrective actions, and Preventative measures. No issues noted.	No relevant exceptions noted
	Evaluates the Effectiveness of Incident Response—The design of incident response activities is evaluated for effectiveness periodically.	O) Inspected SecCom Minutes 20210712.pdf, SecCom Minutes 20220112.pdf, and SecCom Minutes 20220420.pdf as a sample (3) of risk assessment and security review meeting minutes. No issues noted	No relevant exceptions noted

	Periodically Evaluates Incidents—Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes.	P) Inspected SecCom Minutes 20210712.pdf, SecCom Minutes 20220112.pdf, and SecCom Minutes 20220420.pdf as a sample (3) of risk assessment and security review meeting minutes. No issues noted	No relevant exceptions noted
CC7.5 -The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5	Restores the Affected Environment—The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.	A) Inspected DR Run Book_Nov 2021.pdf, DR testing evidence_IT_20211119.pdf, and Letter of Attestation - Dec 2021.pdf as the most current disaster recovery testing results. No issues noted B) Inspected CC7.4.F.PNG a sample of completed data restore request results. No issues noted C) Inspected CC7.5C-1.PNG, CC7.5C-2.PNG, and CC7.5C-3.PNG as a sample (3) of installed patch updates OR a screenshot of installed patch logs. No issues noted	No relevant exceptions noted

	Communicates Information About the Event—Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate (internal and external).	D) Inspected CC7.3f - Incident - Closed.pdf as a sample of resolved incidents which includes root cause analysis, Corrective actions, and Preventative measures. No issues noted.	No relevant exceptions noted
	Determines Root Cause of the Event—The root cause of the event is determined.	E) Inspected CC7.3f - Incident - Closed.pdf as a sample of resolved incidents which includes root cause analysis, Corrective actions, and Preventative measures. No issues noted.	No relevant exceptions noted
	Implements Changes to Prevent and Detect Recurrences—Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.	F) Inspected CC7.3f - Incident - Closed.pdf as a sample of resolved incidents which includes root cause analysis, Corrective actions, and Preventative measures. No issues noted.	No relevant exceptions noted
	Improves Response and Recovery Procedures—Lessons learned are analyzed, and the incident response plan and recovery procedures are improved.	G) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted H) Inspected SecCom Minutes 20210712.pdf, SecCom Minutes 20220112.pdf, and SecCom Minutes 20220420.pdf as a sample (3) of risk assessment and security review meeting minutes. No issues noted	No relevant exceptions noted

	Implements Incident Recovery Plan Testing—Incident recovery plan testing is performed periodically. The testing includes : (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; (4) revision of continuity plans and systems based on test results.	I) Inspected DR Run Book_Nov 2021.pdf, DR testing evidence_IT_20211119.pdf, and Letter of Attestation - Dec 2021.pdf as the most current disaster recovery testing results. No issues noted J) Inspected CC1.4j - SOP - Business Continuity Plan v5.9.pdf as the most current business continuity plan. No issues noted	No relevant exceptions noted
CC8.0 - CHANGE MANAGEMENT			
CC8.1 -The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1	Manages Changes Throughout the System Lifecycle—A process for managing system changes throughout the lifecycle of the system and its components (infrastructure, data, software, and procedures) is used to support system availability and processing integrity.	A) Inspected CC8.1a - SOP - Software Development Lifecycle v3.4.pdf as the most current software development lifecycle (SDLC) policy and procedures. No issues noted. B) Inspected Change Management Policy as the most current, documented change management policy and procedures. No issues noted	No relevant exceptions noted

