Report on a Description of a Service Organization and the Suitability of the Design and Operating Effectiveness of Controls October 1, 2020 through March 31, 2021

CorKat Data Solutions, LLC
infinitepossibilities

AICPA Service Organization Control Reporting
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports

SECURITY & CONTROL LLC
Accounting – Technology - Advisory

Table of Contents

Section 1

Independent Service Auditors' Report

SECURITY & CONTROL LLC
Accounting – Technology - Advisory

Security and Control LLC
2556 Yosemite Street
303.981.9466 | securityandcontrol.com

Independent Service Auditor's Report

To the Management of CorKat Data Solutions LLC:

Scope

We have examined CorKat Data Solutions, LLC (herein referred to as "CORKAT") description of its information technology system entitled "Description of CORKAT's Information Technology System" for processing user entities transactions throughout the period October 1, 2020 to March 31, 2021 (description) and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "CORKAT's Management Assertion" (assertion). The controls and control objectives included in the description are those that management of CORKAT believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the CORKAT Information Technology System that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of CORKAT's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complimentary user entity controls.

CORKAT's responsibilities

In section 2, CORKAT has provided an assertion about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. CORKAT is responsible for preparing the description and its assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives 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, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period from October 1, 2020 to March 31, 2021. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion

- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.

- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.

- evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and suitability of the criteria specified by CORKAT in its assertion.

Inherent limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user-entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in CORKAT's assertion,

a. the description fairly presents CORKAT's Information Technology System that was designed and implemented throughout the period October 1, 2020 to March 31, 2021.

b. the controls related to the control objectives of CORKAT stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2020 to March 31, 2021, and user entities applied the complementary user entity controls assumed in the design of CORKAT's Information Technology System controls throughout the period October 1, 2020 to March 31, 2021.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2020 to March 31, 2021, if complementary user entity controls assumed in the design of CORKAT's controls operated effectively throughout the period October 1, 2020 to March 31, 2021.

Restricted use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of CORKAT, user entities of CORKAT's Information Technology System during some or all of the period October 1, 2020 to March 31, 2021, and their auditors who audit and report on such user entities financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the user entities themselves, when assessing the risks of material misstatement of user entities financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Security and Control LLC

Denver, CO
April 16, 2021

section 2

Service Organization's Assertion

P.O. Box 7451
Loveland, CO 80537
www.corkatdata.com

CorKat Data Solutions LLC
infinitepossibilities

Office: (970) 776-3777
Fax: (970) 776-1869
info@corkatdata.com

April 16, 2021

CorKat's Management Assertion:

We have prepared the description of CorKat Data Solutions LLC (CORKAT) Information Technology System entitled "Description of CORKAT's Information Technology System" for processing user entities' transactions throughout the period October 1, 2020 to March 31, 2021 (description) for user entities of the system during some or all of the period October 1, 2020 to March 31, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risk of material misstatement of user entities' financial statements.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of CORKAT's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of such user entities.

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

a. the description fairly presents CORKAT's Information Technology System made available to user entities of the system during some or all of the period October 1, 2020 to March 31, 2021, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description

   i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including if applicable,

      (1) the types of services provided, including, as appropriate, the classes of transactions processed.

      (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

      (3) The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

P.O. Box 7451
Loveland, CO 80537
www.corkatdata.com

CorKat Data Solutions LLC
infinitepossibilities

Office: (970) 776-3777
Fax: (970) 776-1869
info@corkatdata.com

(4) how the system captures and addresses significant events and conditions other than transactions.

(5) the process used to prepare reports and other information for user entities.

(6) services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.

(7) the specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the service organizations controls.

(8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. includes relevant details of changes to CORKAT's system during the period covered by the description.

iii. does not omit or distort information relevant to CORKAT's Information Technology System, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditor, and may not, therefore, include every aspect of the CORKAT Information Technology System that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period October 1, 2020 to March 31, 2021, to achieve those control objectives if the subservice organization and user entities applied the complementary controls assumed in the design of CORKAT's Information Technology System controls throughout the period October 1, 2020 to March 31, 2021. The criteria we used in making this assertion were that

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization;

ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

section 3

Description of Controls Provided by CorKat

3 Description of Controls Provided by CorKat

Scope of this Report

This report describes CorKat Data Solutions LLC ("CorKat's") information technology system applicable to users of CorKat's information technology services.

Most of the management operations and controls including, human resources, risk management, and policy, are shared between both entities which have common ownership.

This report is intended to provide CorKat's customers and their independent auditors with information about the information technology general controls related to the information technology processing platform at CorKat.

This report was developed to include the controls relevant to those customers who have subscribed to the specific services identified in this report. Any unique customer deployments, including those customers who have not contracted for various services or those who have implemented services which are not in accordance with the controls identified in this report, are outside the scope of this report.

The Tuscon, AZ colocation facility used by CorKat for remote backup is not included within this Description of Controls.

