Empowering the Financial World

FIS

FIS Technology Centers

System and Organization Controls (SOC) for Service Organizations Report
Relevant to Security
for the period from January 1, 2020 to September 30, 2020

Grant Thornton

Report of Independent Service Auditors issued by
Grant Thornton LLP

Contents

GRANT THORNTON LLP
Grant Thornton Tower
171 N. Clark Street, Suite 200
Chicago, IL 60601-3370

D +1 312 856 0200
F +1 312 565 4719

I. Report of Independent Service Auditors

Board of Directors and Shareholders
Fidelity Information Services, LLC

Scope

We have examined Fidelity Information Services, LLC's (FIS) accompanying description of its FIS Technology Centers system titled "Fidelity Information Services, LLC's Description of its System and Controls" (description) throughout the period January 1, 2020 to September 30, 2020 (the "specified period"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria") and the suitability of the design and operating effectiveness of the controls stated in the description throughout the specified period to provide reasonable assurance that FIS' service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The information included in Section V of this report, "Other Information Provided by Fidelity Information Services, LLC," is presented by management of the Company to provide additional information and is not a part of FIS' description. Information about management's responses to testing exceptions has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of the controls to achieve the Company's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

FIS uses Digital Realty, a subservice organization, for hosting services and for managing infrastructure services and operations. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at FIS, to achieve FIS' service commitments and system requirements based on the applicable trust services criteria. The description presents FIS' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of FIS' controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

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

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

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

- obtaining an understanding of the system and the service organization's service commitments and system requirements;
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

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

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

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

Description of tests of controls
The specific controls tested and the nature, timing, and results of those tests are listed in Section IV of this report.

Opinion
In our opinion, in all material respects,

a. The description presents Fidelity Information Services, LLC's FIS Technology Centers system that was designed and implemented throughout the period January 1, 2020 to September 30, 2020, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period January 1, 2020 to September 30, 2020, to provide reasonable assurance that Fidelity Information Services, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Fidelity Information Services, LLC's controls throughout the period January 1, 2020 to September 30, 2020.
c. The controls stated in the description operated effectively throughout the period January 1, 2020 to September 30, 2020, to provide reasonable assurance that Fidelity Information Services, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Fidelity Information Services, LLC's controls operated effectively throughout the period January 1, 2020 to September 30, 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 FIS, user entities of FIS' FIS Technology Centers system during some or all of the specified period, business partners of FIS subject to risks arising from interactions with the FIS Technology Centers system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Grant Thornton LLP

Chicago, Illinois
December 4, 2020

601 Riverside Avenue, Jacksonville, FL 32204
www.fisglobal.com

II. Fidelity Information Services, LLC's Assertion

We have prepared the accompanying description of Fidelity Information Services, LLC's (FIS) FIS Technology Centers system (the "System") titled "Fidelity Information Services, LLC's Description of its System and Controls" throughout the period January 1, 2020 to September 30, 2020 (the "specified period") (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the System that may be useful when assessing the risks arising from interactions with FIS' system, particularly information about system controls that FIS has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

FIS uses Digital Realty, a subservice organization, for hosting services and for managing infrastructure services and operations. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at FIS, to achieve FIS' service commitments and system requirements based on the applicable trust services criteria. The description presents FIS' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of FIS' controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with related controls at FIS, to achieve FIS' service commitments and system requirements based on the applicable trust services criteria. The description presents FIS' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of FIS' controls.

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

A. The description presents the System that was designed and implemented throughout the specified period, in accordance with the description criteria.

B. The controls stated in the description were suitably designed throughout the specified period to provide reasonable assurance that FIS' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the specified period, and if the subservice organization and user entities applied the complementary controls assumed in the design of FIS' controls throughout the specified period.

C. The controls stated in the description operated effectively throughout the specified period to provide reasonable assurance that FIS' service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of FIS' controls operated effectively throughout the specified period.

III. Fidelity Information Services, LLC's Description of its System and Controls

A. Scope and Purpose of the Report

This report describes the control structure of Fidelity Information Services, LLC (FIS or the "Company") as it relates to its FIS Technology Centers system (the "System") for the period from January 1, 2020 to September 30, 2020 (the "specified period") for the Security trust services criteria (applicable trust services criteria). This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of the Company, user entities of the Company's System during some or all of the specified period, business partners of the Company subject to risks arising from interactions with the System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding. This report is not intended to be, and should not be, used by anyone other than these specified parties.

The description, based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), is intended to provide report user entities, business partners, practitioners, and regulators with information about the System, particularly system controls intended to provide reasonable assurance that FIS' service commitments and system requirements were achieved based on the trust services criteria relevant to the applicable trust services criteria set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). It was prepared taking into consideration the attestation standards established by the American Institute of Certified Public Accountants (the "AICPA"). As this description is intended to focus on features that may be relevant to the internal control of FIS' customers and other specified parties, it does not encompass all aspects of the services provided or procedures followed by FIS.

It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. The internal control structures at the Company are not designed to compensate for any weaknesses that may exist if the internal control structure at a user organization is ineffective.

B. About FIS

FIS is a leading provider of technology solutions for merchants, banks and capital markets firms globally. Our 55,000 people are dedicated to advancing the way the world pays, banks and invests by applying our scale, deep expertise and data-driven insights. We help our clients use technology in innovative ways to solve business-critical challenges and deliver superior experiences for their customers. Headquartered in Jacksonville, Florida, FIS is a Fortune 500® company and is a member of Standard & Poor's 500® Index.

Solutions Overview

FIS provides open, integrated solutions with the scalability to leverage multiple technologies. The Company's goal is to deliver high value to its customers when combining software applications and delivery in one of several types of outsourcing arrangements, such as an application service provider, facilities management processing, or an application management (service bureau) arrangement. The Company delivers individual applications through a software licensing arrangement. Based upon the knowledge gained through the foregoing arrangements, some clients also use the Company to manage their IT operations without being provided with any of its proprietary software.

International

FIS provides solutions on a global basis in both licensed and outsourcing models. It employs resources in global operating centers throughout Latin America, Europe, the Middle East, Africa, Asia, and Australia.

Global Positioning

The Company's international operations leverage existing domestic applications and provide services for the specific business needs of customers in targeted international markets. Services are delivered from operations centers around the world. Product and service offerings include a range of financial and payment processing software and services. The Company's services include outsourced card issuer services and customer support, item processing, and retail point-of-sale (POS) check warranty services. The Company's services also include outsourced core bank processing arrangements, application management, software licensing and maintenance, facilities management, and consulting services.

A suite of channel applications enables international clients to deliver customer service by integrating the front- and back-office operations for greater efficiencies, service, and agility in reacting to new market opportunities. The Company's solutions come with a range of value added services to provide an end-to-end solution or single point applications. Check image processing enables clients to reduce the costs of handling paper, while the Company's merchant solutions portfolio supports retail payments.

Australasia

The Company has a center of excellence for card and payment processing based in the region providing processing services to clients in a number of markets. The Company's processing center in the region was established in 2001 and is utilized to provide processing for nearly 10 million credit, debit, and loan accounts.

Europe, Middle East, and Africa

The Company's largest international region, Europe, Middle East, and Africa (EMEA), delivers a range of products and services to clients from Johannesburg to Helsinki. EMEA customers look to the Company to deliver core banking solutions in both licensed and outsourcing models; card processing for debit, credit, and prepaid products; and payment switching solutions that sit at the center of a number of national switches. Company products can be found delivering core banking solutions to multinational clients across multiple locations from a single software instance. The Company utilizes specialized country specific banking solutions for markets like Germany where banking regulation demands specialist solutions, as well as outsourced loan processing on a large scale, and loan syndication solutions for commercial applications. The Company also provides merchant solutions within the region, including check warranty services and merchant acquiring services. All these services are backed-up by a range of value added services from call center solutions to collections management.

