CONVERGYS

System and Organization Controls (SOC 3) Report

Description of Convergys Corporation's Data Center and Call Center Operations relevant to Security, Availability, and Confidentiality

For the Period October 1, 2016 to September 30, 2017

Ernst & Young LLP
1900 Scripps Center
312 Walnut Street
Cincinnati, OH 45202

Tel: +1 513 612 1400
Fax: +1 513 612 1730
ey.com

Independent Service Auditor's Report

The Management of Convergys Corporation

Approach:
We have examined management's assertion that Convergys Corporation maintained effective controls to provide reasonable assurance that:

- the Convergys Corporation's Data Center and Call Center Operations System was protected against unauthorized access, use, or modification to achieve Convergys Corporation's commitments and system requirements
- the Convergys Corporation's Data Center and Call Center Operations System was available for operation and use to achieve Convergys Corporation's commitments and system requirements
- the Convergys Corporation's Data Center and Call Center Operations System information is collected, used, disclosed, and retained to achieve Convergys Corporation's commitments and system requirements

during the period October 1, 2016 through September 30, 2017 based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100A, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Convergys Corporation's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Convergys Corporation's relevant security, availability and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Convergys Corporation's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations:
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability and confidentiality are achieved.

Building a better working world

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion:
In our opinion, Convergys Corporation's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability and confidentiality.

Ernst & Young LLP

December 12, 2017

CONVERGYS

Corporate Headquarters
201 East Fourth Street
Cincinnati, OH 45202

Management's Assertion Regarding the Effectiveness of Its Controls Over the Data Center and Call Center Operations System Based on the Trust Services Principles and Criteria for Security, Availability and Confidentiality

December 12, 2017

We, as management of, Convergys Corporation are responsible for designing, implementing and maintaining effective controls over the Data Center and Call Center Operations System (System) to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in Security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

We have performed an evaluation of the effectiveness of the controls over the system throughout the period October 1, 2016 to September 30, 2017, to achieve the commitments and system requirements related to the operation of the System using the criteria for the security, availability and confidentiality (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this evaluation, we assert that the controls were effective throughout the period October 1, 2016 to September 30, 2017 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Convergys Corporation's commitments and system requirements
- the System was available for operation and use, to achieve Convergys Corporation's commitments and system requirements
- the System information is collected, used, disclosed, and retained to achieve Convergys Corporation's commitments and system requirements

based on the Control Criteria.

Our attached description of the boundaries of the Data Center and Call Center Operations System identifies the aspects of the Data Center and Call Center Operations System covered by our assertion.

Convergys Corporation Management

Overview of Convergys Corporation

Convergys delivers consistent, quality customer experiences in 58 languages and from more than 150 locations around the globe. Convergys partners with its clients to improve customer loyalty, reduce costs, and generate revenue through a portfolio of capabilities, including customer care, analytics, tech support, collections, home agent, and end-to-end selling. Convergys is committed to delighting its clients and customers, delivering value to shareholders, and creating opportunities for Convergys' employees, 130,000-strong in 33 countries around the world. Visit www.convergys.com to learn more about Convergys.

Solutions

Agents

Convergys' agents deliver superior care with their full range of contact center services delivered via phone, email, and chat. Convergys provides solutions across the customer lifecycle, including:

- Customer Service
- Customer Retention
- Technical Support
- End-to-End Selling
- Complex Device Support
- Back Office
- Collections
- Quality Assurance
- Direct Response
- Home Agent

Analytics

Convergys' more than 400 analytics professionals apply techniques that improve the cross-channel experience and customer loyalty, including:

- Post-Contact Surveys
- Relational Loyalty
- Segmentation and Profiling
- Repeat Call Analysis
- Agent Path Analysis
- Agent Performance Management
- Customer Interaction Assessment
- Chat Optimization
- Propensity Modeling
- GIS Mapping
- Voice Analytics

Technology

Convergys' innovative contact center technology solutions include:

- Personalized Selling
- Campaign Management
- Personalized Care
- Email
- Chat
- Intelligent Self-Service
- Collections
- Retention
- Telco Provider Solutions
- Cloud Based Dialer
- Rapport Builder
- Automated Surveys
- Lead Capture
- Voice Analytics

Sustained Competitive Advantage

Quality Delivery

- Global operating model
- Metrics that matter
- Cost effective and consistent service

Comprehensive Solutions

- Breadth and depth of services
- Global capacity and work-at-home
- Analytics and technology

Close Client Engagement

- Account management approach
- Understand unique client needs
- Multiple languages
- Strong operational capability and culture

Overview of Services Provided and Components of the System

Convergys provides agent based call center services to its customers from call center locations across the world. The data center operations include services such as hosting operations, building administration, environmental controls and physical security for the servers and networking equipment hosted at the data centers.

Convergys maintains an intranet portal that houses the company's general information, Human Resources (HR) policies and procedures, system descriptions of all in scope systems and resources, and employee communications. This portal is made available to all employees who require access to these documents. Organizational structure is also made available to employees on the HR portal. Convergys' Data Center and Call Center Operations consists of the following five components:

- Infrastructure – The physical and hardware components of the system (facilities, equipment, networks, and telecommunications infrastructure) except for co-location data centers.
- Software – The programs and operating software of the system (systems, applications, and utilities).

- People – The personnel involved in operating and using the system (developers, operators, users, managers and functional support teams).
- Procedures – The automated and manual procedures involved in administering and operating the system.
- Data – The information used and supported by the system (transaction streams, files, databases, and tables).

Infrastructure

Convergys Corporation's seven data centers, six of which are co-location data centers, house all infrastructure including servers, storage components, firewalls, Intrusion Detection and Prevention System (IDPS), and backup systems that support the services Convergys provides to all clients. Convergys Data Center Operations are supported by the company's Information Technology Security Framework, which is comprised of the following focus areas:

- Vulnerability management
- Penetration testing
- Security information event management (SIEM) tools
- Security Operations Center (SOC)
- Advanced persistent threat (APT) tools
- Security education training and awareness (SETA)
- Disaster recovery and business continuity
- Physical security technology and safeguards
- Change management

Convergys agents have to connect to the Convergys network and authenticate themselves using their assigned unique user ID and password prior to being granted access to infrastructure and other applications and systems. Customer calls to Convergys agents are generally routed through Convergys owned and managed PBX systems. Convergys is responsible for availability of Convergys owned systems and data, including system backups, monitoring of its systems, and identifying and resolving problems. Convergys Call Center Operations are supported by the company's Desktop Security Framework, which is comprised of the following focus areas:

- Logging, host based Intrusion Prevention System (IPS), File Integrity Monitoring
- Antivirus/Malware
- Data Loss Prevention

Software

In addition to the hardware controls, Convergys also utilizes intrusion prevention/detection monitoring, antivirus, malware applications and operating systems to protect the security, availability, and confidentiality of sensitive data. Network Intrusion Detection/Prevention Systems and Data Security Redundant firewalls are in place on the network perimeter, in conjunction with network intrusion prevention/detection on internet-facing and some internal-facing network segments, to protect the network, hosts, and applications from intrusion. Convergys' architecture team develops firewall hardening standards by using firewall build documents. Log files are archived using our SIEM system, which is engineered to collect, monitor, analyze, and report on security event-related activities throughout the IT infrastructure. Convergys' Security Operations Center (SOC) monitors security logs and alerts generated by the SIEM tool.

Safely implementing security patches without compromising service to clients is the focus of the patch/network team. Patches designated as critical/high vulnerability are implemented first, and then the patch/network team applies patches designated as medium/low risk. Testing is performed on all patches to determine the potential impact to production systems. Once testing is complete and patches are approved, patches are scheduled for production via our Technical Change Management Process.

Business applications used by Convergys' agents and related processes and controls are not in scope of this report.