Criteria Used to Describe our Services

CorKat management has identified, discussed, reviewed, and documented the *Description of Controls Provided by CorKat* using the following criteria as guidance:

- we described our procedures, for both automated and manual systems, which provide our services,
- we described any applicable information technology general controls, automated and manual, which support reporting, reconciliation, monitoring, and processing of user entity transactions,
- we described methods by which our system captures and addresses significant events and conditions other than application transactions,
- we described our processes used to prepare reports, automated and manual, and other communication for user entities,
- we described the control objectives and control activities designed to achieve those objectives, including complementary user entity controls (discussed separately at the end of this Section),

- we described other aspects of our control environment, risk assessment process, information and communication, control activities, and monitoring which demonstrate our tone-at-the-top and entity-level controls,
- we described, as applicable, any changes to our controls during the period covered by our description,
- we confirmed consistent application of our controls as designed throughout the period of our description, including manual procedures and controls applied by staff having the appropriate competence and authority to do so.

Overview of CorKat Services

CorKat, is a Loveland, Colorado based privately held IT colocation, managed and infrastructure services provider, established in 2011 to provide cloud-based customers throughout the Rocky Mountain Region and national small to medium sized businesses. CorKat provides IaaS, PaaS, DRaaS, and colocation services for more than 244 customers. CorKat currently has sixteen (16) full time employees, including the CEO.

CorKat, which was established in 2004, are co-located in adjoining facility space, in downtown Loveland, Colorado.

The following provides an overview of CorKat's services:

- **Infrastructure as a Service (IaaS)** including network, hardware, and operating infrastructure management (hypervisor, networks),
- **Platform as a Service (PaaS),** including Managed Hosting (hardware, operating systems, patch management, monitoring), Managed Network (routers, switches, wireless), Managed Storage (local, remote storage), and Managed Security Services (scanning, logging, firewall/IDS, multi-factor authentication), and
- **Disaster Recovery as a Service (DRaaS)** (backup, storage, remote disaster replication), and
- **Colocation services** included physical and environmental data center management.

CorKat's Technology Environment

Information Technology Infrastructure

The following includes a sample of the technologies supported by CorKat:

- Juniper and Cisco network devices,
- Dell servers,
- Sophos antivirus,
- Kiwi and Solar Winds logging,
- VMWare virtual hypervisor,

- Microsoft Server, SQL, IIS,
- Desktop Windows and office automation,
- Spectrum Construction Management and Sage Timberline Financial Accounting applications, and
- CorKat Data Solutions data center (Loveland, CO).

CorKat's data center physical and environmental protection features include:

- Electronic access control systems,
- Closed circuit television systems (CCTV),
- 24x7 onsite security force,
- Automated fire detection,
- Redundant telecommunications, power, water, computer room air conditioning (CRAC) and utility systems, and
- Fortress-designed building.

Relevant Aspects of Control Environment, Risk Assessment, and Monitoring

Business operations are under the direction of the CEO. The Company is supported by the following functional areas:

- Information Technology
- Administration
- Customer Service
- Data Center Operations

Control Environment

Integrity and Ethical Values

The Company has developed an employee handbook, which includes policies that address acceptable business practices, conflicts of interest, and expected standards of ethical behavior. These policies are provided to all new employees and are available on the intranet. Management has a formal hiring and training process for all new employees. There is an established "tone at the top," including hands-on management involvement and continuous communication with staff regarding the organization's responsibility to uphold the highest levels of integrity for both company and customer affairs. This tone is communicated and practiced by management throughout the organization. The importance of high ethics and controls is discussed with newly hired employees during orientation.

The Company requires each employee to sign an acknowledgement of their responsibilities for IT security and customer data protection.

Management Controls

Company management understands and exercises responsibility related to internal control. Company management meet informally almost daily and formally on an annual basis and are involved in all significant business decisions. The Company also utilizes an external accountant and an attorney who support annual filings and provide accounting, tax, and legal advice.

Management team members, which report to the chief executive meet formally on a routine basis, works in close proximity and meet informally daily.

Management's Philosophy and Operating Style

The Company holds regular meetings which enable senior management to maintain contact with and consistently emphasize appropriate behavior to operating personnel. During these meetings, management demonstrates attitudes and actions reflecting a sound control environment and commitment to ethical values.

Organizational Structure

The Company has established appropriate lines of reporting, which facilitate the flow of information to appropriate people in a timely manner. The lines of reporting are communicated to employees through the organization chart, which is updated periodically. Roles and responsibilities are appropriately segregated based on functional requirements. Separation of duties exists and is outlined in employee job descriptions.

Authority and Responsibility

Job descriptions, which formally assign authority and responsibility, are provided to all Company employees. Job descriptions contain references to control-related responsibilities, as applicable. The Information Security Program establishes management's responsibility for all aspects of information security and authorizes management to delegate responsibilities to the Information Security Officer (ISO). The Information Security Program is reviewed and approved annually by management.

All significant agreements and contracts are reviewed and approved by management prior to being executed.