Latin America and Caribbean

Clients within the Latin America and Caribbean (LACB) region rely on the Company to deliver services including core banking, loan origination, card processing, and transaction switching. The processing centers in the region provide outsourced services for payment processing and core banking. The processing center in Mexico City delivers loan processing services for millions of loan accounts. In Brazil, Company software is used to acquire the majority of merchant transactions and one major

retailer has deployed a Company solution to expand its national footprint by delivering bank teller services in hundreds of store locations.

C. Internal Control

Control Environment

The Company's control environment provides discipline and structure for all aspects of internal controls, fosters shared values, and promotes teamwork to meet corporate-wide objectives. The control environment scope of this report covers Human Resources (HR), Security, Operations, Risk Management, and policies and procedures within these business functions.

The Company's control environment influences the way that the business structures activities, establishes its objectives, and assesses its risks. It also influences controls and monitoring procedures within the Company.

An effective control environment is created by establishing controls surrounding the processing of information and by developing policies which promote adherence to the requirements of the control environment. The elements of the control environment include, but are not limited to:

- Integrity and Ethical Values,
- Organizational Structure,
- Enterprise Policies and Standards,
- Assignment of Authority and Responsibility, and
- Human Resources' Policies and Standards.

Integrity and Ethical Values

The Company communicates expectations of integrity and ethics through the statement of corporate values, which requires employees to be open, honest, ethical, responsive, and knowledgeable.

The FIS Employee Handbook, which contains the Code of Business Conduct and Ethics, states the Company's expectations related to integrity and ethics. In order to establish and maintain an effectively controlled organization, the Company stresses the importance of proper employee conduct. As stated within the FIS Employee Handbook, failure to comply with these policies results in corrective action by management. The Code of Business Conduct and Ethics informs employees that violations may result in disciplinary action and provides employees with resources for reporting suspected code violations. Also, it guides employees on proper conduct and gives specific examples of unacceptable behavior as well as potential consequences.

Management monitors employees' compliance with the Code of Conduct through monitoring of customer and employee complaints and through the use of an anonymous third-party administered ethics hotline. The results of the compliance and Code of Conduct monitoring are communicated to the Audit Committee on a quarterly basis. Consequences for non-compliance of job responsibility and security policies, up to and including termination, are addressed within the FIS Employee Handbook which is made available to all new employees upon hire and to existing employees on the Company intranet.

Organizational Structure

The Company's organizational structure provides the framework for defining key areas of authority and responsibility, as well as for establishing lines of reporting. The Company is designed as a vertical structure, with the business lines reporting upward to the Chief Executive Officer (CEO). The Chief Security Officer (CSO) and the Chief Risk Officer (CRO) report independently from operations. The Chief Audit Officer (CAO) reports directly to the Audit Committee of the Board both functionally and administratively.

Each Company division is supervised by members of Executive Management who report to the Chief Operating Officer (COO) of their respective division. Periodic meetings (Business Performance

Reviews) occur in which divisional leaders meet with Executive Management to keep them informed of business matters. The topics include operational issues and customer and sales prospect updates.

Additional business functions exist which are shared by these divisions. Risk and Compliance, Sales and Marketing, Operations Service Delivery (OSD), Human Resources, Accounting, and Corporate Development are run by the corresponding members of the Executive Management team who report directly to the CEO.

The Management Committee is comprised of executives who set and manage the strategic plan of the Company, including establishing the annual operating and capital plan and managing the execution of critical initiatives.

Enterprise Policies and Standards

Policies are any rules or set of rules which require or guide action. Policies are designed to promote the conduct of authorized activities in an effective and efficient manner and are intended to reduce risk and to safeguard Company resources. Policy Owners are required to review, update, and maintain their assigned policies and standards per the review cycle requirements established by the Enterprise Policy Office. Additionally, during the policy review cycle the policy owner must ensure that the policy content conforms with changes in business objectives, risk appetite, applicable laws and regulations, or industry requirements.

Global Security Services is responsible for reviewing, updating, and monitoring the integrity of security policies. Specific responsibilities for the security program are outlined within the Information Security Policy. Corporate Compliance is responsible for the Records Management Policy. The Policy Review Committee serves as the governance body that is responsible to vet, review and provide feedback on corporate policy and standard proposals prior to publication and management of the policy exception process.

Vendor Risk Management

The Vendor Management program is designed to provide consistent management and oversight for third-party vendors. A policy exists that defines requirements for due diligence on vendors with which the Company contracts. The policy dictates that the extent and nature of due diligence performed is dependent on the type of vendor. Ongoing monitoring and oversight of the vendor relationship is dictated by the type of vendor and inherent risk and is pursuant to the FIS Vendor Risk Management Policy.

Either a member of the Legal Department and/or a member of the Procurement Department is responsible for the review of all third-party contracts and for confirming that any third-party contracts include applicable security practices and commitments. On an annual basis, management evaluates the vendors who have access to confidential data or who perform a managed service related to the operations of the System and determines their risk-rating based on their level of access and the sensitivity of data. Based on the risk-rating, the Company either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 Type 2 reports, or the third party is subjected to continuous monitoring controls.

Global Business Resilience

The Board of Directors is responsible for overseeing the Global Business Resilience Program (GBR Program) which monitors the integrity of the Global Business Resilience Policy. Policy was developed in recognition of the commitment to maintain a global resilience program to oversee the Company's ability to provide adequate business and technology recovery plans, capabilities to manage recovery of operations, identification of resiliency risks, and rapid response during an unplanned disruption.

The GBR Program consists of three (3) disciplines:

- Crisis Management (CM) provides command and control for life safety and business-based incidents;

- Business Continuity Management (BCM) prepares for the continuation and/or restoration of business processes; and
- IT Disaster Recovery (ITDR) maintains the necessary ongoing recovery capabilities within IT Services and their supporting components.

The GBR Program is designed to provide guidance and direction to response and recovery team members, business units and general staff and provides oversight for a “top down” corporate-wide approach. A policy and standard exist to define the framework for the safeguards and procedures designed to ensure that critical and essential Company business activities can be maintained during a disruption by implementing controls that:

- Safeguard life, information, and assets of the Company, respectively;
- Ensure continuity of operations conforms to applicable regulatory, insurance and ethical business practices;
- Minimize the impact of unplanned disruptions on our employees, stakeholders, and clients to whom services are provided; and
- Support and agree with the Company's tactical and strategic business plans set by Executive Management.

Assignment of Authority and Responsibility

The Company strives to create accountability and awareness throughout all levels of the organization. The extent of accountability includes assignment of authority and responsibility for operating activities and establishment of reporting relationships and authorization protocols. In order to provide high-quality products and services to its clients, Company management validates that people with the required skill sets are placed at each position throughout the organization. Further, the Company makes available training to prepare employees to perform their job functions.

The Company uses a formal structure for employee assignments which includes written job descriptions that contain job requirements, job-related competencies, and business and professional competencies. Assignments are customized through goal setting, periodic reviews, and updates by management. The Company has separated incompatible duties to help reduce the risk of error or unauthorized activity. For instance, the authorization, recording, custody of assets, and control functions are segregated among different employees to reduce the potential of fraudulent activity. Supervisory positions, including defined approval levels, exist within each functional component of the Company to provide adequate supervisory control of operations.