	Authorizes Changes—A process is in place to authorize system changes before development.	C) Inspected M0677 Account Inquiry Screen Coll Code Region Change Enable per user control, M0679 AutoTrak process remove [ESTed] and VG106 ETL Standard file process (Phase 2) as a sample (3) of completed software development change requests, show the lifecycle of the change request concerning documented authorization before development. No issues noted D) Inspected CC4.2E infrastructure change ticketing system.pdf, CC4.2E infrastructure change ticketing system_ (2).pdf and CC4.2E infrastructure change ticketing system_.pdf as a sample (3) of completed deficiency tickets (change requests). No issues noted	No relevant exceptions noted
	Designs and Develops Changes—A process is in place to design and develop system changes.	E) Inspected M0677 Account Inquiry Screen Coll Code Region Change Enable per user control, M0679 AutoTrak process remove [ESTed] and VG106 ETL Standard file process (Phase 2) as a sample (3) of completed software development change requests, show the lifecycle of the change request concerning documented authorization before development. No issues noted F) Inspected CC4.2E infrastructure change ticketing system.pdf, CC4.2E infrastructure change ticketing system_ (2).pdf and CC4.2E infrastructure change ticketing system_.pdf as a sample (3) of completed deficiency tickets (change requests). No issues noted	No relevant exceptions noted

	Documents Changes—A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.	G) Inspected CC4.2C infrastructure change ticketing system--.jpg, CC4.2C infrastructure change ticketing system.pdf, and CC4.2C infrastructure change ticketing system_.pdf as a screenshot of the infrastructure change ticketing system. No issues noted H) Inspected CC4.2d - software development ticketing system.jpg as a screenshot of the software development ticketing system. No issues noted	No relevant exceptions noted
	Tracks System Changes—A process is in place to track system changes before implementation.	I) Inspected CC4.2C infrastructure change ticketing system--.jpg, CC4.2C infrastructure change ticketing system.pdf, and CC4.2C infrastructure change ticketing system_.pdf as a screenshot of the infrastructure change ticketing system. No issues noted J) Inspected CC4.2d - software development ticketing system.jpg as a screenshot of the software development ticketing system. No issues noted	No relevant exceptions noted
	Configures Software—A process is in place to select and implement the configuration parameters used to control the functionality of the software.	K) Inspected CC4.2C infrastructure change ticketing system--.jpg, CC4.2C infrastructure change ticketing system.pdf, and CC4.2C infrastructure change ticketing system_.pdf as a screenshot of the infrastructure change ticketing system. No issues noted L) Inspected CC4.2E infrastructure change ticketing system.pdf, CC4.2E infrastructure change ticketing system_ (2).pdf and CC4.2E infrastructure change ticketing system_.pdf as a sample (3) of completed deficiency tickets (change requests). No issues noted	No relevant exceptions noted

	Tests System Changes—A process is in place to test system changes before implementation.	M) Inspected M0677 Account Inquiry Screen Coll Code Region Change Enable per user control, M0679 AutoTrak process remove [ESTed] and VG106 ETL Standard file process (Phase 2) as a sample (3) of completed software development change requests, show the lifecycle of the change request concerning documented authorization before development. No issues noted N) Inspected CC4.2E infrastructure change ticketing system.pdf, CC4.2E infrastructure change ticketing system_ (2).pdf and CC4.2E infrastructure change ticketing system_.pdf as a sample (3) of completed deficiency tickets (change requests). No issues noted	No relevant exceptions noted
	Approves System Changes—A process is in place to approve system changes before implementation.	O) Inspected M0677 Account Inquiry Screen Coll Code Region Change Enable per user control, M0679 AutoTrak process remove [ESTed] and VG106 ETL Standard file process (Phase 2) as a sample (3) of completed software development change requests, show the lifecycle of the change request concerning documented authorization before development. No issues noted P) Inspected CC4.2E infrastructure change ticketing system.pdf, CC4.2E infrastructure change ticketing system_ (2).pdf and CC4.2E infrastructure change ticketing system_.pdf as a sample (3) of completed deficiency tickets (change requests). No issues noted	No relevant exceptions noted