Human Resources

Management has established human resource practices that demonstrate its commitment to integrity, ethical behavior, and competence. All positions have written job descriptions including education and experience requirements. Management reviews compensation of all senior staff to ensure that pay is commensurate with responsibilities.

The Company has formal hiring practice designed to ensure that each new employee is qualified for the specific job responsibilities. Hiring policies include minimum education and experience requirements, background checks, reference checks, and the execution of confidentiality statements.

Employees are evaluated annually on their job performance and fulfillment of company objectives and expectations by their supervisors and by the management team.

Risk Assessment

The Company have a risk assessment process designed to identify and manage risks that could affect their ability to provide reliable processing for user organizations. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks.

The risk assessment methodology includes the periodic production of risk assessment reports which contain the following:

- An inventory of critical technology,
- Documented changes in the technology or operating environment,
- Ongoing system monitoring of controls to safeguard against the identified threats/vulnerabilities and the resulting risk levels, and
- A formal insurance program.

Monitoring

Management personnel monitor the quality of internal control performance as a routine part of their activities. Management, together with external contract auditors, assessors, and consultants perform ongoing audit functions to ensure the system of controls are continuously enforced and regularly reviewed.

The Company performs routine reviews of network, server and infrastructure availability, problem ticket resolution, and open items to determine whether services are continuously provided in a consistent, high-availability state.

Information Systems and Communication

The Company has implemented various methods of communication to ensure that all employees understand their individual roles and responsibilities regarding customer services and controls and to ensure that significant events are communicated in a timely manner. These methods include formal job descriptions, orientation for newly hired

employees, a company intranet, weekly forums and the use of electronic mail messages to communicate time-sensitive messages and information. The intranet provides access to company announcements, policies and procedures, and management emails.

The Company has also implemented various methods of communication to ensure that user organizations understand the role and responsibilities with respect to customer service and to ensure that significant events are communicated to users in a timely manner. These methods include use of formal contracts that address the scope of services to be provided and the responsibilities under the contracts.

The Company provides a test environment for customers that are contracting for services. Customer Support staff are responsible for maintaining customer relationships and communicating pertinent matters to customers. Customers are also encouraged to communicate questions and problems to the Companies. Such matters are logged and tracked until resolved.

Control Objectives and Related Controls

The Company's control objectives and related controls are included in Section 4 of this report, *Independent Service Auditors' Description of Tests of Controls and Results* to eliminate redundancy. Controls are presented in Section 4, in the leftmost column titled, "Controls Specified by CorKat."

The following provides a summary of the control activities designed and implemented by the Company for their information technology general controls (ITGC) environment.

(1) IT Management, Organization and Oversight Controls |

The management team takes an active and continuous role in the monitoring of daily activities, including customer service, technology processing, and staff management and oversight. The entity is organized around both customer-facing and internal support functions which are segregated to support of internal control objectives, including Operations, Administration, Customer Service, and Technology.

The management team are in continuous communication with each other and staff members. Management attends conferences and continuing education in their respective fields to ensure currency and timeliness of regulatory and industry changes, and the results are communicated to the entire enterprise.

The Company has developed a formal human resource program for recruitment, onboarding, retention, and separation of employees. Human resources oversees annual security training performance reviews and ongoing staff compliance and maintains the enterprise HR Handbook.

The Company has formally documented policies, procedures and in many cases business practices to provide instruction and facilitate efficient and error-free

processing. An information security officer (ISO) has been appointed who reports to the management team.

The Company has a risk management program which continuously monitors and evaluates business and technology risks, includes insurance protection and provides backup strategies and procedures in the event of a business disruption.

(2) Logical Access and Security Controls |

The Company has deployed a multi-layer logical access and security control environment which includes access controls at the host, application, network, and remote access layers.

The Company has deployed authentication controls for network and systems logical access, and logs all security-related events. Logical security enforces need-to-know, need-to-access authentication, authorization, and accounting measures for critical technologies.

Access to internal systems, including administrative and supervisory access to operating and database systems is restricted to a minimum number of IT staff.

The Company has deployed extensive security and operational IT monitoring, logging and reporting systems designed to ensure timely notification of inappropriate or abnormal system activity.

Server and network devices are hardened before deployment and monitored to ensure routine patches are deployed in a timely manner.

(3) Network Security Controls |

The Company has deployed a defense-in-depth network security architecture which includes the use of stateful firewalls, system and network monitoring, antivirus, and real-time logging and accounting.

The Company utilizes secure (encrypted) data transmission techniques when transmitting sensitive information across public networks.

The Company has deployed an enterprise-wide antivirus and malicious software program.

Remote access is multi-layered and limited based on a need-to-have approach and is restricted to the minimum number of IT staff whose job functions require remote login.

(4) Computer Operations Controls |

The Company has documented policies, procedures and practices for computer operations, system and network monitoring, data backups and business continuity, and problem management.

Network and system monitoring tools have been deployed to monitor real-time events and provide alerts to critical technology (including on call) support staff.