Human Resources’ Policies and Standards

The mission of Human Resources is to hire quality employees and sustain the wellness of all Company employees. HR is actively involved in the hiring process, administration of employee benefits, development of employee education, and management of the performance evaluation process.

The Company has formal personnel policies and procedures addressing screening, hiring, transfers, and employee terminations. Organizational structure and job descriptions define an employee’s assigned responsibilities and reporting. Thorough screening throughout the hiring process increases the assurance that potential employees are qualified for the responsibilities of their positions. Offers of employment are contingent upon the satisfactory completion of a pre-employment background screening. New personnel background checks include, but are not limited to, a criminal record check, global sanctions and enforcement check, SSN trace and validation, credit check, education verification, employment history, and a drug test, where applicable. Background checks, including a drug screening, are performed for all new contractors prior to employment. The results of the background drug and credit screens are reviewed by HR to determine final employment eligibility.

New hires complete required paperwork in Workday and completed forms and acknowledgements are also stored in their documents folder in Workday.

The Company utilizes training and monitoring to prepare employees to perform their job functions. Company employees are required to participate in annual security awareness training, which includes

information regarding the process to notify members of the Information Security Department of possible security breaches and the limitation on the use of information systems. New employees participate in an orientation program introducing them to the Company, its functions, and job-specific training. Training may include on-the-job training, seminars, and internal and external online courses.

The employee's job responsibilities are reinforced through on-the-job training and specialized development programs such as supervisory skills training. With an emphasis on ongoing feedback, managers and employees have quarterly connects to stay connected and aligned on performance and development. The year-end review is also performed to evaluate performance. Connects are done online. In order to provide uninterrupted service during high volume periods, cross-training of employees is also performed.

An Employee Termination Checklist is used to determine if necessary considerations are addressed. This list includes retrieving Company property such as mobile phones, keys, security badges, and credit cards. Personnel policies require immediate removal of employees who have been involuntarily dismissed. Building and information security officers are notified of terminations and transfers.

Risk Assessment

FIS has established corporate functions to help ascertain that enterprise risk and compliance is properly prioritized, assessed, monitored for change, and reported accurately. These enterprise programs help the organization meet emerging risks and expected requirements through adapting and evolving with industry trends. Individual business units are responsible for applying the risk assessment process to their business activities, the results of which establish the risks for which controls need to be identified. To the extent that the risks relate to internal control over financial reporting, control objectives are established and are described within the relevant SOC 1 report. If the risks relate to the trust services categories, controls are established to achieve the applicable trust services criteria and are described within the relevant SOC 2 report.

During the annual risk assessment process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors which may threaten the achievement of business objectives and/or impact security. The potential threats to system objectives are updated based on these reviews.

The Company's annual risk assessment includes an assessment of fraud risk and considers opportunities for unauthorized acquisition, use, or disposal of assets; altering the Company's reporting records; committing other inappropriate acts; and the threats and vulnerabilities which could arise specifically from the use of IT and access to information.

Audit and Risk Committees of the Board

The FIS Audit Committee of the Board (Audit Committee) and the FIS Risk and Technology Committee of the Board (Risk Committee) assist the Board of Directors in the oversight and integrity of the Company's financial statements, compliance with legal and regulatory requirements, and the performance of the Company's internal audit, enterprise risk management, and information security functions. The Audit Committee also oversees the independent registered public accounting firm's qualifications and independence. Management from finance, compliance, risk, internal audit, and information security provide quarterly updates of their program structure, annual plans, and/or strategy for approval by their respective Committee. In addition, risk management, internal audit, and information security provide quarterly metric reporting on the status and impact of enterprise developments and strategic initiatives.

A Charter has been adopted by the Audit Committee and Risk Committee to guide each committee in the exercise of their respective responsibilities. The Audit Committee Charter requires it to oversee the functions of Internal Audit.

Executive Risk and Technology Committee

The Company has established an Executive Risk and Technology Committee (ERTC), which is comprised of members of Executive Leadership and their designees with the exception of the

Chairman, President and Chief Executive Officer. The Chairman, President and Chief Executive Officer is an invitee and the escalation point for Committee matters. The purpose of the Committee is to provide Executive Management oversight of the Company's overall operational, information security, compliance, credit, regulatory, strategic, reputation, technology, and other risks (collectively, the "Enterprise Risks").

The ERTC positions the corporation to comply with current industry requirements and practices related to program structure, Board oversight, and overall transparency. The Committee provides a structure and process for management to demonstrate its risk management focus through various risk programs: Policy and Governance, Controls Validation and Product Compliance, Enterprise and Operational Risk, Regulatory Relations, and Technology Shared Services. These programs help the organization meet emerging risks and expected requirements through adapting and evolving with industry trends.

Compliance

The Corporate Compliance Department is responsible for both enterprise, as well as product and services, compliance. Corporate Compliance is responsible for ensuring the Company complies with the applicable laws and regulations for the areas in which it operates, as well as ethics, sales and marketing, etc. The Department is also responsible for the oversight of certain business units and products that must directly comply with applicable regulations. Software and other processing services used by its clients are also under the oversight of the Corporate Compliance Department. The Corporate Compliance Department supports the various roles, responsibilities, and procedures for addressing new or amended federal regulations that impact applicable Company products and services.

Corporate Compliance is responsible for monitoring applicable regulations and for confirming that product features enable clients to comply with those regulations. Corporate Compliance interfaces with internal and external areas to assess the impact of change in regulatory requirements on Company products/services and to address identified regulatory issues related to Company products. When federal regulatory changes require application or product/service changes, Corporate Compliance works with application, product, or service teams to initiate a project to perform the required changes. Corporate Compliance also works with these teams throughout the design, modification, testing, and implementation phase of the project to help meet the necessary regulatory requirements and deadlines.

Strategic Initiatives

FIS is continuously making enhancements in the areas of their corporate functions. The Company has implemented several security measures within the organization designed to improve their Information Security and Risk Management departments. In addition, the Company has applied an organizational structure that provides the Chief Security Officer (CSO), Chief Risk Officer (CRO), and Chief Audit Officer (CAO) with the authority to establish and enforce security across the organization. The Company has a process for oversight of the Risk Management and Information Security functions and monitoring and resolution of Information Security-related risks. The Company has also formalized the Risk Management function to define roles and responsibilities and has implemented a risk assessment process.

Control Activities

FIS' selection, development, and deployment of controls are primarily addressed by the Company's policies and procedures and are described within the Company's SOC reports. The relevant system descriptions and controls are detailed in Sections III and IV of these reports.

The following general control framework is considered relevant for the assessment:

Application Controls:

- Development
- Application Security
- Input
- Processing
- Output

Information Technology (IT) General Computing Controls (GCCs):

- Physical Security and Environmental Controls
- Logical Security
- Network Security
- Computer Operations
- Change Management

Information and Communication

Information

The Company has enterprise wide and business unit level information systems which capture pertinent information related to the business performance of the organization. These systems provide information related to recording and assessing financial performance and other information needed to carry out individual activities around compliance, financial, and operational controls. The Company has implemented various methods of communication to help employees understand their individual roles and responsibilities.

A description of the Company's products and services, including boundaries and commitments, is documented and communicated to internal and external users through the FIS website, the FIS Client Portal, or through client contracts.

