INDEPENDENT SERVICE AUDITOR'S REPORT

VENTIV TECHNOLOGY, INC.

Integrated Risk Management, Claims, and Digital Application Hosting Services

Report on a Description of a Service Organization's
System and the Suitability of the Design and Operating Effectiveness of Controls
(SOC 1® Type 2)

For the Period
November 1, 2019 to October 31, 2020

VENTIV TECHNOLOGY, INC.

Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls

TABLE OF CONTENTS

AGL CPA Group, LLC
Service + Expertise = Value
1870 Buford Hwy, Suite 100
Duluth, GA 30097
http://aglcpa.com

IINDEPENDENT SERVICE AUDITORS' REPORT

To the Board of Directors of Ventiv Technology, Inc.:

Scope

We have examined Ventiv Technology, Inc.'s ("Ventiv Technology") description of its Integrated Risk Management (IRM), Claims, and Digital application hosting services system entitled "Description of the Ventiv Technology System Used to Manage and Control the Integrated Risk Management (IRM), Claims, and Digital Application Hosting Services" throughout the period November 1, 2019 to October 31, 2020 (description) and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Ventiv Technology, Inc.'s Assertion" (assertion). The controls and control objectives included in the description are those that management of Ventiv Technology believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the 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 Ventiv Technology'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 complementary user entity controls.

Ventiv Technology uses subservice organizations to provide colocation data center services including maintaining and monitoring certain physical and environmental controls over components of the system. The description includes only the control objectives and related controls of Ventiv Technology and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Ventiv Technology can be achieved only if complementary subservice organization controls assumed in the design of Ventiv Technology's controls are suitably designed and operating effectively, along with the related controls at Ventiv Technology. Our examination did not extend to controls of the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section V, "Other Information Provided by Ventiv Technology," is presented by management of Ventiv Technology to provide additional information and is not a part of Ventiv Technology's description of its system made available to user entities during the period November 1, 2019 to October 31, 2020. Other information presented by Ventiv Technology's has not been subjected to the procedures applied in the examination of the description of the Integrated Risk Management (IRM), Claims, and Digital application hosting services system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Integrated Risk Management (IRM), Claims, and Digital application hosting services system and accordingly, we express no opinion on it.

Service organization's responsibilities

In Section III, Ventiv Technology has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Ventiv Technology is 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, 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 auditors' 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 the 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 November 1, 2019 to October 31, 2020. 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 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, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization 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 providing Integrated Risk Management (IRM), Claims, and Digital application hosting services. 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 IV.

Opinion

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

a. the description fairly presents the Integrated Risk Management (IRM), Claims, and Digital application hosting services system that was designed and implemented throughout the period November 1, 2019 to October 31, 2020.

b. the controls related to the control objectives 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 November 1, 2019 to October 31, 2020 and subservice organizations and user entities applied the complementary controls assumed in the design of Ventiv Technology's controls throughout the period November 1, 2019 to October 31, 2020.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period November 1, 2019 to October 31, 2020 if complementary subservice organization and user entity controls assumed in the design of Ventiv Technology's controls operated effectively throughout the period November 1, 2019 to October 31, 2020.

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 Ventiv Technology, user entities of Ventiv Technology's system during some or all of the period November 1, 2019 to October 31, 2020, 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 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.

AGL CPA Group, LLC

Duluth, Georgia
November 15, 2020

II. MANAGEMENT'S ASSERTION

Assertion of the Management of Ventiv Technology, Inc.:

We have prepared the description of Ventiv Technology, Inc.'s ("Ventiv Technology") system for providing the Integrated Risk Management (IRM), Claims, and Digital application hosting services entitled "Description of the Ventiv Technology System Used to Manage and Control the Integrated Risk Management (IRM), Claims, and Digital Application Hosting Services" throughout the period November 1, 2019 to October 31, 20120 ("description") for user entities of the system during some or all of the period November 1, 2019 to October 31, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial statement reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves when assessing the risks of material misstatement of user entities' financial statements.

Ventiv Technology uses subservice organizations to provide third-party colocation data center services to maintain and monitor certain physical and environmental controls over components of the system. The description includes only the control objectives and related controls of Ventiv Technology and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organizations.

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 Ventiv Technology's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

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

1) The description fairly presents the system for managing IRM, Claims, and Digital application hosting services made available to user entities of the system during some or all of the period November 1, 2019 to October 31, 2020 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:

    a) 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:

        i) The types of services provided, including, as appropriate, the classes of transactions processed.

        ii) 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.

iii) 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.

iv) How the system captures and addresses significant events and conditions other than transactions.

v) The process used to prepare reports and other information for user entities.

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

vii) The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the controls.

viii) 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.

b) Includes relevant details of changes to the system for managing the IRM, Claims, and Digital application hosting services during the period covered by the description.

c) Does not omit or distort information relevant to the 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 auditors and may not, therefore, include every aspect of the system for managing the IRM, Claims, and Digital application hosting services that each individual user entity of the system and its auditor may consider important in its own particular environment.

2) The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period November 1, 2019 to October 31, 2020 to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of Ventiv Technology's controls throughout the period November 1, 2019 to October 31, 2020. The criteria we used in making this assertion were that:

a) The risks that threaten the achievement of the control objectives stated in the description have been identified by management.

b) 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.

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

Signed and acknowledged by:

/Dinesh Senanayake/
Chief Operating Officer

/Rahul Vaidya/
Chief Information Officer

III. DESCRIPTION OF THE VENTIV TECHNOLOGY SYSTEM USED TO MANAGE AND CONTROL THE INTEGRATED RISK MANAGEMENT (IRM), CLAIMS, AND DIGITAL APPLICATION HOSTING SERVICES

Ventiv Technology Overview

Ventiv Technology, "the Company" is a global company in the insurance industry with offices in London, Sydney, Los Angeles, San Ramon, Chicago, Atlanta (headquarters office), and Noida, India. Ventiv was formerly a unit of Aon PLC, and became an independent company in 2014 when it was acquired by Symphony Technology Group. In 2019, Ventiv was acquired by TailWind Capital.

Ventiv has more than 40 years of experience in the technology business. The Company serves more than 550 organizations and 350,000 users around the world.

One of Ventiv Technology's core values is always maintaining a client focus. The Company recognizes the unique needs of different clients and their professionals specialize by product, function and client industry—all coordinated by client delivery leads, or territory vice presidents, who factor in a holistic view of the client's needs.

By truly listening to their clients and working with them as a partner, Ventiv Technology develops solutions that work with their business. In this manner, the Company helps clients to uncover risks and discover new opportunities to make their businesses more successful, now and into the future. Ventiv Technology's services include Integrated Risk Management systems (IRM), analytics, claims management software, risk information consulting, data management consulting, enterprise risk management consulting, incoming certificate management, and casualty risk management tools.

To stay connected with current and prospective clients, Ventiv Technology updates the online portal http://www.ventivtech.com with innovative solutions; publishes client case studies; hosts client conferences; hosts Ventiv University; and provides updates via social media sites like LinkedIn, Twitter and Facebook.

Scope of the Report

This report has been prepared to provide information on the controls applicable to Ventiv Technology's IRM (formerly RiskConsole and RiskConsole Advanced), Digital (formerly Capture), and Claims (formerly IVOS) Application Hosting Services.

To provide these services, Ventiv Technology uses a variety of third-party providers ("subservice organizations") that provide colocation data center services for physical and environmental protections. DataSite is a subservice provider that provides the primary colocation data center services to Ventiv Technology. Cyxtera is a subservice provider that provides colocation services to Ventiv Technology in Denver, CO. Citadel100 is a subservice provider for the primary applications and infrastructure for the hosting services provided in the European Union. HP Corporation is a subservice provider for the disaster recovery applications and infrastructure for the hosting services provided in the European Union.

The scope of this report only includes controls related to Ventiv Technology's IRM, Digital, and Claims Application Hosting Services. The scope of this report does not extend to the controls of the subservice organizations.

Services Provided

Today, the insurance industry faces significant cost and operational issues. Most financial transactions occur electronically in real time, leveraging data to enhance performance. Launched in 2001, IRM is the pioneer in browser-based risk information technology. Utilized by over 275,000 users in over 40 countries, IRM was designed to give clients an integrated enterprise-wide view of risk exposure and deliver critical risk management intelligence. IRM has the ability to maintain a wide variety of risk and insurance information with full multilingual and multicurrency capabilities.

Ventiv IRM ("IRM") (formerly RiskConsole and RiskConsole Advanced) is an all-in-one system that turns risk and insurance data into insights. It allows clients to manage and analyze their risk data, renewal data collection, incidents and claims, policies, ERM, premium allocation, risk financing, and more—all from one integrated system.

In addition to allowing manual data entry, IRM consolidates data from multiple external sources and internal systems like HR, payroll, fleet, etc. This means clients can establish a repository of risk information in the most efficient manner, giving a complete business picture. IRM is software that helps to actively reduce total cost of risk by improving the efficiencies, effectiveness, and compliance.

The integrated insurance platform handles all insurance transactions, including claims administration, medical bill review, and policy administration. By managing all of clients' vital insurance processes for multiple lines of business, Ventiv helps organizations make the process transformations that deliver administrative savings, streamline workflows, reduce claims costs, and control expenses.

Ventiv Digital ("Digital") (formerly Capture) is an Integrated Risk Management Solution built upon completely re-envisioned technology from the browser all the way back to the server. Digital gives risks managers everything they want from a risk platform; analytics and reporting, enhanced performance, automation and a user experience that supports risk managers in how they want to work, view and analyze data, and make information-based risk and insurance decisions.