People

The following functional teams at Convergys support the Business Process Outsourcing (BPO) services operations and technology infrastructure:

- Data Network Engineering – Responsible for supporting a scalable, secure and efficient technology infrastructure
- Voice Network Engineering – Responsible for programming and telecommunications support to monitor and assist with all VoIP (voice over internet protocol) and telecommunication services
- Call Center Site Operations – Responsible for call handling of prospective customers, handling customer inquiries, and promoting the sale of products and/or services
- Quality – Responsible for evaluating calls in order to provide exceptional customer service and technical resolution, and to deliver feedback and coaching to Call Center Operations personnel
- Security – Responsible for the security technologies, event monitoring and incident response

Convergys believes that helping employees understand the company's business and philosophy is critical in creating a more motivated and productive work environment. An employee's immediate manager is considered the primary communication link for company information and encourages open communication at all levels, particularly between employees and their managers. Convergys believes it is important to provide timely, updated and accurate information on policies, programs, activities and decisions to employees. The company provides consistent information, uses the most efficient distribution channels available, and maintains effective communication vehicles to support and facilitate an effective control environment.

Convergys has developed an IT policies training module as part of its security awareness training to help ensure that employees of the organization are aware of and adhere to controls put in place to preserve and protect the investment in information and to:

- Help ensure security, confidentiality, processing integrity and availability
- Prevent unauthorized use/disclosure for commercial or malicious purposes
- Foster compliance and help ensure operational procedures exist for specific legal regulations such as Payment Card Industry (PCI) Security Standard, Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), and industry standards relating to data privacy and information security
- Reduce the risk of loss by accidental or intentional means
- Preserve Convergys' rights in the event of such a loss

The training module applies to all company employees, contractors, vendors and other individuals who have access to company information or the company's electronic communications systems. All individuals or entities using company information, connecting to its network or other IT infrastructure are required to adhere to the IT policies.

Procedures

Convergys has documented policies and procedures that support the management, operations, monitoring and controls over data center operations and call center security. All employees are expected to adhere to Convergys policies and procedures. Specific examples of relevant policies and procedures include, but are not limited to, the following:

- Policy Management and Communication
- System Security
- Network Operations
- Security Patch Management
- Technical Change Management
- Data Backups

- Data Classification
- Incident Response and Reporting

Data

Data, as defined by Convergys, and relevant to Convergys' Data Center and Call Center Operations System, includes the following:

- Security logs and reports
- System files
- Error logs

Security logs and reports are generated by network devices, security appliances and other tools used by Convergys. Access to and availability of these reports is limited by job function. Reports delivered externally will only be sent using a secure method—encrypted email, secure FTP, or secure intranet sites.

Subservice Organizations

Convergys utilizes multiple co-location providers including ViaWest, Inc., T-System, CyrusOne, ATT, and Verizon. The co-location services include hosting operations (e.g., facility and data center management), environmental safeguards for the facility as well as building maintenance services. Convergys requires subservice organizations to adhere to Convergys internal policies, procedures, and other applicable regulations. Convergys obtains third party System and Organization Control (SOC) reports from these subservice providers on an annual basis. The organizations are as follows:

- ViaWest – Richardson, Texas and Aurora, Colorado
- T-System – Jacksonville, Florida
- Cyrus One – Cincinnati, Ohio
- ATT – Ashburn, Virginia
- Verizon – Denver, Colorado

Convergys management evaluates the SOC reports from each co-location data center and evaluates the defined complementary user entity controls (CUECs) to confirm that Convergys has sufficient controls in place to address the CUECs. Convergys controls are validated by management on an annual basis.

Controls in place at these organizations are not included in the scope of this report; however Convergys management has identified controls at Convergys that address the risks of the services provided by the co-location data centers. These Convergys controls are identified and included within the scope of this report.

Scope Exclusion

Convergys completed an acquisition of a German company, buw, on August 1, 2016. All facilities within the former buw entity are not included in the scope of this report.

Business applications used by Convergys' agents and related processes and controls are not in scope of this report.