The Company has a formal backup and recovery program which includes hourly full volume snapshots and backups of data to an alternate location.

(5) System Development and Change Management Controls |

The Company has developed a formal system development life cycle (SDLC) policy combined with a change control policy which guides all development and deployment of infrastructure (servers, network devices, etc.) and applications, both customer-facing and internal.

All changes are documented, tested and approved before deployment – through duties properly segregated among staff.

The Company maintains segregated development, test and production technology environments.

(6) Physical and Environmental Protection Controls |

The Company has documented policies, procedures and practices for data center physical security including access controls, perimeter protection, visitor controls and monitoring.

Supplemental power has been deployed to ensure consistent and reliable power supply in the event of a power disruption.

Automated fire detection and alarm systems have been deployed to protect against fire hazards.

Changes in Controls

There have been no significant changes to our information technology general control environment during the period covered by our description.

Application of our Controls

Management meets frequently to discuss business, technology, customer, and control items of interest. Management monitors the application of our controls to achieve our desired results of effectiveness and efficiency and to ensure our controls were consistently applied as designed throughout the period of our description, including ensuring whether any controls, manual or automated, were applied or accessed, by individuals who have the appropriate competence and authority to do so.

User Entity Control Considerations

The Company's information technology general controls were designed with the assumption that certain controls would be implemented by user organizations. 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 the following controls have been placed in operation at user organizations:

- Controls to provide reasonable assurance that changes to user processing options (parameters) are appropriately authorized, approved, and implemented.
- Controls to provide reasonable assurance that user transactions are appropriately authorized, complete, and accurate prior to submission to the company.
- Controls to provide reasonable assurance that user erroneous input data are corrected and resubmitted.
- Controls to provide reasonable assurance that user output reports are reviewed by appropriate individuals for completeness and accuracy.
- Controls to provide reasonable assurance that user output received from the Company is routinely reconciled to relevant user organization control totals.
- Controls over user operating system, utilities, database management systems, application-level security, features, and functions, including authentication, authorization, and accounting (logs) – which are not provided under the Company's services offering.
- User specific controls which are not provided under a managed service contract offering with the Company.

The list of user-organization control considerations presented above does not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations.

section 4

Independent Service Auditor's Description of Tests of Controls and Results

4 Independent Service Auditor's Description of Tests of Controls and Results

4.1 Tests of Operating Effectiveness

Our tests of the effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period from October 1, 2020 to March 31, 2021. Our tests of the operational effectiveness of controls were designed to cover key control activities throughout the period of October 1, 2020 to March 31, 2021, for each of the controls listed in section 4, including the controls specified by CorKat, which are designed to achieve specific control objectives, also listed in section 4. In selecting a particular test of the operational effectiveness of controls, we considered the nature of the items being tested, the types and competence of available evidential matter, the nature of the audit objectives to be achieved, the assessed level of control risk, and the expected efficiency and effectiveness of the test. Our testing of controls did not include the Tuscon, AZ colocation facility utilized for CorKat backups.

4.2 Description of Testing Procedures Performed

Tests performed of the operational effectiveness of controls are described in general below and in more detail on the following pages:

Corroborative Inquiry: Conducted inquiries of appropriate personnel and corroborated responses with other personnel to ascertain the compliance of controls.

Observation: Observed application of specific controls, including online systems observation of system state, parameters, logs and program settings, and performed online observation walk-throughs (console reviews) of selected security and control processes.

Inspection: Inspected documentation, logs, system security settings, system states, configurations, and reports, indicating performance of the controls.

Reperformance: Reperformed specific control activities.

4.3 Control Objectives, Related Controls and Tests of Operating Effectiveness

IT MANAGEMENT, ORGANIZATION, AND OVERSIGHT CONTROLS
Control Objective 1.0

Controls provide reasonable assurance that information technology (IT) management, organization and oversight policies are documented and operating in accordance with management's intended purpose.

Controls Specified by CorKat	Testing Performed by Security and Control LLC	Test Results
1.1 CorKat has established an **IT security program** to oversee security management, led by the **Information Security Officer** (ISO). The ISO routinely meets with executives and technical staff as well as customers to discuss functional, operational, and security issues.	Corroborative inquiry of key personnel to confirm that the enterprise-wide IT security program has been developed, including documented IT security policies and formal appointment of an ISO. Performed a process walk-through with key personnel of the IT security program. Inspected documentation related to the IT security program to confirm its existence, including ISO appointment and responsibilities, IT security policies, and documentation from staff meetings.	No exceptions noted.
1.2 CorKat has developed **IT security policies** approved by senior management which include procedures for protecting company and customer assets (facilities, hardware, software, and data) and responding to, reporting and investigation of security violations.	Corroborative inquiry of key personnel to confirm the existence of enterprise-wide IT security policies which address technical, administrative and management security activities for all employees. Performed a process walk-through with key personnel of the IT security policies. Inspected IT security policies and procedures to confirm the completeness and currency of requirements and applicability for protecting company and customer IT assets.	No exceptions noted.
1.3 CorKat has instituted **IT security awareness training**. All new employees receive security awareness training and all	Corroborative inquiry of key personnel to confirm that IT security training is provided to new employees and update training is conducted periodically. Performed a process	No exceptions noted.