Digital allows companies to streamline risk, insurance and claims processes requiring data intake. It is powerful, versatile, and easy-to-use tool that ensures your field employees have the right tools to provide high-quality, complete risk, insurance, and claims information.

Ventiv Claims ("Claims") (formerly IVOS) is a web-based application used for a variety of insurance-related transactions. This system serves as a single solution for all insurance needs, including:

- Claims administration – a complete set of claims automation tools to deliver administrative savings, streamline workflow, reduce claims costs, and control expenses in high cost areas
- Policy administration and underwriting – a wide array of capabilities to develop, process and administer policies, as well as underwrite and rate coverage
- Event reporting and management – ability to Digital information immediately after an event or incident, providing an opportunity to prevent claims and losses from ensuing in the future
- Document imaging – scanned documents and electronic files that enable clients to move to a paperless business environment with seamless data-driven workflow and management

By managing all these business processes for multiple lines of insurance, Claims helps organizations undergo an extensive process transformation, from disjointed and inefficient to integrated and streamlined. Claims is highly flexible and can be customized to meet any organization's unique business requirements. Companies can leverage Claims as an integrated "one-system" solution, or they can simply select the components they need.

Ventiv Technology manages and provisions the entire technology environment. This provides clients with the ability to adapt to changing community needs, upgrade the solutions, guarantee performance and deliver superior security levels.

The services provided by Ventiv Technology within the scope of this examination are for hosting services provided for clients.

Description of Relevant Transactions Processed

Due to the configurable nature of IRM, Digital, and Claims, the reporting produced by IRM, Digital, and Claims will vary based on client use. IRM, Digital, or Claims does not directly impact client accounting records. Ventiv does not initiate any transactions on behalf of customers. Clients are responsible for the review, approval, and use of the systems, data and reporting produced by IRM, Digital, and Claims as input to their accounting records and financial statements.

Control Environment Elements

Organizationally, Ventiv Technology, follows a traditional model. The global Ventiv Technology Board is composed of Ventiv Technology Executives. The Board meets frequently to discuss matters pertinent to the Company and to review financial information. Executive committee meetings, annual management and technology meetings, and product management meetings confirm that Ventiv Technology has defined goals that support the Company's mission.

Ventiv Technology's Human Resources Department works with department hiring managers to select and hire talented employees in order to build winning teams and deliver business results with excellence. Formal background checks and drug tests are performed for all potential employees. All new hires are required to complete new hire training and to review and sign off on the Code of Conduct, Security Awareness Training and Information Security Policy within the first weeks of employment. Initial training and ongoing awareness training are required and tracked by an online system. The online system includes automated alerts, tracking and reporting, which are used to help promote and monitor compliance with policies and regulatory requirements.

The Human Resources Department facilitates the annual performance appraisal process to recognize employees for their contributions and innovative ideas and formally track performance against their individual goals. Employees are offered on-going training to stay current or enhance their skill sets and obtain certifications.

Monitoring

The Chief Information Officer is responsible for overall planning, directions and control operations within the Ventiv Technology departments. The departments are organizationally divided into teams according to the service areas, allowing for clearly defined responsibilities, effective downward and upward communications, and performance (including control) monitoring.

The Information Technology (IT) Department manages, develops and enhances the internal corporate facing applications; and supports and administers internal applications, databases and operating systems located in the Ventiv Technology data center or hosted by third party providers.

The Finance, Legal Operations, and Administration Department oversees the legal and contractual agreements with clients and vendors and performs financial and business operations analysis.

The Global Professional Services Organization (PSO) handles client data conversion services, client ETL, report development, configurations, global customer support, relationship management, and account direction. Project Management Teams actively lead the successful execution of all projects, and the Business Analysis Team provides the input data for the relevant reporting.

Information and Communication

The Information Security and Data Privacy Department provides security, privacy and compliance oversight for both internal and client facing aspects of the organization.

Confidentiality, integrity and availability are the key drivers in the Ventiv Technology Internal Controls Framework. Ventiv Technology utilizes industry standards, country, federal and state/provincial regulatory guidelines to ensure that customer data is appropriately safeguarded and processed in compliance with regulatory requirements.

Ventiv Technology utilizes a variety of automated and manual systems to provide the appropriate information and communication necessary to effectively manage the business. The Executive Management Team meets on a regular basis and as necessary to review financial results, discuss and resolve day-to-day issues with Company performance, oversee operating activities, and develop strategy for the future. An open line of communication exists between the Executive Management Team and other members of management and staff. Multiple communication paths exist to help ensure that processes function as intended and issues are identified and resolved in a timely manner.

Risk Assessment Process

An annual risk assessment is performed based on Special Publication 800-30, Risk Management Guide for Information Technology Systems, published by the National Institute of Standards and Technology (NIST) and is also based on ISO 27001 standard published by International Organization for Standardization. Ventiv Technology uses this risk assessment to evaluate the adequacy of controls and identify any necessary new or revised controls. Ventiv also maintains the ISO 27001:2013 and ISO 27018:2014 certifications.

Release-related penetration tests and vulnerability scans are a part of the risk assessment process. Ventiv Technology uses an independent company to perform penetration testing. In addition, Ventiv Technology conducts internal penetration testing with an off the shelf tool. Another independent company provides weekly vulnerability scans. This overall approach, including internal assessment and independent test results, allows management to evaluate and manage risks based on severity and appropriately balance the costs and benefits. Risks are tracked, prioritized, accepted or remediated, monitored, and reassessed to help ensure protection of client data.

Description of IRM, Digital, and Claims Processes

Change Management

Ventiv Technology follows a formal change management process from the initiation of the change through development, testing and approved implementation.

Application Changes

Application changes are deployed via releases. An internal ticketing system is used to track and approve the change/story records. The initiator enters the change description, such as title, change category and summary, and functionality description within the ticketing system.

The Release Management team is a central hub for all code change requests. Only the Release Management group enters change control requests for software changes in the internal tracking tool.

Depending on the type of the change, approval of the change request is obtained from the Development Team Lead, Delivery Management or Technology Management. The approved change request is directed to the Development Team Manager, and the change is assigned to a developer, who starts coding on a dedicated development platform.

The Subversion tool is used to control the code change management process. The developer checks out the code from the Subversion system, which prevents another developer from making changes to the same code. Once the code is checked out, the developer makes the required change within the development environment. When coding is complete, the developer performs unit testing. When the unit testing is completed, the developer checks the code back into Subversion, and the Development Team migrates the code to the quality assurance (QA) environment.

Once the code change is migrated to the QA environment, testing is performed. Once all the changes/stories from the release are closed, regression and user acceptance testing (UAT) are performed by development, the professional services teams and clients (when necessary). All results are sent to the Product Management Team.

Once all testing has been completed for a change or story, approvals are granted within the ticketing system by Development Team Lead, Release Management and Technology Management. The approval provided by all three groups represents that the change is authorized, tested, approved and ready to be released into production.

Each release consists of several changes or stories, and each change consists of several tasks. In addition, all changes are implemented into production as part of a release package. Prior to a major release, a notice is sent out to the designated administrator of each client to inform them of the release.

IRM changes are moved into production by the IT Operations Team. Application changes are migrated by IT Operations with root access (sudo), and database changes are migrated using the IRM database schema owner account.

Digital changes are moved into production by the IT Operations Team.

Claims changes are moved into production by the IT Operations and IT Support teams. Application changes are migrated by IT Operations with root access (sudo), and database changes are migrated using the Claims database schema owner account.

The IT Operations Team is not involved with the development or QA testing of any product.

Smaller versions of releases are called patches. Patches follow the change management process with the exception that they are performed during maintenance windows, and UAT is not performed for all patches on the IRM or Digital systems. Claims does not utilize patches; all code changes are deployed via full deployment. In the rare event a client requests a patch instead of full deployment, such change is discussed and approved prior to deployment.

Emergency application changes follow the change management process with accelerated deployment timelines, sometimes automatic approval (for certain type of changes) or verbal approval and immediate implementation. Such changes are documented after the fact in the ticketing system.

Direct Data Changes

Direct data changes made by the IT Operations team are made to work around defects or gaps within the application (such as modifying application metadata that cannot be done through the application). These changes follow the change management process, with the exception that data changes are generally not tested by the Quality Assurance team; rather, they are tested by the Support team and IT Operations team managing the change, based on the requirements for each change type.

Infrastructure/Platform Changes

Server changes (Linux, Windows, Apache, etc.) originate from their respective vendors. Upon vendor notification for an upgrade, IT Operations will track the change in the ticketing system and will test a change in the development and UAT environments prior to implementation in the production environment.

Windows Server upgrade service is used to apply patches to Windows servers. The server communicates to the Windows update server looking for patches and upgrades. If a software upgrade, update or patch exists, the server downloads the update. Even though these updates are automatically downloaded to each blade server that runs on Windows, the IT Operations team is responsible for evaluating the upgrades. The team approves or denies the patch or upgrade and submits a change ticket in the ticketing system for the approved changes for approval, testing and implementation tracking.

Oracle enhancements, upgrades and patches are based on the Oracle recommendations. For each change, Database Administration (DBA) submits a request to Oracle or downloads an existing patch. The patch is tested in the development and UAT environments by the quality team. The DBA team determines when the patch needs to be released and creates a script to migrate the patch. These types of changes require Technology Management approvals and are implemented by the DBA team during the maintenance window.