	Deploys System Changes—A process is in place to implement system changes.	Q) Inspected IT projects installation - Dec 2nd - VG106i.msg, IT projects installation - Mar 29, 2022 - VG106k & VG219 & M0679.msg and RE IT projects installation - Mar 25, 2022 - VG219 & M0677.msg as the project tracking mechanism for deployment notifications to affected parties. No issues noted	No relevant exceptions noted
	Identifies and Evaluates System Changes—Objectives affected by system changes are identified, and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle.	R) Inspected M0677 Account Inquiry Screen Coll Code Region Change Enable per user control, M0679 AutoTrak process remove [ESTed] and VG106 ETL Standard file process (Phase 2) as a sample (3) of completed software development change requests, show the lifecycle of the change request concerning documented authorization before development. No issues noted S) Inspected CC4.2E infrastructure change ticketing system.pdf, CC4.2E infrastructure change ticketing system_ (2).pdf and CC4.2E infrastructure change ticketing system_.pdf as a sample (3) of completed deficiency tickets (change requests). No issues noted	No relevant exceptions noted
	Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents—Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified, and the change process is initiated upon identification.	T) As inquired, CC8.1t - Incident.pdf required immediate remediation. No issues noted U) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted	No relevant exceptions noted

	Creates Baseline Configuration of IT Technology—A baseline configuration of IT and control systems is created and maintained.	V) Inspected CC8.1a - SOP - Software Development Lifecycle v3.4.pdf as the most current software development lifecycle (SDLC) policy and procedures. No issues noted. W) Inspected Change Management Policy as the most current, documented change management policy and procedures. No issues noted X) Inspected CC3.4g - IT Policy - Server and Security System Standards v3.9.pdf (Pg 6,7 & 9) as the most current, documented server build and hardening procedures. No issues noted Y) Inspected CC7.1b PA Firewall Configuration Hardening Guidelines v2.pdf as the most current, documented firewall hardening procedures. No issues noted	No relevant exceptions noted

	Provides for Changes Necessary in Emergency Situations —A process is in place for authorizing, designing, testing, approving, and implementing changes necessary in emergencies (that is, changes that need to be implemented in an urgent timeframe).	Z) As inquired Emergency Change Process is not different than the normal change Process. If there needs to be an emergency change, it still goes through the same approval process. Inspected Change Management Policy as the most current, documented change management policy and procedures. No issues noted	No relevant exceptions noted
CC9.0 - RISK MITIGATION			
CC9.1 -The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1	Considers Mitigation of Risks of Business Disruption—Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the entity's objectives during the response, mitigation, and recovery efforts._	A) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted B) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted	No relevant exceptions noted
	Considers the Use of Insurance to Mitigate Financial Impact Risks—The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.	C) Inspected CC9.1c - 29. Generic COI (To whom so ever it may concern).pdf as the most current insurance declaration pages. No issues noted	No relevant exceptions noted

CC9.2 -The entity assesses and manages risks associated with vendors and business partners.			
CC9.2	Establishes Requirements for Vendor and Business Partner Engagements—The entity establishes specific requirements for a vendor and business partner engagement that includes: (1) scope of services and product specifications (2) roles and responsibilities, (3) compliance requirements, (4) service levels.	A) Inspected CC1.1e - ARC - COLLECTION AGENCY AGREEMENT.pdf, CC1.1e - Provana Master Solution Agmt - CBV Collection Services 062421.pdf and CC1.1e Sample Contract Templates as a sample (2) of executed service agreements for vendors used in the scope of this engagement. No issues noted	No relevant exceptions noted
	Assesses Vendor and Business Partner Risks—The entity assesses, periodically, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives._	B) Inspected CC1.1e - ARC - COLLECTION AGENCY AGREEMENT.pdf, CC1.1e - Provana Master Solution Agmt - CBV Collection Services 062421.pdf and CC1.1e Sample Contract Templates as a sample (2) of executed service agreements for vendors used in the scope of this engagement. No issues noted	No relevant exceptions noted
	Assigns Responsibility and Accountability for Managing Vendors and Business Partners—The entity assigns responsibility and accountability for the management of risks associated with vendors and business partners.	C) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted	No relevant exceptions noted
	Establishes Communication Protocols for Vendors and Business Partners—The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners.	D) Inspected CC1.4e - CS Policy - Vendor Management v3.8.pdf as the most recent vendor management policy and procedures. No issues noted	No relevant exceptions noted
	Establishes Exception Handling Procedures from Vendors and Business Partners —The entity establishes exception-handling procedures for service or product issues related to vendors and business partners.	E) Inspected CC2.2b - Policy - Incident Response v3.10.pdf as the most current incident response policy and procedures. No issues noted	No relevant exceptions noted