	employees are required to undergo periodic update training.	walk-through with key personnel of the IT security awareness training program. Inspected IT security awareness training documents to confirm that training is conducted during the new employee onboarding process and that periodic awareness updates are provided.	
1.4	CorKat has a **human resource** process for hiring, training, employee development, performance evaluation management, retention activities, termination, and record keeping. CorKat has developed **job descriptions** which describe primary job functions, responsibilities and minimum qualifications. The company has developed a performance management program which requires **annual reviews**.	Corroborative inquiry of key personnel to confirm that a formal employee hiring, development, retention, training, evaluation and termination program exists. Performed a process walk-through with key personnel of the human resource program. Inspected the employee handbook, job descriptions, onboarding and termination checklists, to confirm that a formal employee management program exists. Corroborative inquiry of key personnel to confirm that personnel are provided professional development objectives and that their performance is reviewed annually by management against these objectives. Inspected a sample of employee job descriptions to confirm that employees are provided standards of performance and job function objectives which guide their job responsibilities.	No exceptions noted.
1.5	All new CorKat employees are subjected to **pre-employment screening** including background checks that include name, address, social security verification, and criminal history reviews. Reference checks and face-to-face interviews	Corroborative inquiry of key personnel to confirm that employees are subjected to pre-employment background checks including criminal records checks, employment reference checks, and management interviews prior to commencement. Performed a process walk-through with key personnel of the pre-employment screening process.	No exceptions noted.

	are also performed. All **employment offers** are contingent upon successful completion of all pre-employment screening.	Inspected a sample of employee background checks and the employee handbook to confirm that pre-employment screening is performed and management interviews are conducted to assess the individual's technical skills and ethical behavior necessary to meet company standards. Examined a sample offer letter to confirm the requirement that new hires complete pre-employment screening.	
1.6	CorKat employees receive a copy of the **employee handbook**. This handbook includes critical company policies covering: ethics, reporting questionable behavior, information sensitivity, customer confidentiality, and the acceptable use of company resources. Each employee **acknowledges** receipt and understanding of the handbook in addition to confidentiality statements.	Corroborative inquiry of key personnel to confirm that all employees are provided copies and sign acknowledgement of their reading and understanding of the employee handbook and confidentiality statements. Performed a process walk-through with key personnel of the employee handbook. Inspected the employee handbook and a sample of employee acknowledgements to confirm that the handbook addresses individual employee responsibilities for conduct, ethical behavior, customer confidentiality, and reporting of any questionable behavior and acceptable use of company assets and information sensitivity and that employees sign their acknowledgement of the document.	No exceptions noted.
1.7	CorKat has an **insurance and risk management program** which includes protection related to extra expense, property and casualty, and liability.	Corroborative inquiry of key personnel to confirm that the company conducts annual IT security risk assessments and maintains IT related insurance policies for extra expense, property and casualty, and liability protection. Inspected insurance policies to confirm that critical IT and business assets were covered with reasonable deductibles for extra expense, property and casualty, and liability protection.	No exceptions noted.

LOGICAL ACCESS AND SECURITY CONTROLS

Control Objective 2.0

Controls provide reasonable assurance that logical access to systems, networks, applications, and data is restricted to properly authorized individuals and such individuals are restricted to performing authorized and appropriate actions.

Controls Specified by CorKat	Tests Performed by Security and Control LLC	Test Results
2.1 CorKat has established a process for **provisioning** new employees, changing access privileges and for disabling separating employee system access. Access request forms are reviewed and approved by the management.	Corroborative inquiry of key personnel to confirm the existence and completeness of user access forms and user provisioning and account administration policies, procedures, and practices. Inspected policies, procedures, access request forms, desktop references, and online computer screens to confirm that access provisioning is conducted in accordance with management policy. Inspected documentation supporting user access provisioning and account administration including approved access requests and use of security templates (roles and groups) – with appropriate management approval - for defined company roles and responsibilities. Inspected a sample of user access request forms and compared these against in-place logical access rights and privileges to confirm requests are approved and access appears appropriate based upon their job duties and responsibilities. Performed online walk-throughs to confirm the processes for provisioning, changing and disabling user accounts along with access rights/privileges and the timeliness and completeness of restricting or deleting user access upon notification of employee hire, change, or termination.	No exceptions noted.