Communication

The Company has implemented various methods of communication to help ascertain that significant events are communicated in a timely manner. These methods include items such as orientation and training programs for newly-hired employees, periodic communications addressing corporate strategy and product information, printed materials, online Web-based information services, self-study, classroom-based training sessions, and the use of electronic mail messages to communicate time-sensitive information. Managers hold periodic staff meetings as needed.

The Company's corporate policies, guidelines, and ethical values are documented within the Employee Handbook. New employees and contractors utilize Regulatory University to review and acknowledge that they have read, understand, and will follow the security policies and the Company's Code of Conduct. Human Resources actively monitors the Employee Handbook to maintain that the information is accurate and current and that employees have easy access to its contents when needed.

The following formal written policies and standards are in place to support enterprise functions: Information Security, Risk Management, and Network Security. The Company's corporate security policies are communicated to employees on the FIS intranet and reviewed/acknowledged utilizing Regulatory University.

The Company's security commitments and customer responsibilities, which include responsibilities for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are described on the FIS website and within system documentation.

The Security Incident Response Policy and Issue Management Standard documents provides instructions to report issues and are communicated to appropriate employees. Clients are notified if the FIS Security Incident Response Team (FSIRT) determines that a specific, direct client impact related to security incidents has occurred. FIS security changes are communicated to both internal and external users on the FIS Client Portal.

Monitoring

Continuous monitoring and ongoing evaluations of established controls are critical components of the Company's internal control environment. Monitoring provides management oversight on the internal control design and operating effectiveness. The Company evaluates the effectiveness of its system of internal controls through management reviews, internal audits, and external audits performed on a

regular basis. The Executive Risk and Technology Committee provides management oversight to the overall risk management direction, culture, and policy for risk at the Company.

The Company is periodically examined by the Federal Banking Agencies (FBA), an interagency examination organization comprised of the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (FRB), and the Federal Deposit Insurance Corporation (FDIC). Examination results are communicated to Company management and the Audit Committee.

The Company has engaged third-party auditors to perform various external audits which are focused on internal controls over financial reporting and compliance with specific criteria and international standards throughout the year. These audits necessitate that management prepare an assertion confirming that the controls are suitably designed and operating effectively. Throughout the year, each business unit reviews process narrative documentation, helping to ensure the accuracy and design compliance of the controls included in the scope of each audit.

The Company and relevant business units that store, process, and/or transmit cardholder data are subject to Payment Card Industry (PCI) compliance and undergo annual certification. Assessments are completed by certified Qualified Security Assessors (QSAs). Clients can validate the Company's PCI Data Security Standard (DSS) status by visiting the FIS Client Portal.

Security incidents are evaluated to determine whether the incident could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws and regulations. For all instances of unauthorized use or disclosure of personal information, the affected information is appropriately identified.

Internal Audits

The Company has an independent Internal Audit department which reports functionally and administratively to the Audit Committee of the Board of Directors. Internal Audit performs its duties in accordance with a charter which is reviewed and updated by the Chief Audit Executive (CAE) and approved annually by the Audit Committee. Internal Audit is an independent, objective assurance and consulting activity designed to add value and improve the corporation's operations. Internal Audit aids the Company in accomplishing its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of management controls, risk management, and governance processes. In this regard, Internal Audit is charged with independently evaluating the control environment and providing assurance services to the Audit Committee, and management on the effectiveness of controls and the various programs that management has established to mitigate risk to the Company.

Internal Audit prepares an annual audit plan, which is submitted for review and approval to the Audit Committee. Updates to the annual plan are reviewed and approved at the Audit Committees' quarterly meetings. Internal Audits are performed based on Internal Audit's annual risk assessment process, which includes a variety of inputs, such as prior audit coverage and results, changes within the business, management interviews and reporting packages, emerging trends, risk assessments prepared by the Risk Management department, and other relevant Internal Audit practices. This information is used to prepare the Internal Audit risk assessment, which is a top-down and bottom-up analysis used to prioritize audit coverage based on risk. Audit coverage may be defined in a number of areas, such as financial, information technology and security, compliance/regulatory, and operations.

Audit results are communicated to the audited party, executive management, and to the Audit Committee, concurrently. In addition, Internal Audit has a follow-up process whereby audit observations and management remediation plans are monitored for resolution with reporting to management occurring twice a month. Retesting of observations is performed to validate completion on all critical, high and medium risk observations with low risk observations being subject to Internal Audit management judgement.

D. Overview

The FIS Little Rock Technology Center (LRTC), FIS Brown Deer Operations Center (BDOC), FIS New Berlin Data Center (NBDC), FIS Phoenix Technology Center (PTC), and Digital Realty Phoenix Technology Center (PHX2) are five of FIS' strategic sites supporting the design, development, implementation, operation, maintenance, and monitoring of FIS-developed and hosted applications and services. The security principle refers to the protection of the system components from unauthorized access, both logical and physical. Information provided through these systems is susceptible to unauthorized access during transmission and while it is stored on other parties' systems. Limiting access to the system components helps prevent potential abuse of system components, theft of resources, misuse of software, and improper access to, use, alteration, destruction, and/or disclosure of information. Key elements for the protection of system components include permitting authorized access and preventing unauthorized access to those components.

Components of the System

Key System Components

A master list of FIS system components is maintained, accounting for additions and removals, for management's use. In addition, the Company utilizes a configuration management database to capture key system components and to support ongoing asset and service management commitments and requirements.

People

Personnel involved in the operation of FIS' system includes developers, operators, users, and managers. FIS is comprised of enterprise wide groups, as well as specific teams (IT Information Security, Risk Management, Facilities, IT Development, and IT Technology Services) that are involved in the operation of the FIS Technology Centers system.

The Company has a staff of approximately 55,000 employees organized in the following functional areas:

Corporate

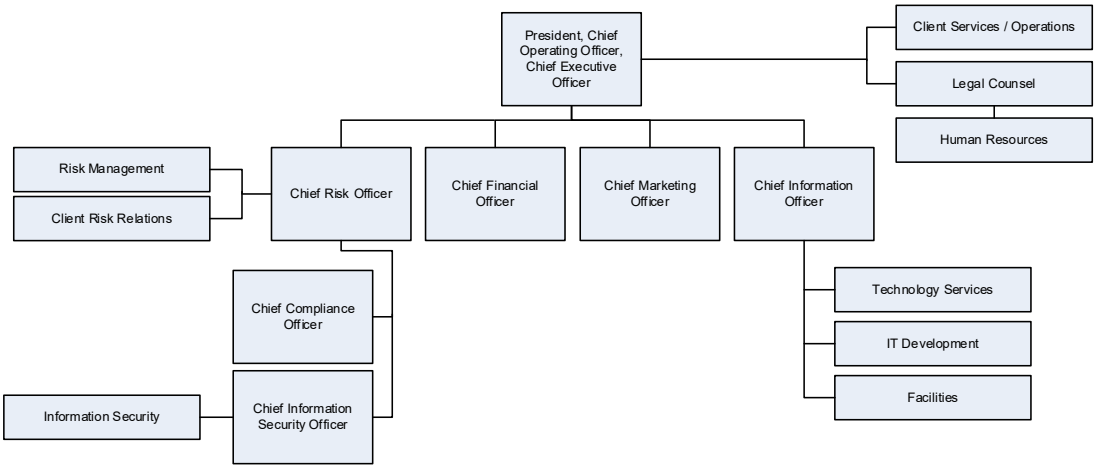
- The Business Professional group includes executives, senior operations staff members, and Company administrative support staff members, including risk management, non-IT project management, business planning, facilities, legal, training, contracting, accounting, finance, human resources, and internal audit.
- The Sales and Marketing group includes marketing, sales, and sales support staff members including corporate communications, public relations, product marketing, account executives, and product sales.