Infrastructure changes are initiated, tested, and implemented within the IT Operations Department, which consists of the System Administration, Database Administration, and Network teams. These changes follow the change management process, with the exception that operating system and database updates are generally not tested by the Quality Assurance Team; rather, they are tested by the IT Operations Team managing the change, based on the requirements for each change type. Infrastructure changes only require the head of IT Operations to approve within the ticketing system.

Emergency changes follow the change management process, but the changes are applied on an expedited timeline. In addition, these changes are not required to be preapproved; instead, these changes are typically approved after they are implemented.

Physical Access

In general, all technology hardware, software and peripherals are owned and managed exclusively by Ventiv Technology. Ventiv Technology utilizes data centers in the US and European Union ("EU") built from the ground up with the express purpose of providing secure and highly available cloud solutions.

Data Center Locations

Ventiv Technology maintains its primary US data center in Marietta, GA. DataSite provides Ventiv Technology with colocation data center services at this location, including related security and availability. These services provided by DataSite are not included within the scope of this examination.

Ventiv Technology maintains its primary EU data center in Citywest, Ireland. Citadel100 provides Ventiv Technology with colocation data center services at this location, including related security and availability. These services provided by Citadel100 are not included within the scope of this examination.

The Company's critical processing equipment (IRM, Digital, and Claims production servers, QA servers, and Development servers) and client data is located in these primary data centers. Clients have the option of storing data in the US or EU data center. However, client production data is not transferred between the primary data centers or split between the primary data centers.

Ventiv Technology maintains its disaster recovery US data center in Denver, CO. Cyxtera Corporation provides Ventiv Technology with colocation data center services at this location, including related security and availability. These services provided by Cyxtera are not included within the scope of this examination.

Ventiv Technology maintains its disaster recovery EU data center in Santry, Ireland. HP Corporation provides Ventiv Technology with colocation data center services at this location, including related security and availability. These services provided by HP are not included within the scope of this examination.

Physical Security Procedures and Controls Performed by Co-location Data Center service providers listed above

The main entrances to the data centers are manned by security personnel 24 hours a day, 7 days a week, 365 days a year, and all auxiliary entry points require use of a key card for access. Access to the data center facilities are restricted to authorized personnel via key card authentication. At the entrance to sensitive areas of the data center, access is further restricted through biometric authentication.

Individuals with authorized access to the data centers must obtain their key cards from the main security desk after logging in to a journal and surrendering government-issued identification. The identification is retained by the security guard for the duration of the visit and until the key card is returned.

Upon entry to the data centers, individuals must pass through a man trap to gain access to the general facility. Users must scan their access card at the man trap before entering. An alternating space must remain between consecutive users. Furthermore, key card readers and biometric fingerprint scanners are installed on the direct entry and exit door to the data center room. Authorization must be used in order to enter and exit the data center room.

Upon client request for new employee or contractor access, a photo identification badge will be created, and the individual's biometric information will be programmed into the security system before the badge can be functional for access. All access to the facility is logged electronically within the badge access system as well as the digital video recording system, which has cameras covering the facility.

Physical Security Procedures and Controls Performed by Ventiv Technology

Access to the US and EU data centers is approved and granted only to the Ventiv Technology IT resources that require such access to perform their job duties. When a new IT employee is hired that requires access to a data center, the Director of IT or CISO approve the request when they send the email to the respective data center to provision the access.

In order to grant physical access, Director of Infrastructure & Operations or CISO will send an email request (with an updated access list) to the data center support team to create a badge for the new employee and add the user to the approved list of authorized users.

When an employee with data center access is terminated (voluntarily or involuntarily), the Director of Infrastructure & Operations or CISO completes the removal of data center access as part of the termination process. Notification of the termination is performed via phone with a follow-up email or via email and takes place before an involuntary termination is communicated to an employee to allow for access to be removed while the employee is meeting with Human Resources and management. This helps ensure that the employee has no access to any of the US or EU data centers after the termination announcement. The employee is escorted directly out of the building, and personal items are shipped to the employee at a later date. The Director Infrastructure & Operations or CISO notifies the US or EU data centers of the termination so that access to the data center facility is not permitted. The user's photo key card is destroyed.

If the termination is voluntary, access to the data centers is removed on the last day of employment. Access to the building is determined based on the arrangement between the employee and management regarding the employee's departure from Ventiv Technology. If a user resigns by telephone or email, the user's access to the facility and data centers is removed, and the key card is destroyed.

A review of data center access is performed by the Director of Infrastructure & Operations or CISO quarterly for all the data centers. During this review, the Director of infrastructure & Operations or CISO determines whether users with access to the data centers are appropriate based on their job responsibilities. If the Director of Infrastructure & Operations or CISO deems a user's access inappropriate, access is removed.

All visitors, including contractors, must be escorted inside the data centers by an authorized Ventiv Technology employee. Visitors are required to sign the visitor log and surrender a form of government issued ID at the front security desk prior to entrance to the restricted area. Ventiv Technology employees from other offices must sign in and be escorted as well.

All visitors to Ventiv Technology's main office must sign the visitor log with the front desk receptionist and present a form of government-issued ID for the duration of the visit. Visitors are issued a temporary visitor badge that allows access to the front door and back offices from 8 a.m. to 6 p.m. These badges do not allow access to the data centers or to secure IT rooms within the office space.

Logical Access

The process to control users' access starts when a new person joins Ventiv Technology. For every new hire at Ventiv Technology, HR or the employee's direct manager submits a user access request ticket within the internal ticketing system. Access is set up via Active Directory group. The ticket indicates the types of access required for the new user, including access to applications, databases, operating systems and the data center. Once the user access request form has been submitted, it is then routed to the appropriate group. A member of the Support Group sets up the new user profile based on the access levels specified within the access request ticket. The process of modifying or deleting a user's access at Ventiv Technology follows the same process and is tracked by a ticket.

Ventiv Technology clients require access to the IRM, Digital, and Claims applications as a part of the business model. IRM has different instances configured within the application, and each client has access only to the instance configured specifically for that client. When a new client instance is set up, a contract is initiated between the client and Ventiv Technology. The contract specifies the number of users the client needs to be set up within the client's subsystem. This information is provided in a spreadsheet that includes the names of the users to be set up and the level of access within the system for each individual or the users are added via a user load. This contract is in writing and is signed by both Ventiv Technology and the client contact. The Ventiv Technology Client Delivery Lead (CDL) assigns access within the IRM application as specified within the written contract.

Although all clients have a client delivery lead assigned to their instance within IRM and Digital, some clients still require Ventiv Technology to perform user administration on their behalf. In such cases, when a new user is hired by the client who requires access to their instance within IRM, an email request is generated by an authorized approver (typically the Client Administrator) and is sent to the client delivery lead at Ventiv Technology. The CDL then reviews the email to validate that it was initiated by the appropriate person. The CDL also reviews the contract to validate that the additional request does not exceed the number of users specified within the contract agreement. Once this has been verified, the CDL sets up the user within IRM.

It is the client's responsibility to notify the CDL at Ventiv Technology in the event that the client user is terminated. The request to modify or delete a client user's access within IRM or Digital follows the same process and can be completed either by a client's employee set up with administrative rights within the client instance or the Ventiv Technology CDL or Support Group.

The Claims-hosted environment provides all clients with their own instance of the Claims application. The Claims security model is highly configurable. All clients are responsible for defining and administering their unique security configuration. The system provides multiple levels of security, including groups, roles and users that can be applied virtually anywhere in the application to limit access. Once security is defined for a group, role or user to be limited to "view only," that same restriction automatically applies to the User Interface, Claims Reporter and other data access mechanisms in the application.

Administration to the IRM, Digital, and Claims applications is client specific, and therefore, the administrators only exist at the client/instance level. Client Administrators fall within one of four user groups as outlined below:

- Group 1: Client Administrators (CRS) – When a new client is set up within IRM, Digital, or Claims, the client provides Ventiv Technology with a defined list of employees who require access to the system and the level of access required by each individual. The client also specifies one or more individuals to be set up as the client administrator(s). These individuals have administrator privileges to that client only.
- Group 2: Client Delivery Teams – These individuals are Ventiv Technology employees and have administrator access to one or more clients in order to provide support services.
- Group 3: IRM Technical Support Personnel – These individuals are Ventiv Technology employees and have administrator access to one or more clients in order to provide technical support services.

A periodic review of access appropriateness is performed for Ventiv Technology employee groups to validate that they remain current employees and still require access.

There are no shared user accounts within the IRM or Digital applications. Access to the IRM and Digital applications is gained through the use of individual user accounts and requires a password. Ventiv Technology implements a standard password policy as noted below:

- Minimum length required is eight characters.
- At least one upper case letter is required.
- At least one lower case letter is required.
- At least one numeric or special character is required.
- Password changes are forced every 60 days (client configurable)
- Account lockout policy is set at three invalid logon attempts.

Access to the Claims application is gained through the use of individual user accounts. There is one shared account used by Support and IT resources to log in to the client's application. This account can be disabled at the client's request.

While the Claims passwords are set up and managed by each client independently, Ventiv Technology requires a minimum baseline for password security of hosted client as follows:

- Minimum length is eight characters.
- At least one upper case letter is required.
- At least one lower case letter is required.
- At least one numeric character is required.
- Password changes are forced every 90 days.
- Account lockout policy is set at three invalid logon attempts.
- Minimum failed login delay is set at 30 minutes.