	Inspected a sample of employee separation requests to confirm notification timeliness and completeness, and observed online that user's access was appropriately deleted in a timely manner.	
2.2 CorKat has established procedures for ensuring that all new systems or existing systems (servers, devices, and platforms), when undergoing significant change, are configured using industry-standard **hardening** security settings (parameters) and that ongoing security advisories relating to security patches have been applied in a timely manner.	Corroborative inquiry of key personnel to confirm the timeliness and completeness of implementing system hardening and patch management changes. Performed a process walk-through with key personnel of the system deployment and hardening process. Inspected a selection of system patches and updates and performed an online walk-through to confirm the testing and movement to production of critical system changes. Observed online and inspected of system configuration, parameters and services to confirm that hardening processes are applied.	No exceptions noted.
2.3 CorKat has implemented employee **access controls** for systems (network devices, operating systems and databases) to enforce identification, authentication, and authorization for access to all systems. These controls include unique user accounts, complex automatically-expiring passwords, and access control list (ACL) authorization controls. User access is based upon business need-to-have and implemented through role-based security, limiting users to only their required authorizations.	Corroborative inquiry of key personnel to confirm the existence and completeness of processes designed to enforce identification and authentication controls on network, operating systems and database platforms. Inspected IT security policies, procedures, desktop references, and online computer screens to confirm the implementation of appropriate identification and authentication system controls. Inspected online system security settings to confirm enforcement of the following strong user identification and authentication management parameters and logical access rules for employee access:	No exceptions noted.

	Password length minimums, Forced password expiration, Prohibition of reusing previous passwords, Password syntax complexity, Invalid password attempt lockouts, Terminal timeouts, One-way encryption of passwords, and Masking of the password on terminal screens. Corroborative inquiry of key personnel and inspection of a sample of user access request forms to confirm that system authorization and access is granted based upon formal documentation. Inspected a sample of users' access rights, permissions, and privileges and confirmed that each had management approved access requests on file and that access rights, permissions, and privileges appear appropriate for their job function. Scanned the entire listing of system users and their roles/groups and associated permissions and inquired to confirm that access appears appropriate for individual's group and user responsibilities.	
2.4 CorKat has limited system, network, database and security **administration** capabilities to those system and security technicians having a specific requirement in performing their job duties. Administrators utilize multi-factor authentication (MFA) for all system-level access.	Corroborative inquiry of key personnel to confirm that system, network, database and security administration access is granted based upon formal documentation and adheres to established policies and procedures and that only a limited group of IT administrators are provided this access. Performed a process walk-through with key personnel of the IT administrative rights process. Inspected a listing of all users with administrative (executive) access to network, server, and security	No exceptions noted.

	environments to confirm adherence to documented policies and procedures and that these users had a legitimate business need. Inspected online and performed corroborative inquiry to confirm the use of MFA for administrative system-level access.	
2.5 CorKat has implemented **logging** for operating systems, applications, network, and security devices. Logs are routinely reviewed and archived for future reference.	Corroborative inquiry of key personnel to confirm that operating system, applications, network, and security devices audit and logging is activated and that logs are monitored in accordance with documented policies and procedures. Performed a process walk-through with key personnel of the IT log monitoring process. Performed online inspection of a sample of operating system, application, network, and security device platform logs noting that logs are activated, retained for at least 90 days, archived during backups, and provide security-relevant user, activity, time, date, and action information within the log entries.	No exceptions noted.

NETWORK SECURITY CONTROLS
Control Objective 3.0

Controls provide reasonable assurance that the network infrastructure is protected against unauthorized access and modification.

Controls Specified by CorKat	Tests Performed by Security and Control LLC	Test Results
3.1 CorKat have deployed rule-based router controls and **firewalls** to restrict external users from gaining unauthorized access to the network. A *defense in depth architecture* has been implemented to segment the network into un-trusted, (demilitarized) and trusted (internal) network segments.	Corroborative inquiry of key personnel to confirm that network policies have been established and that network devices have been deployed in a defense-in-depth approach to prevent network intrusion. Performed a process walk-through with key personnel of the IT network design, architecture, tools, monitoring, and management process. Inspected documentation including network diagrams, IP addressing schemas, and configuration interfaces and performed visual observation and tracing of a sample of critical network components to confirm deployment of routers with access control entries (ACEs), firewalls and intrusion prevention systems (IPS) and segmentation and routing of all public traffic to the demilitarized zones (DMZs). Inspected a sample of firewall configurations to confirm that appropriate ACEs and firewall rule settings have been established for public internet access and that high risk services, ports and protocols have been denied.	No exceptions noted.
3.2 CorKat utilizes encryption tunnels into the internal networks and systems and multi-layer authentication for **remote access authentication** into the corporate environment.	Corroborative inquiry of key personnel and end users and inspection of documentation including network diagrams to confirm deployment of remote access authentication. Performed a process walk-through with key personnel of the remote access process.	No exceptions noted.