	Assesses Vendor and Business Partner Performance—The entity periodically assesses the performance of vendors and business partners.	F) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted G) Inspected CC3.2a - Policy - Risk Management v3.6.pdf and CC3.3b - SOP - Internal Audit v1.3.pdf as the most current internal audit program. No issues noted	No relevant exceptions noted
	Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments—The entity implements procedures for addressing issues identified with vendor and business partner relationships.	H) Inspected CC1.4e - CS Policy - Vendor Management v3.8.pdf as the most recent vendor management policy and procedures. No issues noted	No relevant exceptions noted
	Implements Procedures for Terminating Vendor and Business Partner Relationships — The entity implements procedures for terminating vendor and business partner relationships.	I) Inspected CC1.4e - CS Policy - Vendor Management v3.8.pdf as the most recent vendor management policy and procedures. No issues noted	No relevant exceptions noted

A1.0 - Additional Criteria for Availability

A1.1 -The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

A1.1	Measures Current Usage—The use of the system components are measured to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.	A) Inspected CC4.1a - network server monitoring software management console.jpg as a screenshot of the network/ server monitoring software management console. No issues noted B) Inspected A1.1.B.msg as a sample of capacity forecasting. No issues noted	No relevant exceptions noted

	Forecasts Capacity—The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity.	C) Inspected A1.1.B.msg as a sample of capacity forecasting. No issues noted	No relevant exceptions noted
	Makes Changes Based on Forecasts—The system change management process is initiated when forecasted usage exceeds capacity tolerances.	D) Inspected CC4.1a - network server monitoring software management console.jpg as a screenshot of the network/ server monitoring software management console. No issues noted E) Inspected A1.1.B.msg as a sample of capacity forecasting. No issues noted	No relevant exceptions noted
A1.2 -The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			
A1.2	Identifies Environmental Threats—As part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.	A) Inspected CC3.1h - PCI_DSS_v3-2-1_AOC_SAQ_D_CBV_2022[FINAL]_Signed.pdf, CC3.1g3 - CBV FINAL SOC 2 Type 2 Report - 063021.pdf, CBV_DMZ_June2022.csv, CBV_External_June2022.csv, CBV_Noblestats_June2022.csv, External Penetration Test.pdf, Internal Penetration Test.pdf, CBV_Websites_June2022.csv as the most current Risk Assessment (RA). No issues noted	No relevant exceptions noted