There is a special user group within the IRM application that is referred to as "light users." These user accounts are flagged and have limited functionality. Access provided by these accounts is limited to entering incident data only. In addition, to authenticate light users, the source URL and IP address have to match. This special group of users does not require a password to access the IRM application, as functionality is limited to data entry. However, light users do have to enter their employee ID. The employee ID is then matched against the employee database to validate that the employee ID is valid. In addition, light users are employees of the client and not Ventiv Technology; thus, it is the client's responsibility to add/delete/modify light users' access within IRM. It is also the client's responsibility to review light users' access periodically.

The Linux operating system hosts the primary Oracle databases. An Active Directory account must exist in order to create a Linux account. When administrators log in to a Linux server, they are authenticating against the Active Directory domain (Kerberos), which then either lets them access the Linux server if they have a matching account or denies them access if not. This is a centralized authentication method.

In order to gain administrative privileges within Linux, a user must be a member of the IT Operations group and a user must authenticate to Linux first and then switch user (SU) into the Oracle or Root accounts. An individual must be set up within the "sudoers" file to be able to SU into the Oracle or Root accounts in Linux.

The Server Engineering Team performs a monthly review of user access to the Root or Oracle accounts on each Linux production server and all accounts on each Linux box. The Server Engineering Team reviews these reports to validate that the users listed are current Ventiv Technology employees and continue to need Linux access based on their job responsibilities.

Database Admin Access to production databases is limited to the members of the DBA Team. DBA Team members are granted administrator access (via the DBA role), which allows Database Administrators (DBAs) to perform sensitive functions within Oracle and make changes to data structures.

IRM, Digital, and Claims database changes are performed by the DBA Team using the respective database schema IDs. Simple IRM and Digital changes like running prepackaged deployment scripts can also be done by System Administrators using the IRM and Digital database schema accounts. The password for the database schema account in IRM and Digital is changed every 90 days and is communicated by the System Administrators in a password-protected Excel file in advance so that the application can be configured with the new credentials. The DBA Team keeps a different password-protected Excel file in a Subversion (SVN) repository for DBA Team usage. The SVN folder is restricted to only the Active Directory DBA group; thus, the password file is protected at the folder level and at the file level. The password change for the Claims database schema account follows the same process with an exception that the temporary password is changed every time the account is used, in addition to being changed every 90 days.

The DBA Manager monitors the use of the IRM and IRM database schema account weekly and checks to see if a correlating change request was approved to use it. The DBA Manager documents the findings from the review in the Technology Intranet system and posts the usage of the account for the past week. If someone uses the account without an approved request, then a ticket is created and routed to the Information Security Team and the individual and the individual's supervisor are notified and re-educated on the importance of following the process. A review is also performed to confirm that the change made was appropriate. Annually, the Information Security Team reviews the security audits and tailors the annual awareness training based on the emerging issues.

Database accounts within Oracle follow a standard password policy as follows:

- Minimum length required is eight characters.
- At least one upper case letter is required.
- At least one lower case letter is required.
- At least one number or special character is required.
- Password changes are forced every 90 days.
- Account lockout policy is set at three invalid logon attempts.

The Window servers are hosted by the Active Directory domain and can be accessed only by a member of the Active Directory Windows server Admin group. Authentication for the blade servers takes place at the Active Directory level.

Active Directory user accounts adhere to the standard password policy as follows:

- Minimum length required is eight characters.
- At least one upper case letter is required.
- At least one l lower case letter is required.
- At least one number or special character is required.
- Password changes are forced every 90 days.
- Account lockout policy is set at three invalid logon attempts.

Monthly, the Server Engineering Manager reviews the Active Directory user and Domain Administrators access to confirm that access is granted to current Ventiv Technology Server Engineering employees and is based on their job responsibilities.

Subversion is a change management tool used by developers to check in and check out code. User access to Subversion is limited to members of the Software Engineering Team and Professional Services. An administrator account is used to administer access to Subversion, and only the Software Engineering Manager has knowledge of the password to this account. Authentication for Subversion is done via Active Directory. A review of Subversion access is performed by the Director of Software Engineering quarterly. During this review, the Director of Software Engineering determines whether users with Subversion access are current Ventiv Technology employees, current Software Engineering Team members and have appropriate access based on their job responsibilities.

Internet Access

Access to IRM, Digital, and Claims is gained by accessing the application URL. Users are prompted to enter their user ID and password to gain access to the application itself. The application servers and web servers reside on physically separate machines. Client access to IRM and Digital is set up in such a way that a client can access and modify data that is owned by only that client. A client does not have the ability to view or modify other data within the IRM, and Digital environment that is not owned by that client. Client access to Claims applications is based on the client-specific application URL.

The IRM, Digital, and Claims applications do not allow for direct indexing from a standard search engine or from unauthenticated web browsers. As an example, if an individual references an internal address directly into a web browser, the application would automatically route the individual to the authentication screen, where the individual would be required to authenticate to the application using the individual's logon credentials. Individual user names and passwords are stored for each user, and a user must authenticate using the user's logon credentials. Informational traffic between the browser and the web server is encrypted.

Firewalls with integrated IDS/IPS are in place at the perimeter of Ventiv Technology. The firewalls are fully redundant and are deployed in front of the web and/or application servers. Internet traffic must pass through one of these firewalls. Access to the production firewall systems is limited to the Network Engineering Team. Firewall and network changes follow the Ventiv Technology change management process. An internal ticketing system is used to create, approve and track tickets for each change. In addition, on a monthly basis, the configurations of the firewalls in place are reviewed for appropriateness and to detect any changes made in the past month.

The firewalls perform the content filtering and block attacks, and system logging is enabled to view the Internet traffic history. This log includes information such as invalid logons, penetration attempts and other security-related information. The firewall sends notifications for each attempt of unusual or suspect activity to the Network Engineering Team. Each alert is reviewed and investigated, and a Technology Intranet ticket is created to track the potential issue. The investigation may include pulling information from other sources and logs to fully understand risks or threats. The results of the investigation are tracked within the ticket.

Activities for the Apache servers are logged on a continuous basis. The log includes information such as invalid logons, penetration attempts and other security-related information. These logs are reviewed and signed off monthly by a member of the Server Engineering team. If any unusual or suspicious activity is identified, a ticket is created in the ticketing system and the potential issue is investigated. The ticket is updated to track progress and resolution.

Third-party penetration testing is performed annually and vulnerability scanning is performed on an ongoing basis. The results of the tests and scans are discussed internally and with the vendors, and each applicable (critical/high, major) issue is tracked in the ticketing system until fully resolved. If a change is required as a result of the tests or scans, the change follows the established change management process.

All resolved issues are confirmed in the next pen test or vulnerability scans after they had been fully implemented.

A formal procedure for handling intrusion events is maintained and enforced by Ventiv Technology. When an intrusion event is raised, the individual who identified the issue creates a ticket within the ticketing system and notifies the on-call team member. Once the ticket has been created, the Information Security team is notified of the ticket. The IT Operations team or the Information Security Team then reviews the record and works with Server Engineering to determine the appropriate resolution and implementation timing.

If changes to the production environment are required for the incident resolution, the request is entered, which follows the change management process. Upon completion, the Director of Infrastructure & Operations or the Information Security Team and Server Engineering confirm that the resolution was successful, update the Security Incident Record status to "Resolved" and close the record.

System Operations

Application jobs are monitored by IT Operations. Since these jobs execute the reporting features of the applications, they are mainly used for the front-end client interfaces. Some jobs (such as in Claims) are controlled by the customer via the scheduler interface in the application. In case of an error, a client reports an issue to the client delivery team who creates a support ticket. Jobs can also self-resolve, such as a transient issue that prevents an individual job execution from succeeding but does not affect future executions (e.g., network availability prevents emails from being sent temporarily). In the case of a self-resolving job, a ticket is not created, as the issue exists only temporarily. Each request is treated as a formal change and follows the Ventiv Technology change management process.

The addition of a new database job follows the change management process. A change to an existing job follows the change management process if the change is made to the job's function. Changes to an existing job's schedule are considered routine changes and do not follow the change management process.

New job requests follow the change management process. The initial request for a new job is tracked through a ticket, which includes the request and desired completion date. When the change is completed, the ticket is updated with the resolution steps and date and closed.

Physical standby databases are monitored using Oracle Enterprise Manager. When a standby database has an issue applying changes from production, an alert is generated and is sent to the DBA Team. The DBA on call is responsible for manually troubleshooting the issue and resuming the log application process.

System-based job schedule changes are performed on the IRM Linux production servers. Since these changes do not require application code changes, the changes are performed in the production environment. System-based jobs primarily consist of Cron jobs. These jobs are used for purposes such as maintenance of log files and system outputs.

Monitoring agents have been installed on each machine, including the web servers, primary production server, blade servers and other reporting servers. In the event that a system error is encountered, an enterprise monitoring tool triggers a system event and automatically sends out a notification to the on-call support individual as well as the Server Engineering Team. Once the on-call individual is notified of the error, he/she is responsible for resolving the problem and tracking the issue through Technology Intranet.

Access to system-based job schedules is restricted through system-level su_oracle and su_root access that is limited to the Server Engineering and DBA Teams.

Backups / Data Replication

Ventiv Technology' backup policy is defined and documented and has been implemented for the servers.

The primary Oracle database instances consist of multiple Real Application Clusters (RAC) servers, each with a Linux operating system. Oracle's Physical Standby solution is used for local and remote backups of the primary databases.

For IRM and Digital, there are two local physical standbys in place, serving as local recovery options in the event of an issue with the primary database.

The remote physical standby also serves as the disaster recovery solution. Management has a defined Recovery Point Objective (RPO) for the production database, which is the maximum acceptable data loss, as measured by time.

The web and application servers are not backed up continuously since they do not store client data. The configurations are backed up twice a day leveraging VMware's SRM tools.