Information Technology

- The Physical Security Group is responsible for monitoring access to the facilities 24 hours per day, seven days a week and dispatching staff members to investigate system violations and take action.
- Engineers and critical facilities personnel inspect on-site environmental systems and perform maintenance activities, as needed.
- Information Security, including the Enterprise Information Security and Security Authorization Services Groups, is responsible for setting the information security policies and procedures and for the design of security architecture. This Group is also responsible for logical security administration and performing vulnerability scans and penetration tests. The Information Security Group includes the following teams:
    - The Network and Security Services Delivery (NSSD) team is responsible for asset and capacity management, patch and vulnerability management, and network monitoring.
    - The Security Architecture and Solutions team is responsible for communicating enterprise wide standards for network, WANs, patch maintenance, and firewalls.

  - The FIS Security Incident Response Team (FSIRT) is engaged to analyze, coordinate, investigate, and respond to events and mitigate the impact when a security incident is identified.
- Operations personnel manage operations 24 hours a day, seven days per week, supporting online processing, batch processing, report generation, and system back-up functions in multiple shifts.
- The Enterprise Project Management Office (EPMO) is responsible for product development standards including Software Development Life Cycle (SDLC). Additionally, members of the Project Management Group lead multi-disciplinary project teams composed of various levels of personnel, vendors, and clients which are created for development-related projects and the delivery of software and/or outsourced solutions to external clients.
- The Change Management Department is responsible for providing oversight and maintaining the practices FIS uses to perform and regulate production environment changes.
  - The Security Administration Team reviews and approves the architecture and design specifications for new systems development and acquisition to help ensure consistency with the Company's security objectives, policies, and standards.

Group Reporting to Executive Management for Teams Relevant to FIS' Technology Centers System



Scope

Infrastructure, Software, and Data

- **Infrastructure** – The infrastructure includes the physical and hardware components of FIS' system, including facilities, computers, mobile devices, equipment, and networks. FIS maintains and operates an enterprise wide network. Physical components for the FIS Technology Centers are located within the Little Rock Technology Center, Brown Deer Operations Center, New Berlin Data Center, Phoenix Technology Center, and Digital Realty Phoenix Technology Center facilities.
- **Software** – The software includes the programs and operating components of FIS' system including supporting operating systems and utilities. A variety of operating systems are used.
- **Data** – The data includes the information components of FIS' system, including transaction streams, files, databases, and tables. A variety of database systems and Mainframe and UNIX file systems are used, in addition to non-database files. The files, databases, and data tables and their associated movement via data movers and scheduled jobs support the transaction streams related to the operation of FIS' system.

Physical components for the FIS Technology Centers are located in the Little Rock Technology Center, Brown Deer Operations Center, New Berlin Data Center, Phoenix Technology Center, and Digital Realty Phoenix Technology Center facilities. FIS utilizes the FIS Technology Centers to house applications and databases for the in-scope systems. The following Information Technology (IT)

General Computing Controls (GCC) supporting operations are performed at the FIS Technology Centers: Physical Security, Logical Security, Change Management, and Computer Operations.

The scope of the report is limited to the supporting production operating systems and databases at the FIS Technology Centers.

A separate SOC 1 Type 2 report titled "FIS Technology Centers General Computing Controls (GCCs)" encompasses the underlying IT GCC environment for FIS Technology Centers. The GCC report is available for users of this report and contains controls relating to: physical security and environmental controls; computer operations including job processing and problem management; change management; and logical security, including access administration for databases and operating systems. Application/Tool specific change management is covered within the corresponding FIS SOC 1 Type II Application/Tool specific reports and is not in the scope of this SOC 2 report.

Procedures

The procedures include the automated and manual processes and procedures involved in the operation of FIS' system. FIS has developed policies and standard procedures to operate, maintain, and secure FIS' system.

Physical Security

An access control system utilizing individual badge identification, door protection by an electronic badge reader or locked with limited access to the physical key, closed circuit camera monitoring, and on-site physical security guards stationed within strategic locations provides the facility physical security and protection. Security personnel monitor physical access points at the Technology Center locations and validate that physical access is limited to authorized personnel using video surveillance cameras and a badge reader system. Physical Security staff members within the Technology Centers Center are responsible for monitoring access to the facility 24 hours a day, seven days a week and for dispatching staff to investigate system violations and for taking action, if necessary.

Badge access readers restrict access to all external access points at the Technology Center locations and to sensitive areas within the facilities. Badge use is recorded by the access control system and includes the badge number, door accessed, time of access, and whether the action was successful or unsuccessful. Unauthorized physical access attempts at the Technology Center locations are monitored real-time and are logged and acted upon by security personnel. Log information is retained for a minimum of one year.

Company access cards provide identification, validation, and authentication of employees, contractors, and visitors with valid access requirements based on the information provided on the required badge registration form, with the authorization approval. Cards lost or not returned by terminated personnel can be immediately disabled within the badge reader system without being physically retrieved.

Access to the facility and operations area is restricted by an electronic card key system set-up based on badge access requests. Security levels are established within the card key system to validate that access to secure areas is restricted to authorized individuals. Physical access to the Technology Center locations is granted based upon job responsibility, according to a defined process, which requires management approval to validate that badge access is accurately granted. The ability to implement changes to physical access rights at the Technology Center locations is limited to defined administrative personnel to prevent unauthorized changes.

Physical access to sensitive areas within the Technology Center locations is reviewed monthly by management to validate that employee access is commensurate with job responsibilities.

The physical access of terminated employees is removed within one business day following notification from Human Resources or management.

Visitors are issued a temporary visitor card after registering with Physical Security and providing positive proof of identification via a valid government issued photo ID. Visitor/temporary access to the

Technology Center locations is logged and visitors are escorted by an authorized Company employee to prevent unauthorized access.

Administrative access rights to the badging system are restricted based on job responsibilities.

Logical Security

General Security Controls

Logical access for FIS' users and privileged accounts for the servers, operating systems, and supporting infrastructure located at the Technology Center locations is requested and approved by management based upon business need and job responsibilities. A valid username and password set in accordance with Company policy, including password length, expiration, history, complexity, and number of failed login attempts are required to access the servers, operating systems, and supporting infrastructure. The use of group or shared network IDs is not permitted unless approved by management. In addition, inactive user sessions are terminated after a defined period of time for the servers, operating systems, and supporting infrastructure location at the Technology Centers locations.

The FIS Access Control Policy requires the timely notification of employee separations by the reporting Manager to HR. Active Directory access is configured to be automatically disabled every 15 minutes when the employee's status within the HR system is changed to "terminated." Logical access to Active Directory is removed and/or updated within five business days of termination date/last day worked or based on job change reports.

A manual request from an authorized client requestor or approval from authorized FIS personnel must be received before a new client user is set up within the servers, operating systems, and supporting infrastructure located at the Technology Center locations.

Privileged access is governed via a password vault. Users must first log in with their usernames and passwords and are then provided appropriate access as an Administrator. Logging on the password vault is enabled to track individuals accessing privileged accounts. Privileged access rights to the servers, operating systems, and supporting infrastructure at the Technology Center locations including the ability to make changes to logical access rights and access to schedule and execute jobs at the Technology Center locations is limited to authorized personnel based on job responsibilities. In addition, access to modify network device configurations, including firewall rule settings, is restricted to appropriate personnel to prevent unauthorized changes. Direct access to the in-scope databases is restricted to appropriate personnel based on job function. Logical access is reviewed by management for the servers, operating systems, and supporting infrastructure located at the Technology Center locations on a quarterly basis to validate that user access levels are appropriate.