	Observed online the remote access configuration and conducted a walk-through of remote access to confirm the use of authentication and encrypted tunnels for remote access. Inspected a sample of remote user access accounts to confirm appropriateness for their job function. Observed online that network and server layer authentication is used to manage administrative access to production systems.	
3.3 CorKat has deployed **antivirus** protection on workstations and servers common to malicious intrusions to prevent, detect and eradicate software logic attacks. Antivirus is updated frequently to ensure software currency.	Corroborative inquiry of key personnel to confirm the existence, currency, and completeness of antivirus software designed to detect and eradicate malicious programs. Performed a process walk-through with key personnel of the IT antivirus process, including signature updates, deployments, and scans. Observed online and inspected documentation to confirm the use of antivirus for a sample of desktops, servers, and email common to malicious intrusions and that antivirus signature updates are frequent and distributed to all endpoints on a routine basis. Observed online and inspected documentation for a sample of antivirus logs to confirm that antivirus protection updates are downloaded daily and pushed to endpoint devices in a timely manner.	No exceptions noted.
3.4 CorKat has a policy and has deployed controls to prohibit the **transmission of sensitive customer** and employee data across public networks including using network transmission encryption.	Corroborative inquiry of key personnel to confirm the policy prohibiting the transmission of sensitive customer and employee data via public email or network transmission, without the use of encryption.	No exceptions noted.

	Observed online the use of secure transmission technologies including: Virtual Private Network (VPN), Secure Socket Layer (SSL), and email encryption for the transmission of sensitive customer, employee and company data over public networks.	

COMPUTER OPERATIONS CONTROLS

Control Objective 4.0

Controls provide reasonable assurance that technology operations procedures are documented, that critical systems and applications are available, and that system incidents are detected, identified and corrected in a timely manner during application processing.

Controls Specified by CorKat	Tests Performed by Security and Control LLC	Test Results
4.1 CorKat has developed **standard operating procedures** (SOPs) for guiding information technology activities. The documentation describes normal operating procedures and identification and reporting of processing or system failures. The operating procedures are available to production support personnel online. Operations procedures cover critical technology activities including: network, operations, security, systems/servers, helpdesk, and problem management. Redundancy is built in at critical points throughout the production environment.	Corroborative inquiry of key personnel to confirm existence, completeness and applicability of computer operations procedures including: network, operations, security, systems/servers, helpdesk, and problem management. Inspected computer operations and policy documentation including network, operations, security, systems/servers, helpdesk, and problem management to confirm existence and completeness of documentation. Observed online a sample of logs and scripts used for network and system/server monitoring of daily backups, security event logging. Inspected online problem management listings to trace activities and events associated with problem tickets to their resolution. Observed network and server hardware redundancy and availability within the data center.	No exceptions noted.
4.2 CorKat has deployed a variety of network, system and application **monitoring tools** that are used to ensure availability and performance.	Corroborative inquiry of key personnel to confirm the use of automated network and server monitoring and alerting on system and network events. Performed a process walk-through with key personnel of the IT monitoring process.	No exceptions noted.

	Observed online the use of network and server monitoring and alerting systems, including alert recipients and confirmed actions taken to resolve a sample of network and server issues.	
4. 3 CorKat performs routine **backups** of critical storage which includes transit to off-site data storage.	Corroborative inquiry of key personnel to confirm the existence and completeness of processes and procedures relating to backup and off-site storage procedures. Performed a process walk-through with key personnel of the IT backup process. Observed online a sample of operations logs and online files, and performed a walk-through of the backup automation to confirm the adherence to routine backup processes. Inspected a sample of automated backup inventory listings and off-site storage documentation to confirm routine backups are replicated off-site.	No exceptions noted.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT CONTROLS

Control Objective 5.0

Controls provide reasonable assurance that business applications are designed and built using industry standard methods and that both infrastructure and business application changes and modifications are authorized, tested, and documented.

Controls Specified by CorKat	Testing Performed by Security and Control LLC	Test Results
5.1 CorKat has established formal **development and change control procedures** which require management approval and testing prior to code deployment. The company has deployed change management ticketing software for all infrastructure and application changes.	Corroborative inquiry of key personnel to confirm the existence of a formal development relating to: system development (custom) and change control including methodical life cycle phases and milestones such as initiation, requirements, design, development, testing, and implementation. Inspected the development and change control documentation to confirm its existence, completeness and applicability to the IT. Inspected a sample of IT project-related documentation to confirm adherence to SDLC methods.	No relevant exceptions noted.
5.2 CorKat has established a **change review process** staffed by management to review and approve all infrastructure (servers, network platform) and application program changes. The company maintains an IT change control policy and related procedures for managing infrastructure and application changes. Only authorized staff have access to production systems.	Corroborative inquiry of key personnel to confirm the existence and completeness of IT change control and configuration management policies, procedures, and practices. Performed a process walk-through with key personnel of the IT change control process. Inspected a sample of change control and configuration management documentation to confirm that infrastructure and application change processes are implemented in accordance with the enterprise policy and that changes are approved by management and tested prior to movement to production.	No relevant exceptions noted.