Production systems are backed up using a near real time replication process. An automated notification is sent to the Server Engineering Team when a backup fails. Once the backup failure is resolved and the backup is rerun successfully, Server Engineering closes the Backup Record within Technology Intranet.

Client Setup for IRM, Digital and Claims

IRM and Digital architecture provides the opportunity to configure client-specific modules. Information in each module can be linked to information in other modules. Integrating this information into Risk Console gives clients a single comprehensive environment for data management, risk analysis and risk reporting.

Ventiv Technology's Professional Services has defined an implementation methodology by which implementations and new client projects are managed.

Once a contract or statement of work (SOW) is signed, the Ventiv Team reviews and confirms the requirements of the project with the client before work begins. Detailed specification documents, as needed per the SOW, are written in a collaborative fashion with the client prior to development. Changes to the specifications required during the development are documented by Ventiv and approved by the client when necessary. Approved specifications are stored in the document repository for future reference as needed.

Ventiv assigns a Project Manager to the client and project, who is then responsible for creating and updating the project plan, communicating with the client regularly, and coordinating the work required to complete the project.

For Claims clients, the Project Manager sets up an area in the Document Repository specifically for the client so that the client can access all of the appropriate documentation for the project, including requirements, specifications, project plans and status reports. Each client user has a unique login to the Document Repository area and only has access to the documents for their implementation project.

IRM and Digital clients access a document repository in their application environment specific to only that client to access the appropriate documentation for the project, including requirements, specifications, project plans and status reports (if required.)

Work is assigned out to the functional teams and is completed per the specifications and/or requirements upon receipt of the signed documentation from the client. However, some collaborative prototyping occurs as specifications are being documented for increased transparency into proposed solutions.

Preliminary testing and validation are completed by the Project Manager/Business Analyst before the client completes UAT. For any changes or customizations outside the original scope, a specifications document is written or updated by Ventiv and reviewed with the client before any changes are made.

Throughout the setup process, periodic status calls are held between Ventiv and the client, during which open issues are discussed and resolutions are agreed upon. This information is tracked within open item logs. On a regular basis, a status report is generated by Ventiv and made available for client review. All custom work, as defined in agreed-to specifications, requires testing and acceptance approval by both Ventiv and the client prior to implementation to production. Subsequent to implementation, a formal sign-off is obtained by the client accepting the final product; however, in some instances the approval is implied; upon notification from Ventiv to the client of the implementation (i.e., non-response to the notification within 10 days would be considered implied approval), or the system going live with client usage.

While the Project Manager oversees the project and provides support to the client during the implementation phase, once the client goes live, support responsibilities transition to the client delivery team. A Client Delivery Lead is assigned to the client where appropriate in the planning phase of the project. The Support Team provides assistance to the client for any issues or changes that may arise once the client is live.

Data Conversion

IRM, Digital and Claims clients provide or cause to be provided from their other vendors, source data for conversion into a IRM or Claims database. The first step in converting client data is to receive or transfer the data from the source system to servers within the Ventiv Technology data conversion facility. Due to the type of information potentially involved (e.g., PHI – protected health information), clients are required to transfer their data in an encrypted form, either through an encrypted tunnel, such as SSH File Transfer Protocol (SFTP), or virtual private network (VPN). In the rare event when data is being transferred via external hard drive, the client must encrypt the data at the file level. Ventiv Technology provides the drive and instructions as to how to encrypt the files.

The Project Manager obtains and provides the pertinent client source information to the Data Services and Conversion Department via submission of a Data Conversion task. The Project Manager coordinates the timing and method for securely transferring the data. In the rare event when clients send data via encrypted hard drive, the Project Manager coordinates with the Ventiv Technology IT group to set up the appropriate security measures to protect the integrity of the client data while on site for conversion.

Upon receiving the client source data for a Claims project, the Project Manager notifies the help desk via a support request to place the data onto secure network servers. For IRM and Digital, the source notifies the data librarian automatically when posted.

The Data Migration Analyst assigned to the project begins the conversion tasks of importing to staging tables, analyzing data, mapping the data, developing the conversion code based on defined requirements, and validating the conversion code for completeness and financial balance. For Claims, the Data Migration Analyst is also responsible for packaging the data for updating a client's production database. For IRM and Digital, the Data Migration Analyst is responsible for turning on the conversion for production processing.

For locally hosted Claims clients, the Project Manager coordinates the return of the encrypted Claims database to the client via secure FTP or encrypted external hard drive. If Ventiv Technology is hosting the Claims environment, then the data is released to IT for placement in the client test environment. Help desk tickets are submitted by the Project Manager to instruct IT how to deliver the converted database. For IRM clients, the production database is updated and is released to the client.

At this point, the UAT phase begins. During UAT, the client is responsible for executing a wide variety of test processes to validate whether data mapping is accurate and complete, financial balancing is accurate, and functional requirements within the software have been met. As part of the UAT for the trial conversion process for Claims, the client is required to provide the control totals and balancing reports for each source conversion and approve the conversion process, financial balancing and functional requirement before the final conversion process begins. If no control totals are initially provided, the Implementation team requests the control totals from the client. If a client cannot provide the control totals, then the Implementation team requests the acknowledgment from the client that control totals cannot be provided and data should be loaded as is.

For Claims conversions, the Ventiv Technology data team typically performs 1-3 loads of trial validation prior to handing off to the client. The data team receives Trial Validation sign off from the client prior to any subsequent and final source database load. The final conversion process for Claims entails execution of the repeatable steps developed for the trial UAT, including the transfer of data to and from the client database.

IRM and Digital conversions/data loads have a constant validation via ongoing trials and the final sign off occurs prior to client go live.

Data Loading

IRM and Digital clients require data from third parties to be converted and processed into their databases on an ongoing basis. Ventiv Technology developed conversion templates to be used with various data sources. These conversion templates are deployed to specific clients where data is received. These types of conversions may require minimal customizations to the fields or code mapping.

There are other sources that require Ventiv Technology to create a custom conversion program. In these cases, Ventiv Technology requires that a specification document be completed by a member of the Implementation Team (Project Manager, Client Delivery Lead or Business Analyst) and signed off by the client. The specification outlines the mapping for the fields, mapping for the lookup values, and any special business rules and/or validations that need to be incorporated into the process. The conversion program is developed and tested by the Data Migration Analyst. The Data Migration Analyst includes balancing steps in the data load conversion program to balance to the source controls totals, if totals are provided. A further reconciliation is completed by the Project Manager/Business Analyst assigned to the Implementation Team.

The Data Migration Analyst provides the business rules and financial validation documents. The business rules output is used to identify potential issues in the client's data or load conversion program that need to be corrected. The financial validation document is used to balance back to the data provider's control total document. The conversion must be accepted by the client prior to the load being certified production ready. In some instances, clients' use of the conversion in production constitutes as signoff and acceptance.

In general, data conversion and ongoing loads fall into four main categories and depending on the type of the data loads, the setup and sign off evidence is retained as follows:

1. Non-financial standard loads retain UAT sign off
2. Non-financial custom loads retain specs (such as data mapping) and UAT sign off
3. Financial standard loads retain the business rules, financial validation, loss runs and UAT sign off
4. Financial custom loads retain specs (such as data mappings), the business rules, financial validation, loss runs and UAT sign off

Note: In instances where a client does not provide signoff, use of data conversion or load in production constitutes signoff and acceptance.

Production loads are run 24 hours a day, 7 days a week, excluding the system maintenance periods. There is a process that polls the SFTP server for files posted that need to be processed into the IRM and IRM system. There are a number of checks and validations that each file must pass before the data is actually loaded into the system. This is an automated process with error-handling logic incorporated into the process to notify specified parties via email in case of failures. If the checks and validations produce an error, the load is stopped until the issue is resolved. Transmission of data to Ventiv Technology is performed via secured protocols (e.g., SFTP, PGP or GPG).

The system continually checks for expected files. Alerts are provided to assigned personnel and the client (if requested) on load attempt, success and failure. Upon data load, the tool itself checks, based on defined parameters, for variances outside of specified tolerance levels. If variances outside these levels occur, the load would be stopped and investigated by Ventiv Technology personnel. The Data Operations Analyst reports to the Client Delivery team the variance along with any load specific details. The Client Delivery Team/Data Operations Analyst consults with the client or data source about the variance and obtains an approval before the load is allowed to run further.

Data Transmission and Storage

For IRM and Digital, data conversion templates are defined using a proprietary tool called ETL. Access to this tool is controlled with IRM user security.

SFTP servers where these files are stored is restricted to appropriate team members within the PSO organization.

For Claims, the conversion scripts are stored on a network drive, and are restricted to the appropriate team members with the PSO organization.

Access to client claims data is limited to a minimum number of individuals who have a direct business justification to access the data. Typically, this includes the Data Conversion Team members and Business Analysts. If data is received via means other than electronic transfer, such as an encrypted external hard drive, the physical media is delivered to IT, which logs, tracks and stores the data within a secure area while on site at the Ventiv Technology Data Conversion facility.

Client data that is no longer needed for conversion or implementation support is removed from the network servers. After determining that the Claims data is no longer required by the Project Manager, Business Analyst and Data Migration Analyst on the account, a help desk ticket is submitted to IT personnel instructing them which conversion databases and source files are to be removed from the conversion servers. The system is configured to automatically delete client raw data from the staging area and file servers within a specified time after the data load is received and/or placed into production.