Servers are built according to documented (User Group) build standards.

Unisys Mainframe and DMSII Security Controls

Security controls for the Unisys Mainframe provide logical access control over transactions, data, and program files. The controls protect production and test data residing on disk and tape and also provide protection in both background (batch) and foreground (time-sharing or online) processing. Access controls such as user names, passwords, and strong authentication are implemented as part of the Data Center framework.

The procedures for provisioning users are reviewed annually to verify that a formalized and documented process exists to grant and periodically review access to applications and environments that have the potential to process, store, or transmit financially relevant information.

The Enterprise Information Security Group, including the Security Authorization Services Group, is responsible for logical security administration. Authorized Company management personnel are responsible for requesting and authorizing access privileges for their employees and are responsible for notifying the Security Authorization Services Group for changes in access needs, including new employees, terminations, and transfers. Requests indicate whether access is to be granted through predefined profiles based on job responsibility or assignment to specific groups and resources. The use

of user profiles and assignment to specific resources helps to validate that access granted to employees is authorized based upon job responsibilities. Changes are communicated to the Security Authorization Services Group via Request Forms, Employee Move, Add, Change (EMAC) requests, Case Management System (CMS) requests, or other approved corporate communications.

The Unisys Mainframe parameters are set to control minimum password lengths, complexity requirements, and maximum password lifetime. Unisys termination updates are done manually upon notice of each termination.

Logical security tools and/or native platform level security functions are in place to help secure the Unisys Mainframe used by FIS to support computer operations. At a minimum, the Unisys Mainframe has authentication controls requiring users to provide a valid user ID and password to obtain access to platform resources. Additionally, access restrictions are in place on the Unisys Mainframe and define user access to specific resources by user or group IDs.

Quarterly employee inactivity reviews are performed on the Unisys Mainframe; quarterly employee access reviews are performed for the Unisys Mainframe to confirm that access is commensurate with job responsibility, and reports detailing employee access to specific resources are generated by the Security Authorization Services Group and are distributed to authorized approvers. Authorized approvers are responsible for reviewing the reports and for notifying the Security Authorization Services Group of required access changes.

The Unisys Mainframe access control software allows for customized logging and exception reporting. Exception reports denoting access violations are generated each business day and are reviewed as necessary by the Security Authorization Services Group. Violation reviews are documented, and potential security violations are reported to the data owner when necessary. The data owner is responsible for investigating and resolving the problem with the employee and reporting the resolution to the Security Authorization Services Group.

Client users are defined as Security Administrators to specific applications. The client Security Administrator accounts are set up in accordance with the standard access approval process and are restricted to administering access for their environment.

Firecall IDs are not used for the Unisys Mainframe environment; access requests follow the central access request and approval process using the EMAC tool discussed above.

IBM Mainframe, VSAM, DB2, IMS, and CICS Security Controls

Security controls for the IBM Mainframe provide logical access control over transactions, data, and program files. The controls protect production and test data residing on disk and tape and also provide protection in both background (batch) and foreground (time-sharing or online) processing. Access controls such as user names, passwords, and strong authentication are implemented as part of the Data Center framework.

The procedures for provisioning users are reviewed annually to verify that a formalized and documented process exists to grant and periodically review access to applications and environments which have the potential to process, store, and/or transmit financially relevant information.

The Enterprise Information Security Group, including the Security Authorization Services Group, is responsible for logical security administration. Authorized Company management personnel are responsible for requesting and authorizing access privileges for their employees and are responsible for notifying the Security Authorization Services Group for changes in access needs, including new employees, terminations, and transfers. Requests indicate whether access is to be granted through predefined profiles based on job responsibility or assignment to specific groups and resources. The use of user profiles and assignment to specific resources helps to validate that access granted to employees is authorized based upon job responsibilities. Changes are communicated to the Security Authorization Services Group via Request Forms; EMAC requests; CMS requests; or other approved corporate communications.

The IBM Mainframe parameters are set to control minimum password lengths, complexity requirements, and maximum password lifetime. The IBM Mainframe termination updates are performed manually upon notice of a termination.

Logical security tools and/or native platform level security functions are in place to help secure the IBM Mainframe, DB2, IMS, and CICS used by FIS to support computer operations. At a minimum, IBM Mainframe, DB2, IMS, and CICS have authentication controls requiring users to provide a valid user ID and password to obtain access to platform resources. Additionally, access restrictions are in place on the IBM Mainframe, DB2, IMS, and CICS and define user access to specific resources by user or group IDs.

Periodic access reviews are performed on the IBM Mainframe, DB2, IMS, and CICS systems to confirm that access is commensurate with job responsibility. Quarterly employee inactivity reviews are performed for the IBM Mainframe, DB2, IMS, and CICS. Quarterly employee access reviews are performed for the IBM Mainframe, DB2, IMS, and CICS, where reports detailing employee access to specific resources are generated by the Security Authorization Services Group and are distributed to authorized approvers. Authorized approvers are responsible for reviewing the reports and for notifying the Security Authorization Services Group of required access changes.

The IBM Mainframe RACF and ACF2 access control software allow for customized logging and exception reporting. Exception reports denoting access violations are generated each business day and are reviewed as necessary by the Security Authorization Services Group. Violation reviews are documented, and potential security violations are reported to the data owner when necessary. The data owner is responsible for investigating and resolving the problem with the employee and for reporting the resolution to the Security Authorization Services Group.

Client users are defined as Security Administrators for specific applications. The client Security Administrator accounts are set up in accordance with the standard access approval process and are restricted to administering access for their environments.

Firecall IDs are used for the IBM Mainframe environment, and access requests follow the central access request and approval process using the Employee Move-Add-Change (EMAC) and Case Management System (CMS) tool.

UNIX Servers Security Controls

Logical access to the UNIX servers is controlled to include limited access to directories, authorities, file ownership rights, and allowable times of access. The Identity Management (IDM) solution, BoKs, is used to restrict access to the UNIX servers. In conjunction with application security, these controls protect production data residing on the UNIX servers within the Company's production environment. Application security provides additional protection detailing the type of transaction categories, data, application, and system resources which may be accessed from and within a particular application. Administrative access to the BoKs controlled UNIX servers is restricted based on the BoKs' user class, which gives users the ability to check out the root password, as well as sudo (i.e., substitute/switch/super user) into root.

Access controls such as user names, passwords, and strong authentication are implemented. To access the BoKs controlled UNIX servers, dual factor authentication is utilized via RSA SecurID® to identify and authenticate users via a valid user ID and a one-time passcode. Authenticating to the BoKs' controlled UNIX servers requires provisioning via user class in BoKs' and RSA Security Console's user group membership. Non-BoKs' UNIX servers are controlled by user names and passwords.

The procedures for provisioning users are reviewed annually to verify that a formalized and documented process exists to grant and periodically review access to applications and environments which have the potential to process, store, or transmit financially relevant information.