	Designs Detection Measures—Detection measures are implemented to identify anomalies that could result from environmental threat events.	B) Inspected A1.2B Temperature and humidity control.JPG, A1.2B Backup HVAC.JPG, A1.2B fire suppression system.JPG, A1.2B fire suppression system_.JPG, A1.2B main HVAC.JPG, A1.2B Temperature and humidity control(main HVAC).JPG, A1.2B Temperature, and humidity control.JPG, A1.2B Temperature and humidity control__.JPG, A1.2B Temperature and humidity control___.JPG and A1.2B Temperature and humidity control Switch room.JPG as evidence of HVAC protection systems, fire suppression systems, environmental monitoring and temperature, and humidity controls. No issues noted	No relevant exceptions noted
	Implements and Maintains Environmental Protection Mechanisms— Management implements and maintains environmental protection mechanisms to prevent and mitigate environmental events.	C) Inspected A1.2B Temperature and humidity control.JPG, A1.2B Backup HVAC.JPG, A1.2B fire suppression system.JPG, A1.2B fire suppression system_.JPG, A1.2B main HVAC.JPG, A1.2B Temperature and humidity control(main HVAC).JPG, A1.2B Temperature, and humidity control.JPG, A1.2B Temperature and humidity control__.JPG, A1.2B Temperature and humidity control___.JPG and A1.2B Temperature and humidity control Switch room.JPG as evidence of HVAC protection systems, fire suppression systems, environmental monitoring and temperature, and humidity controls. No issues noted	No relevant exceptions noted
	Implements Alert to Analyze Anomalies—Management implements alerts that are communicated to personnel for analysis to identify environmental threat events.	D) Inspected Ticket 819643.pdf, Ticket 822621.pdf, and Ticket 825479.pdf as a sample of environmental monitoring notifications. No issues noted	No relevant exceptions noted

	Responds to Environmental Threat Events—Procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures periodically. This includes automatic mitigation systems (for example, an uninterruptable power system and generator backup subsystem).	E) Inspected A1.2e - Narrative - Physical Security v2.0.pdf as the most current environment protection policy and procedures. NO issues noted F) Inspected A1.2F UPS System Switch room _.JPG, A1.2F UPS System Switch Room.JPG, A1.2F UPS System.JPG, A1.2F UPS System_.JPG, and A1.2F UPS System____.JPG as evidence of UPS systems and generator backup systems. Inspected Ticket 819643.pdf, Ticket 822621.pdf, and Ticket 825479.pdf as a sample of environmental monitoring notifications. No issues noted	No relevant exceptions noted
	Communicates and Reviews Detected Environmental Threat Events—Detected environmental threat events are communicated to and reviewed by the individuals responsible for the management of the system, and actions are taken, if necessary.	G) Inspected Ticket 819643.pdf, Ticket 822621.pdf, and Ticket 825479.pdf as a sample of environmental monitoring notifications. No issues noted	No relevant exceptions noted
	Determines Data Requiring Backup—Data is evaluated to determine whether the backup is required.	H) Inspected A1.2h - Narrative - AS400 Backup v1.5.pdf as the backup and restore policy and procedures. No issues noted	No relevant exceptions noted
	Performs Data Backup—Procedures are in place for backing up data, monitoring to detect backup failures, and initiating corrective action when such failures occur.	I) Inspected CC7.4.E.PNG as a screenshot of the backup system schedule(s). No issues noted J) Inspected CC7.4.F.PNG a sample of completed data restore request results. No issues noted	No relevant exceptions noted
	Addresses Offsite Storage—Back-up data is stored in a location at a distance from its principal storage location sufficient that the likelihood of a security or environmental threat event affecting both sets of data is reduced to an appropriate level.	K) Inspected A1.2.K.PNG as the screenshots of completed backup data exports to external storage. No issues noted	No relevant exceptions noted

	Implements Alternate Processing Infrastructure—Measures are implemented for migrating processing to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	L) Inspected DR Run Book_Nov 2021.pdf, DR testing evidence_IT_20211119.pdf, Letter of Attestation - Dec 2021.pdf, and Business Continuity Plan as evidence of a functioning disaster recovery site. No issues noted	No relevant exceptions noted
A1.3 -The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3	Implements Business Continuity Plan Testing—Business continuity plan testing is performed periodically. The testing includes: (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; (4) revision of continuity plans and systems based on test results.	A) Inspected CC1.4j - SOP - Business Continuity Plan v5.9.pdf as the most current business continuity plan. No issues noted	No relevant exceptions noted
	Tests Integrity and Completeness of Back-Up Data—The integrity and completeness of backup information are tested periodically.	B) Inspected CC7.4.F.PNG a sample of completed data restore request results. No issues noted	No relevant exceptions noted