Complementary User Entity Control Considerations

Ventiv Technology systems were designed with the assumption that certain complementary controls would be implemented by user organizations. In certain situations, the application of specific controls at user organizations is necessary to achieve certain control objectives included in this report. The users of this document should consider their internal control environment in conjunction with Ventiv Technology's control environment and the specific controls described herein. Each client must evaluate its own internal controls to determine if the Complementary User Entity Controls and procedures are in place.

This section describes other internal control structure policies and procedures that should be in operation at user entities to complement the control structure policies and procedures at Ventiv Technology. User auditors should consider whether the following policies and procedures have been placed in operation at user entities:

Control Objective 2: Physical and Logical Access

- User access requests sent to the service organization are authorized and approved.
- The designated IRM and Digital client administrator is appropriate to have administrative access in the client environment.
- IRM and Digital client user groups consist of users who are part of the client's organization. Their access can vary from administrator-level access to read-only access. All clients are responsible for defining and administering their unique security configuration. In addition, it is the client's responsibility to periodically review access for its users.
- Access to Claims application is gained through the use of individual user accounts. Their access can vary from administrator-level access to read-only access. All clients are responsible for defining and administering their unique security configuration. In addition, it is the client's responsibility to periodically review access for its users.
- When a client employee is terminated, the client administrator disables the terminated user's access within IRM and Digital or the termination is communicated to the CSR at the service organization.
- Minimum hardware and software requirements specified by the service organization are maintained by the user organization.
- Physical and logical access to the service organization's systems via terminals or PCs at user locations is restricted to authorized individuals.
- Passwords granting access to the network or through the application are kept confidential by the user organization personnel.
- Light users are employees of the client and not Ventiv Technology; thus, it is the client's responsibility to add/delete/modify light users' access within IRM. It is also the client's responsibility to review light users' access periodically.

Control Objective 3: Internet Access

- Internet firewall and extranet gateway controls are in place at the user organizations and functioning effectively.
- Remote access functionality is secure at user organizations.

Control Objective 6: Client Setup

- Instructions and information provided to the service organization from the user organization are in accordance with the provisions of the servicing agreement or other applicable governing documents between the service organization and the user organization
- Written notification of changes in the designation of user organization individuals authorized to instruct the service organization regarding activities is adequately communicated to the service organization.
- For IRM and Digital, customer implementations with customization for configuration, data and/or reporting, and data conversion and loads, user organizations perform adequate user acceptance testing.
- Clients are responsible for communicating any issues identified during user acceptance testing to the service organization and providing timely approval (explicit or implicit) of test results.
- Proper and adequate business rules are implemented to avoid situations where fraudulent activities can be performed within the application. In addition, verify that proper approvals are built into the system to provide oversight and review of transactions.
- Periodic status reports for client implementations are reviewed by the client and other stakeholders.

Control Objective 7: Data Conversion and Loading

- Data quality reports are received and reviewed by appropriate user organization personnel for completeness and accuracy. Errors in data quality are monitored and are reported to the service organization.

Control Objective 8: Transmission and Storage

- Notification of changes to the user organization's data stored at the service organization is authorized and approved by the appropriate individuals at the user organization and is adequately communicated to the service organization.
- Ensure that data provided to Ventiv Technology for database conversion is transferred in an encrypted form, through an encrypted tunnel, VPN, or file ~~l~~evel encryption.

Complementary Subservice Organization Controls

As noted in the Section III, "Description of the Ventiv Technology System Used to Manage and Control the Integrated Risk Management (IRM), Claims, and Digital Application Hosting Services" section above, Ventiv Technology utilizes colocation data center service providers ("subservice organizations") as part of delivering its overall application hosting services.

Ventiv Technology's system was designed with the assumption that controls would be implemented by the subservice organizations to implement and maintain effective internal controls. This section highlights controls that management of the service organization assumes, in the design of the service organization's system, will be implemented by the subservice organizations and are necessary to achieve the control objectives stated in management's description of the service organization's system.

The subservice organizations are responsible for:

- Implementing physical access controls in the data center to protect systems against unauthorized access, use, or modifications.
- Providing environmental control devices within the data center to protect systems.

IV. INFORMATION PROVIDED BY THE INDEPENDENT SERVICE AUDITORS

When using information produced by the service organization, we evaluated whether the information was sufficiently reliable for our purposes, including, as necessary, obtaining evidence about the completeness and accuracy of the information and evaluating whether the information was sufficiently precise and detailed for our purposes.

The type of tests that may have been performed on the effectiveness of controls detailed in the following section include:

Type	Description
Inquiry	Inquired of appropriate personnel. Inquires seeking relevant information or representation from Company Personnel were performed to obtain, among other evidential support, the following: o Knowledge and additional information regarding the policy and procedures o Corroborating evidence of the policy and procedures As inquiries were performed for substantially all controls, the test was not listed individually for every control shown in the accompanying matrix.
Corroborative Inquiry	Inquired of more than one appropriate personnel for a single test of controls. Compared responses from inquired personnel to corroborate the accuracy, consistency and completeness of responses.
Inspection	Inspected documents and records indicating performance of the controls. This included among other things: o Examination of source documentation and authorization to verify propriety of transactions and records. o Examination of documents and or records for evidence of performance, such as existence of electronic approval, signatures, or initials. o Examination of Company system documentation, such as operations manuals, flow charts, and job descriptions.
Observation	Observed the application or existence of specific controls as represented.
Re-performance	Re-performed the control, or processing of the application control, to help ensure the accuracy of its operation. The testing included, among other procedures, the following: o Obtaining evidence of the arithmetical accuracy and correct processing of transactions by re-performing independent calculations. o Re-performing the matching of various system records by independently matching the same records and comparing reconciling items to the Company's prepared reconciliation if applicable.

Control Activity	Tests of Operating Effectiveness	Test Results
Control Objective 1: Change Management Controls provide reasonable assurance that operating system, database, and application software development and maintenance is authorized, tested, and approved prior to implementation into production.		
1.1 Application system and software development and testing is performed in distinct development and test environments that are physically and/or logically separated from the production environment.	Inquired about the separate networks for the Development, QA, and Production environments. Observed sperate servers setup for development, QA, and production environments to verify that they were separate.	No exceptions noted.
1.2 The ability to implement application system and software changes is restricted to authorized personnel that are independent of the development process.	Inquired about the application and software access restrictions. Inspected a sample of application system and software changes tickets to verify that the individual migrating the change into production and not the individual involved in the development process. Inspected the appropriate active directory group and applicable change management software users to verify that only appropriate individuals could make changes to the production applications.	No exceptions noted.
1.3 When necessary, emergency changes to the supporting infrastructure follow the change management process and are authorized, tested, and approved.	Inquired about the emergency change management process. Inspected a sample of emergency infrastructure change tickets to verify that emergency infrastructure changes were authorized, tested if applicable and approved.	No exceptions noted.
1.4 Application changes are authorized, tested (if applicable) and approved by authorized personnel prior to implementation to production.	Inquired about the application change management process. Inspected a sample of application change tickets to verify that application changes were authorized, tested, (if applicable) and approved by authorized individuals prior to implementation.	No exceptions noted.

Control Activity	Tests of Operating Effectiveness	Test Results
1.5 Database, operating system, firewall, and other infrastructure changes are authorized, tested (if applicable) and approved by authorized personnel prior to implementation to production.	Inquired about the infrastructure change management process. Inspected a sample of infrastructure change tickets to verify that infrastructure changes were authorized, tested (if applicable), and approved.	No exceptions noted.

Control Activity	Tests of Operating Effectiveness	Test Results
Control Objective 2: Physical and Logical Access Control provide reasonable assurance that physical and logical access to the Ventiv Technology IRM, Digital, and Claims applications, data, computer resources and job scheduling software is limited to authorized and appropriate personnel.		
2.1 Access to Ventiv facilities is restricted to authorized personnel via key card authentication.	Inquired about facility access restrictions. Observed key card scan devices in use at the Ventiv Office entrance doors to restrict physical access to the facility. For a sample of terminated employees the auditor verified they were timely removed from the badge system	No exceptions noted.
2.2 Administrative access to the badge access system is restricted to authorized personnel. Physical access requests to the data center are documented and approved by authorized personnel.	Inquired about badge system access restrictions. Inspected the data center access list to verify that data center access is only available to authorized personnel.	No exceptions noted.
2.3 Physical access to the data center is removed as a component of the employee termination process.	Inquired about the process for removing data center access. Inspected the data center access list to verify that data center access is only available to authorized personnel.	No exceptions noted.
2.4 Data center access is reviewed on a quarterly basis. Any required changes are formally requested/submitted and follow the data center access process.	Inquired about the data center access review process. Inspected a sample of quarterly data center access reviews or verify data center access was reviewed quarterly and any required changes were formally requested/submitted and followed the data center process	No exceptions noted.

Control Activity	Tests of Operating Effectiveness	Test Results
2.5 Visitors are required to be escorted on company property.	Inquired about the process for escorting visitors. Inspected the Ventiv Information Security Policy to verify that visitors were required to be escorted on company property.	No exceptions noted.
2.6 The in scope systems are configured to authenticate users via multifactor authentication, including a unique username and password in accordance with established authentication and password standards.	Inquired about multifactor authentication and password standards. Observed Ventiv personnel authenticate to in scope systems via multifactor authentication to verify that in scope systems were configured to authenticate users via multifactor authentication. Inspected the password settings for the in scope systems to verify that password standards were configured.	No exceptions noted.
2.7 Administrator access to the in-scope systems is restricted to authorized personnel.	Inquired about administrator system access restrictions. Inspected the users with administrator access to the in scope systems to verify that administrator access was limited to authorized personnel.	No exceptions noted.
2.8 A termination ticket is completed and access is disabled and removed as a component of the employee termination process.	Inquired about the process for removing a terminated user's system access. Inspected the Active Directory listing and termination tickets for a sample of terminated employees to verify that access to the in scope systems was removed for each terminated employee.	No exceptions noted.