The Enterprise Information Security Group, including the Security Authorization Services Group, is responsible for logical security administration. Authorized Company management personnel are responsible for requesting and authorizing access privileges for their employees and are responsible for notifying the Security Authorization Services Group for changes in access needs, including new

employees, terminations, and transfers. Requests indicate whether access is to be granted through predefined profiles based on job responsibility or assignment to specific groups and resources. The use of user profiles and assignment to specific resources helps to validate that access granted to employees is authorized based upon job responsibilities. Changes are communicated to the Security Authorization Services Group via Request Forms, DASH requests, CMS requests, or other approved corporate communications.

The UNIX server parameters are set to control minimum password lengths, complexity requirements, and maximum password lifetime. The UNIX server termination updates are done manually upon notice of a termination.

UNIX (BoKs) goes through periodic access reviews to confirm that access is commensurate with job responsibility. Quarterly employee inactivity reviews are performed for UNIX (BoKs). Quarterly employee access reviews are performed for UNIX (BoKs), where reports detailing employee access to specific resources are generated by the Security Authorization Services Group and are distributed to authorized approvers. Authorized approvers are responsible for reviewing the reports and for notifying the Security Authorization Services Group of required access changes.

Windows and SQL Servers Security Controls

Logical access to Windows and SQL servers is controlled by native Windows security. A valid user ID and password are required to gain access to Windows server system resources. This mechanism, in conjunction with application security, protects production data residing on Windows and SQL servers within the Company's production environment. Windows and SQL server access control features include the ability to limit access by shares, directories, group and group access rights, file ownership rights, user access rights, and allowable times of access. Application security provides additional protection detailing the type of transaction categories, data, applications, and system resources which may be accessed from and within a particular application.

The procedures for provisioning users are reviewed annually to verify that a formalized and documented process exists to grant and periodically review access to applications and environments which have the potential to process, store, and/or transmit financially-relevant information.

The Enterprise Information Security Group, including the Security Authorization Services Group, is responsible for logical security administration. Authorized Company management personnel are responsible for requesting and authorizing access privileges for their employees and are responsible for notifying the Security Authorization Services Group for changes in access needs, including new employees, terminations, and transfers. Requests indicate whether access is to be granted through predefined profiles based on job responsibility or assignment to specific groups and resources. The use of user profiles and assignment to specific resources helps to validate that access granted to employees is authorized based upon job responsibilities. Changes are communicated to the Security Authorization Services Group via Request Forms; DASH requests; CMS requests; or other approved corporate communications.

Active Directory (AD) and SQL server parameters for the domain are set to control minimum password lengths, complexity requirements, and maximum password lifetime. Active Directory) and SQL server termination updates are performed manually upon notice of a termination. There is also a scheduled interface which runs every 15 minutes to check the AD databases against the Oracle HR employee/contractor database. Once an employee or contractor is terminated within Oracle, his/her AD account is automatically disabled.

Quarterly employee inactivity reviews are performed for the Windows and SQL servers; quarterly employee access reviews are performed for the Windows and SQL servers where reports detailing employee access to specific resources are generated by the Security Authorization Services Group and are distributed to authorized approvers to confirm that access is commensurate with job responsibility. Authorized approvers are responsible for reviewing the reports and for notifying the Security Authorization Services Group of required access changes.

HP NonStop and Enscribe HP SQL Servers Security Controls

HP NonStop servers restrict logical access through the use of the Safeguard security product. Safeguard provides controls beyond standard Guardian operating system file and user security. It is an optional product which the Company has chosen to use for additional security. The Information Security Group maintains the Safeguard security administrator access ID and performs additions, deletions, and updates to the active Safeguard database. The Safeguard security administrator ID owns subject, objects, and access control lists. The Company has chosen to use a combination of Safeguard sub-volume and Safeguard file security to protect HP NonStop server system files.

The procedures for provisioning users are reviewed annually to verify that a formalized and documented process exists to grant and periodically review access to applications and environments which have the potential to process, store, and/or transmit financially relevant information.

The Enterprise Information Security Group, including the Security Authorization Services Group, is responsible for logical security administration. Authorized Company management personnel are responsible for requesting and authorizing access privileges for their employees and are responsible for notifying the Security Authorization Services Group regarding changes in access needs, including new employees, terminations, and transfers. Requests indicate whether access is to be granted through predefined profiles based on job responsibility or assignment to specific groups and resources. The use of user profiles and assignment to specific resources helps to validate that access granted to employees is authorized based upon job responsibilities. Changes are communicated to the Security Authorization Services Group via Request Forms, DASH requests, CMS requests, or other approved corporate communications.

HP NonStop server parameters are set to control minimum password lengths, complexity requirements, and maximum password lifetime. HP NonStop server termination updates are performed manually upon notice of a termination.

Quarterly employee inactivity reviews are in place for HP NonStop and Enscribe HP SQL servers; quarterly employee access reviews are performed for HP NonStop and Enscribe HP SQL where reports detailing employee access to specific resources are generated by the Security Authorization Services Group and are distributed to authorized approvers to confirm that access is commensurate with job responsibility. Authorized approvers are responsible for reviewing the reports and for notifying the Security Authorization Services Group of required access changes.

IBM i Servers Security Controls

Logical access to the IBM i servers is controlled to include roles and special object authority. In conjunction with application security, these controls protect production data residing on IBM i servers within the Company’s production environment.

The procedures for provisioning users are reviewed annually to verify that a formalized and documented process exists to grant and periodically review access to applications and environments which have the potential to process, store, and/or transmit financially relevant information.

The Enterprise Information Security Group, including the Security Authorization Services Group, is responsible for logical security administration. Authorized Company management personnel are responsible for requesting and authorizing access privileges for their employees and are responsible for notifying the Security Authorization Services Group for changes in access needs, including new employees, terminations, and transfers. Requests indicate whether access is to be granted through predefined profiles based on job responsibility or assignment to specific groups and resources. The use of user profiles and assignment to specific resources helps to validate that access granted to employees is authorized based upon job responsibilities. Changes are communicated to the Security Authorization Services Group via Request Forms; DASH requests; CMS requests; or other approved corporate communications.

IBM i servers parameters are set to control minimum password lengths, complexity requirements, and maximum password lifetime. IBM i servers termination updates are performed manually upon notice of a termination.

Quarterly employee inactivity reviews are in place for the IBM i servers; quarterly employee access reviews are performed for the IBM i servers where reports detailing employee access to specific resources are generated by the Security Authorization Services Group and distributed to authorized approvers to confirm that access is commensurate with job responsibility. Authorized approvers are responsible for reviewing the reports and for notifying the Security Authorization Services Group of required access changes.

Oracle Database

Logical access to the Oracle database is controlled through granted roles. In conjunction with application security, these controls protect production data residing on Oracle databases within the Company's production environment. The granted role of DBA gives users' highly privileged access to the Oracle Databases.

The procedures for provisioning users are reviewed annually to verify that a formalized and documented process exists to grant and periodically review access to applications and environments which have the potential to process, store, and/or transmit financially-relevant information.

The Enterprise Information Security Group, including the Security Authorization Services Group, is responsible for logical security administration. Authorized Company management personnel are responsible for requesting and authorizing access privileges for their employees and are responsible for notifying the Security Authorization Services Group for changes in access needs, including new employees, terminations, and transfers. Requests indicate whether access is to be granted through predefined profiles based on job responsibility or assignment to specific groups and resources. The use of user profiles and assignment to specific resources helps to validate that access granted to employees is authorized based upon job responsibilities. Changes are communicated to the Security Authorization Services Group via Request Forms; DASH requests; CMS requests; or other approved corporate communications.

The Oracle database parameters are set to control minimum password lengths, complexity requirements, and maximum password lifetime. The Oracle database termination updates are performed manually upon notice of a termination.