	Observed a sample of online version control libraries noting segregation and naming standards for test objects, version control, and production objects. Inspected a sample of change requests for infrastructure and application changes, and both normal and emergency changes to confirm management approvals, completeness of documentation, and existence of change testing. Corroborative inquiry of key personnel to confirm that production system access is granted based upon formal documentation and adheres to established policies and procedures and is limited to authorized staff.	
5.3 CorKat policy requires that infrastructure and application changes (system and network), both routine and emergency, are only migrated to the production environment **after successful completion of testing** and appropriate signoff by management.	Corroborative inquiry of key personnel to confirm the existence and completeness of IT change control and configuration management policies, procedures, and practices including routine and emergency changes to infrastructure and applications. Performed a process walk-through with key personnel of the IT production control process. Inspected a sample of change control and configuration management documentation to confirm that infrastructure and application change processes are implemented in accordance with the enterprise policy and that changes are approved by management and tested prior to movement to production.	No relevant exceptions noted.

PHYSICAL AND ENVIRONMENTAL PROTECTION
Control Objective 6.0

Controls provide reasonable assurance that data center physical security access control is restricted and monitored and that environmental protection supports reliability and availability of critical technology assets.

	Control Activity Specified by CorKat	Tests Performed by Security and Control LLC	Test Results
6.1	The CorKat data center is **constructed** with barrier, fire, and environmental protection for both the building and data center. The data center is in a light industry and office environment with no significant local hazards.	Corroborative inquiry of key personnel to confirm that the construction and location of the data center provides reasonable protection against man-made, natural, or technological hazards. Inspected documentation relating to the floorplan and construction and observed the area location, building, and data center to confirm the construction, location and resilience against hazards.	No exceptions noted.
6.2	The CorKat data center is equipped with an electronic **access control system** which is logged and monitored 24x7. Data center access requires approval from management and is provided to only those personnel having a legitimate need to access.	Corroborative inquiry of key personnel to confirm the existence, completeness, appropriate design, and operational administration of the card reader physical security access control system for the data center. Inspected a sample of personnel with access to the data center and corroborative inquiry with key personnel to confirm their currency, appropriateness, access approvals, and access levels provided to confirm the reasonableness of each user's access in accordance with their job responsibilities. Inspected a sample of terminated personnel and reviewed the computer room access listing to confirm they no longer have access to the data center.	No exceptions noted.

6.3	CorKat data center **visitors** are required to provide identification for access to the data center. Visitors are escorted at all times within the data center. Access requests must be pre-approved by management for access. All visitors must complete the sign-in log.	Corroborative inquiry and observation of data center visitor procedures, including submission of appropriate identification, sign-in, and escort procedures, to confirm adherence to documented policies. Inspected a sample of documentation including visitor logs, physical security procedures, and onsite staffing procedures for the data center to confirm access restrictions require documented pre-visit approval and that access to the data center and data center cabinets is restricted to only those specific personnel who have been pre-approved by management.	No exceptions noted.
6.4	CorKat has deployed closed circuit television (**CCTV**) throughout the data center and the cabinet areas to monitor activity and movement throughout the data center. CCTV archives are retained a minimum of 90 days. CCTV monitoring is performed by operations staff.	Corroborative inquiry of key personnel to confirm the existence and adequacy of the CCTV system for the data center and computer cabinets. Further inquired to confirm the design, implementation (visibility positioning) and ongoing monitoring and administration of these devices. Noted that the systems are only accessible to technology staff. Inspected a sample of CCTV online historical file images to confirm their retention is a minimum of 30 days for the data center. Observed the CCTV system equipment in operation for the data center and computer cabinets to confirm the coverage, visual positioning and completeness as well as direct observation (real-time monitoring) capabilities. Observed ongoing monitoring of CCTV by operations staff.	No exceptions noted.

6.5	The CorKat data center is equipped with independent computer room air conditioning (**CRAC**) in addition to automated temperature and humidity monitors.	Corroborative inquiry of key personnel to confirm the existence, completeness and appropriateness of computer room air conditioning services for the data center, including type, capacity, monitoring, and independence of the systems from the building services. Observed environmental protection systems for the data center to confirm their existence and operation.	No exceptions noted.
6.6	The CorKat data center is equipped with automated fire detection **fire detection** systems linked to 24x7 central site monitoring. The data center maintains hand held fire extinguishers. Local fire department inspections are routinely performed.	Corroborative inquiry of key personnel to confirm the existence and adequacy of fire protection systems, including fire detection and fire suppression systems and fire alarm monitoring and to confirm that local fire department inspections are routinely conducted for the data center. Observed fire protection system equipment including smoke, automated fire suppression, and hand-held extinguishers for the data center to confirm their existence, re-charge and inspection currency.	No exceptions noted.
6.7	The CorKat data center is equipped with uninterruptible power supplies (**UPS**) and auxiliary power generators which provide backup power to all essential data center operations and systems, with short-term (daytanks) fuel capacity onsite. Agreements have been established for long-term fuel replenishment. The UPS provides in-line filtered and regulated electrical power to the data center	Corroborative inquiry of key personnel to confirm the existence, maintenance and testing of UPS and backup diesel generator and fuel supply for the data center. Observed UPS and backup diesel generators to confirm their existence and capacity to support technology requirements.	No exceptions noted.

floor. These systems are routinely tested.		