Control Activity	Tests of Operating Effectiveness	Test Results
2.9 Access to the applications, databases and operating systems is granted based on formal approved requests.	Inquired about the process for granting access to applications, databases and operating systems. Inspected access request tickets for a sample of new users to verify that access to applications, databases, and operating systems was granted based on formal approved requests.	No exceptions noted.
2.10 Privileged Access to the applications, databases and operating systems is reviewed on a periodic basis. Any changes required are formally requested and follow the logical access administration process.	Inquired about the privileged access request and review process. Inspected a sample of monthly and quarterly access reviews of the applications, databases and operating systems to verify privileged access was periodically reviewed and access changes were formally requested. Inspected the approval and tracking of access request changes to the in-scope systems to verify that access change was appropriate and approved.	No exceptions noted.
2.11 Access to update the job scheduler is restricted to authorized personnel.	Inquired about job scheduler access restrictions. Inspected the list of users with access to update the job scheduler to verify that access to update the job scheduler is properly restricted.	No exceptions noted.
2.12 Client data access is restricted to authorized client and Ventiv Technology personnel.	Inquired about client data access restrictions. Observed a sample of users log in to each of the in scope applications and confirmed that each application required unique login credentials and was secured by a TLS connection to restrict access to client data to clients and authorized Ventiv Technology personnel.	No exceptions noted.

Control Activity	Tests of Operating Effectiveness	Test Results
Control Objective 3: Internet Access Controls provide reasonable assurance that access to the IRM, Digital, and Claims websites is restricted and deviations from standard expected activity are identified, investigated, and resolved.		
3.1 Direct and indirect access to web facing applications from unauthenticated web browsers is restricted. The web server's configuration does not allow for direct indexing through standard search engine.	Inquired about web facing applications access controls. Observed attempts to access the web facing applications login pages through direct and indirect means to verify that the user was redirected to the standard login page of each application.	No exceptions noted.
3.2 Users are required to authenticate to the in-scope applications using a valid username and password.	Inquired about application authentication controls. Observed Ventiv personnel log into the in-scope applications to verify that users were required to authenticate using their user name and password.	No exceptions noted.
3.3 Web communication sessions are encrypted using TLS encryption.	Inquired about internet access controls. Inspected screenshots of the IRM, Digital, and Claims login screens and encryption certificates to verify that connections to web facing applications were protected using encryption.	No exceptions noted.
3.4 A firewall system is in place to filter unauthorized inbound network from the Internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall rule.	Inquired about firewall access controls. Inspected the firewall rules configuration settings to verify the firewall was configured to deny inbound network connections from the internet that were not explicitly authorized by a firewall rule.	No exceptions noted.

Control Activity	Tests of Operating Effectiveness	Test Results
3.5 A third-party security service is used to monitor the network for unauthorized network attempts. Critical alerts are sent real time to the network engineering group for follow-up and resolution. Additionally, network monitoring tools are in place to prevent unauthorized access to the network.	Inquired about the third party network monitoring and alerting service. Inspected the third party monitoring and alerting configuration settings and an example email alert to verify that critical alerts were sent real time to the network engineering group. Inspected documentation to support that alerts were followed up and resolved.	No exceptions noted.
3.6 Ongoing vulnerability scanning and testing is performed to identify known risks. Risks are assessed, and action items are created to mitigate risks.	Inquired about vulnerability scanning and testing. Inspected the vulnerability scanning reports and test results for a sample of weeks to verify that scanning and testing was performed and identified risks were assessed and addressed by management.	No exceptions noted.
3.7 Administrative access to the firewall system is restricted to authorized personnel.	Inquired about access to firewall system software and configurations. Inspected the list of users with access to the firewall system software and configurations to verify that access to the firewall system was restricted to appropriate personnel.	No exceptions noted.
3.8 Third party application penetration testing is performed annually to identify risks and vulnerabilities to the in-scope applications. Risks are assessed and action items are created to mitigate the identified risks. Development teams perform Nessus & OWASP ZAP scans prior to code being deployed to production.	Inquired about the third party penetration testing services and process for assessing and mitigating risks. Inspected the internal vulnerability scans to verify that development teams performed internal vulnerability scans prior to code being deployed to production.	No exceptions noted.

Control Activity	Tests of Operating Effectiveness	Test Results
Control Objective 4: Computer Operations Controls provide reasonable assurance that processing is scheduled, critical platforms are monitored, and deviations are identified and resolved.		
4.1 IT personnel monitor system level production job schedules when a job is implemented.	Inquired about the process for monitoring production system job schedules. Inspected examples of production job monitoring to verify production job schedules were monitored when a job was implemented.	No exceptions noted. -
4.2 Deviations in production processing are monitored via automatic alert, documented (as required) and resolved.	Inquired about the process for monitoring, documenting, and resolving production processing deviations. Inspected the centralized monitoring tool, the automated alert configuration, and examples of alerts to verify that production processing deviations were monitored, documented as required, and resolved.	No exceptions noted.
4.3 Job scheduling requests are documented, approved and processed in accordance with Ventiv Technology policies and procedures.	Inquired about the process for documenting, approving, and processing job scheduling requests. Inspected the Information Security Policy to verify that job scheduling requests are required to be documented, approved, and processed in accordance Ventiv's policies and procedures.	No exceptions noted.

Control Activity	Tests of Operating Effectiveness	Test Results
4.4 Security events and incidents are monitored, investigated, addressed, documented, and reported in accordance with Ventiv Technology policies and procedures.	Inquired about the process for monitoring, investigating, addressing, documenting, and reporting security events and incidents. Inspected the Incident Response Procedure to verify that a procedure was in place to monitor, investigate, address, document, and report security events and incidents. Inspected a list of security incidents to verify that security events and incidents were monitored, investigated, addressed, documented, and reported in accordance with the internal procedures.	No exceptions noted.

Control Activity	Tests of Operating Effectiveness	Test Results
Control Objective 5: Backups Controls provide reasonable assurance that operating systems and related data that have been identified as requiring periodic backup are backed up as scheduled.		
5.1 Data Backup Policies and Procedures have been established by Ventiv Technology Management.	Inquired about database policies and procedures. Inspected the Data Backup Policies and Procedures to verify that backup policies and procedures have been established by Ventiv Technology Management.	No exceptions noted.
5.2 Primary databases are configured to replicate to local and remote servers. (Claims, Digital, & IRM).	Inquired about the primary database replication process. Inspected backup replication settings for the primary databases to verify that primary databases were replicated locally and offsite.	No exceptions noted.
5.3 Replication time is monitored for in-scope databases, and the DBA group receives real-time alerts for deviations from the RPO and resolves them as appropriate.	Inquired about the process for monitoring database replication time, alerting, and resolving replication deviations. Inspected the in-scope database replication configurations to verify that replication time was monitored, DBA personnel were alerted about deviations and deviations were resolved when necessary.	No exceptions noted.

Control Activity	Tests of Operating Effectiveness	Test Results
Control Objective 6: Data Conversion and Loading Controls provide reasonable assurance that client data remains complete, accurate, and valid throughout the conversion process.		
6.1 Control totals that are provided by clients or third-party vendors are balanced between the source and the destination for each financial conversion.	Inquired about the process for balancing financial conversion control totals. Inspected balancing reports for a sample of clients to verify that control total reports were balanced between the source and the destination for each financial conversion.	No exceptions noted.
6.2 Conversion and data load setup is reviewed and approved by the customer.	Inquired about the conversion and data load setup review and approval processes. Inspected client sign offs for a sample of new conversions to verify that conversion and data load setups were approved by the client.	No exceptions noted.
6.3 For IRM clients, the tool automatically notifies specified Ventiv Technology contacts if a data file is not received when expected.	Inquired about the automated IRM data file verification notification tool. Inspected the data file load and email notification queries and examples of data load failure alerts to verify that the tool automatically alerted the designated Ventiv Technology contacts if a data file was not received when expected.	No exceptions noted.
6.4 For IRM clients, the LoadDef engine detects variances outside of the allowed range and alerts are sent to appropriate personnel.	Inquired about the IRM variance detection and alerting tool. Inspected the LoadDef detection and alerting configuration and an example of an email alert to verify that variances were detected and appropriate personnel were notified.	No exceptions noted.

Control Activity	Tests of Operating Effectiveness	Test Results
Control Objective 7: Data Conversion Transmission and Storage Controls provide reasonable assurance that data exchange is securely transmitted and stored data is appropriately safeguarded.		
7.1 For IRM, Digital and Claims, data transmissions are performed using secure protocols: SFTP.	Inquired about data transmission security. Inspected the data transmission settings to verify that SFTP was used for IRM, Digital and Claims data transmissions.	No exceptions noted.
7.2 For Claims, access to the conversion script library is restricted to appropriate personnel.	Inquired about conversion script library access restrictions. Inspected a listing of users with access to the Claims conversion script library to verify that access was limited to appropriate personnel.	No exceptions noted.
7.3 Access to the network file share where data is stored/processed is restricted to authorized personnel.	Inquired about network file share access restrictions. Inspected a listing of users with access to the network file share where data is stored/processed to verify that access was limited to authorized personnel.	No exceptions noted.
7.4 Customer data received on portable media is tracked via tickets and stored in a secure room while it is onsite.	Inquired about the process for tracking and securing customer data received on portable media. Inspected a sample of tracking tickets to verify that customer data transported on portable media was tracked from initial request to receipt to receipt of data.	No exceptions noted.

Control Activity	Tests of Operating Effectiveness	Test Results
7.5 Access to ETL tools are restricted to authorized personnel.	Inquired about the ETL tool access restrictions. Inspected a listing of users with access to the ETL tool to verify that access was limited to authorized personnel.	No exceptions noted.
7.6 Client raw data is deleted from the staging area and file servers 90 days after the data load is received and/or placed into production.	Inquired about the processes for deleting client raw data. Inspected the automated data deletion setting to verify that the system was configured to automatically delete client raw data from the staging area and file servers after 90 days of receipt or placing into production.	No exceptions noted.

Control Activity	Tests of Operating Effectiveness	Test Results
Control Objective 8: Client Setup Controls provide reasonable assurance that clients are set up according to their instructions and that changes to customer setup are authorized, tested, and approved by clients prior to go live.		
8.1 Statement of Work is required to be approved by the client and is stored in the document repository.	Inquired about the process for obtaining and storing client Statement of Work approvals. Inspected Statements of Work for a sample of clients to verify that the Statements of Work were approved by the client.	No exceptions noted.
8.2 Non standard implementations undergo Ventiv Technology testing and must be signed off by the client prior to go-live.	Inquired about the process for testing and obtaining client sign offs for non standard implementations. Inspected testing documentation and client approvals for a sample of clients with custom implementations to verify non-standard implementations were tested and signed off by the client prior to go live.	No exceptions noted.
8.3 The appropriate implementation closure sign off is required to be obtained from the client after the go live for that client and posted to a designated folder in the document repository area.	Inquired about the process for obtaining and storing implementation closure sign offs. Inspected the closure sign offs for a sample of clients to verify that a final sign off was provided by the client after go live.	No exceptions noted.

V. OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

The information included in Section V is presented by Ventiv Technology to provide additional information to user entities and is not part of Ventiv Technology's description of controls. The information in Section V has not been subjected to the procedures applied in the examination of the aforementioned description of Ventiv Technology's controls related to its Integrated Risk Management (IRM), Claims, and Digital application hosting services and, accordingly, AGL expresses no opinion on the descriptions contained within Section V. Note that, as with all information included in Section V of this report, the following information should be used for informational purposes only.

A. Ventiv Technology Contingency Measures

Described in this section are the contingency measures that are in place for Innovative Risk Management (IRM), Claims, and Digital hosted applications. To help determine customers' ability to conduct business with Ventiv Technology, extensive Business Continuity and Disaster Recovery plans have been developed and are in place. These plans and procedures undergo periodic review on an ongoing basis to keep them current and up to date.

Business Continuity Plan Summary

By design, all of Ventiv Technology's employees can work remotely using their laptops and cell phones for normal business processing. The same procedures and controls that are in place to manage traveling employees as well as remote home office resources are available to be utilized if needed for business continuity. The vast majority of our clients are focused on disaster recovery because it is focused on the hosting environment and the applications they are utilizing. For this reason, the majority of our focus is on disaster recovery and ensuring that we can meet our recovery time and point objectives.

Disaster Recovery Plan Summary

The Ventiv Technology Disaster Recovery Plan documents the plan of action for an event affecting the primary data center in Marietta, Georgia. The document outlines the methodology, core procedures and processes in place to ensure appropriate response to an event. The Ventiv Technology Disaster Recovery Plan is a detailed playbook containing proprietary and client confidential information and, therefore, cannot be disclosed outside of Ventiv Technology personnel. The overall objective is to document the process and methodology to protect employees and resources and to provide continued availability of solutions and services to our customers.

The keys to any Disaster Recovery plan include:

- Executive commitment
- Communication
- Continual risk mitigation
- Continual plan maintenance and testing
- Continual service improvement

Executive Commitment

The Ventiv Technology Executive Team is committed to the ongoing support and maintenance of the Disaster Recovery Plan and risk mitigation strategies described in this document. Each member of the Executive Team is part of the effort to maintain, continually communicate and enforce Ventiv Technology's process to provide a superior solution and level of comfort to its customers.

Communication

A comprehensive communication plan is included in the detailed plan documents. Email communication will remain available during an event experienced at Ventiv Technology, regardless of the event level. Email is managed and serviced outside of the Ventiv Technology data centers and environments. Phone call trees and dedicated 800 numbers are used to ensure communication between Ventiv Technology employees and client companies. All employees have copies of the call trees, and the 800 numbers are maintained.

Disaster Avoidance

Ventiv Technology has implemented redundant infrastructures to provide maximum availability of our products and services. The following items outline the core components providing as much disaster avoidance as possible.

Utility Infrastructure

- Multiple Physical POEs (points of entry) for fiber inputs into the data center.
- Redundant bandwidth carriers mean no single point of provider failure.
- Geographically stable (low disaster occurrence location in USA).
- N+1 redundant and paralleled "Hospital-grade" Caterpillar diesel generators provide utility back up for all data center operations. System ensures a power source even in the unlikely scenario that both line power and one generator fail.
- Generator backup - 24 hours of on-site fuel plus emergency refueling service to resupply in an emergency.
- Dense high capacity circuit distribution from 2N redundant Power Distribution Units and associated 2N circuit panels (A/B) prevent circuit failures or load issues.
- 24/7 Electrical circuit load monitoring and management by trained professionals
- 2N or N+1 Power Redundancy on all systems.
- 2N Liebert UPS with valve-regulated lead-acid (VRLA) batteries provide backup at full load with 100% A/B failover redundancy.
- Uninterrupted transfer of power using high capacity UPS and Automatic Transfer Switch (ATS).
- Transfer of power is completely automatic and transparent in the event of an outage.
- Regularly scheduled maintenance with certified critical equipment contractors.

Network Infrastructure

- Dual entrance facilities for telecom carrier circuits.
    - Internet Connectivity provided by two telecom carriers
    - Each carrier utilizes a separate entry point into the building
    - Each carrier is serviced by a different central office (CO)
    - A single carrier can handle full network traffic load
- Redundant network infrastructure
    - Firewalls
    - Routers

- Network Traffic Managers
- Core Switches

Server Infrastructure

Each layer of the server infrastructure is comprised of redundant, fault tolerant components. There are multiple web servers, application servers and database servers that work in parallel, but can also service the load in the event of a failure of any component. The redundancy within the server infrastructure is capable of withstanding multiple concurrent failures.

Storage Infrastructure

- A high availability and encrypted Storage Area Network and storage sub-system have been implemented to mitigate any loss of data due to a single or multiple disk failure.
- Ventiv Technology has also implemented additional safeguards to mitigate the loss of data. These include:
  - Continuous replication of data to storage sub-system located at secondary data center site
  - Creation of local "shadow" copies to allow for quick retrieval of backup data
  - Creation of physical tapes and off-site storage as a recovery point of last resort

Data Center Protection

- Ventiv Technology also considers the physical protection of the data center within its continuity plans.
- The data centers is protected in the following manner.
  - Security guard onsite 24x7x365 monitoring and controlling physical access
  - 24x7x365 automated monitoring for fire/smoke/water/temperature
  - FM 200 fire suppression system
  - Two stage entry to data center to prevent tailgating
  - Biometric and electronic badge required for data center access
  - 90+ day CCTV recorded monitoring

Monitoring

24/7/365 monitoring of generator systems at Network Operations Center -NOC Fail-safe alarm system to prevent false discharge or tampering of system when armed.

Database

Oracle Data Guard technology is utilized to create both local and disaster recovery physical standby databases. These standbys provide backup for logical as well as physical issues and are a proven method for providing effective data backup and recovery.

Disaster Recovery

In the event that the primary data center facility is lost and unusable due to any type of disaster the overall business continuity plan is put into action. The overall plan establishes the procedure for the short term housing for employees, recovery of personal computing resources and facility related issues. The recovery of the client facing applications and data will follow the Disaster Recovery Plan to move the secondary site to a production role.

Second Data Center Site

- Ventiv Technology has established a secondary data center in Oakland, CA. The equipment is housed within a secured area in an industry standard data center facility. The facility is located in close proximity to the Ventiv Technology team in San Ramon, CA.
- The second data center can be referred to as a "hot" site. Equipment needed to run critical customer facing services is staged, operational, maintained and monitored like the primary site. The site is designed to require a minimal amount of configuration and setup to be designated and operating as the primary site. The steps associated with configuration and setups comprise our test plan.
- The site is configured with multiple telecom providers that can quickly establish and expand capacity during a disaster event beyond the static connectivity already in place.
- Ventiv Technology has replicated all core servers and network infrastructure in the second site to mirror the primary facility.
- A second SAN and disk sub-system are in place and receive the replicated data continually.
- The Recovery Time Objective (RTO) is 24 hours
- The Recovery Point Objective (PRO) is 12 hours

Auditing and Plan Testing

The Disaster Recovery Plan is in constant testing. With the replication of the data locally and to the secondary site, Ventiv Technology knows within minutes if the replication is not occurring and can respond accordingly before a disaster occurs. Rigorous process controls have been implemented, which are subject to not only internal audits, but some are also included in our ISO27001:2013 certification which is performed by an independent external audit firm.

In addition, a full disaster recovery test is performed at least once each calendar year to validate the entire solution. Testing involves the actual restoration of services at the secondary site and the Quality team performing regression testing. Ventiv Technology produces an Executive Summary report available to clients after each test exercise.