Quarterly employee inactivity reviews are performed for the Oracle databases; quarterly employee access reviews are performed for the Oracle databases where reports detailing employee access to specific resources are generated by the Security Authorization Services Group and distributed to authorized approvers to confirm that access is commensurate with job responsibility. Authorized approvers are responsible for reviewing the reports and for notifying the Security Authorization Services Group of required access changes.

Access Monitoring (All platforms)

Invalid access attempts and additional resource events as selected by Security Authorization Services personnel are recorded and are logged. In addition, records are extracted from platform applications to facilitate reviews of activity by sensitive IDs, activity against critical system files, and unauthorized activities. Security Authorization Services personnel review security reports periodically. Access violations prompt warning messages and the rejection of access.

Successes and failure to perform the following functions are monitored: changes to the security policy, changes to user and group accounts, access of files and objects, logons and logoffs, use of user rights, and system start-ups and shutdowns. Key events (such as changes to security parameters, user profiles, and/or user rights) are reviewed periodically. Monitoring of other events occurs periodically or as needed. Discrepancies noted are investigated and resolved by Security Authorization Services personnel.

Client Access (All platforms)

Client personnel are responsible for performing and controlling security administration for applications and tools used by their organization. Security administration tools provided by FIS facilitate this control of their organization's user access rights. Various applications and tools control client requests for

system access additions and changes. Upon formal notification from authorized client personnel, Security Authorization Services personnel make access changes for operating systems and other applications and tools which are not controlled by clients.

Client access to FIS applications allows access to be assigned at the individual client user level. This allows the flexibility to grant update authority versus inquiry authority and to define specific transactions and screens which are available to users based upon an employee's job responsibilities.

Data Loss Protection (DLP)

Data Loss Protection (DLP) software is enabled to prevent unauthorized data removal through removable media, except where required by approved business need. Removable media such as USB external drives, thumb drives, and/or CD/DVD-ROM drives are not allowed to be utilized to store Non-public Personal Information (NPI) including, but not limited to, credit card numbers and social security numbers. The Security Authorization Services Group has deployed a desktop program which works in conjunction with the virus protection software, providing the ability to block or allow "write" access to external USB mass storage devices (based on management approval). Read/write access for any corporate information is granted based on approved business need. The DLP Waiver Request form must be completed and approved by management, security governance, and information security operators to receive an exception to this policy.

Antivirus

Antivirus software is implemented and is updated to help protect programs, data, and other information resources from viruses and malware.

SecurID

Security Authorization Services personnel issue user IDs, passcodes, and SecurID tokens. The SecurID tokens generate a one-time, rapidly expiring, passcodes for various system accesses based on management and client authorizations. The RSA SecurID® server is used to identify and authenticate users via a valid user ID and a one-time passcode. Additionally, access control features include the ability to control powerful access rights. Powerful access rights are granted based upon job responsibility and are restricted to authorized personnel.

Remote Access

Remote access to network resources, including mobile access, is controlled through the use of SecurID tokens and/or a Virtual Private Network (VPN), subject to password security settings, to create encrypted private communications when remotely accessing network resources. Users are granted VPN access based on management approval.

Encryption

Company policy states that all transmissions of electronic information from Technology Centers' Data Centers are encrypted as the default setting over public networks via secure transmission protocols (e.g., HTTPS, SFTP, VPN, and TLS). The Encryption Architecture Review Committee (EARC) performs a review of the encryption technologies in place based on a risk-based assessment. In addition, System data is encrypted at rest in accordance with the Encryption Policy. The Encryption Architecture Review Committee (EARC) performs a review of the encryption technologies in place based on a risk-based assessment.

Company policy requires that laptops be encrypted to access the Company's network.

Back-ups

Back-up tapes are encrypted during the back-up process (when feasible), are rotated/transmitted off-site, and are transported in locked containers via a secured courier truck for the Technology Centers. Logical access to the back-up application at the Technology Centers is restricted to appropriate employees based on job function.

E-mail Content Filtering

E-mail content filtering exists to automatically encrypt sensitive data matching known patterns for social security numbers and credit card numbers.

Data Movers

The Company uses the following tools to systematically move data between in-scope applications.

Data Mover Tool	Description
Connect:Direct/ Network Data Mover (NDM)	Connect:Direct/NDM are tools used to take input files from FIS applications or from external third-parties applications and interfaces the files to other FIS applications for input and transaction processing. There are instances of Connect:Direct/NDM on Windows, UNIX, Mainframe, IBM i and HP NonStop servers, which Company users authenticate to through their associated operating system credentials (i.e., Connect:Direct – Mainframe a Company user authenticates using RACF or ACF2 user ID and password). Logical access to Connect:Direct/NDM – Windows is controlled through access to Windows shares, directories, group and group access rights, file ownership rights, and user access rights. Logical access to Connect:Direct/NDM – UNIX is controlled through access to UNIX BoKs user classes. Logical access to Connect:Direct/NDM – Mainframe is controlled through access to Mainframe roles. Logical access to Connect:Direct/NDM – IBM i is controlled through access to IBM i administrator IDs. Logical access to Connect:Direct/NDM – HP NonStop is controlled through access to HP NonStop Safeguard security administrator IDs.
Database Rules Engine (DBRE)	DBRE is a tool that acts as the middleware to transmit transactions from the HP NonStop to other FIS applications in near real-time. Logical access to DBRE is controlled through access to Linux Red Hat granted profiles.
Momentum – FTP and SFTP	Momentum FTP and SFTP are file transmission tools, which are used to bi-directionally transmit data between different FIS applications and other financial institutions, vendors, and FIS locations. Logical access to Momentum FTP and SFTP are controlled through access to Windows shares, directories, group and group access rights, files ownership rights, and user access rights.
MoveIT/ETL/File Mover	MoveIT is a file transmission tool, which is used to bi-directionally transmit data between different FIS applications and other financial institutions, vendors, and FIS locations. Logical access to MoveIT is controlled through access to Windows shares, directories, group and group access rights, files ownership rights, and user access rights.
BARR/TRAN	BARR/TRAN is a file transmission tool, which is used to bi-directionally transmit data between different FIS applications and other financial institutions, vendors, and FIS locations. BARR/TRAN extended file transfer software contains the BARR/TRAN mainframe program that handles specialized file transfer applications. BARR/TRAN reads and writes IBM MVS files and converts the files for transmission. Logical access to BARR/TRAN is controlled through Mainframe roles.
Data Express	Data Express is a file transmission tool, which is used to bi-directionally transmit data between different FIS applications and other financial institutions, vendors, and FIS locations. Data Express supports multiple protocols including: FTP and FTPS, HTTP and HTTPS, and SFTP. Logical access to Data Express is controlled through the application with user ID and role privileges.

In conjunction with application security, these controls protect production data transmitted through the data mover tools.

Network Security

The Company maintains multiple layers of controls to secure, manage, and monitor the network environment. Risk levels for network areas are identified, and security levels are set accordingly to control the level of confidentiality, integrity, and availability. High-availability configurations, where technically feasible, have also been designed into the controls and management functions to facilitate continuity of service.

The Company utilizes multiple control layers to secure, manage, and monitor threats and risks to the network environment. Network devices (e.g., routers, switches, firewalls) are deployed and are maintained to prevent threats to the Company's environment. Network security controls include a combination of security tools and processes which are utilized to safeguard systems against unauthorized network access. These components include, but are not limited to, routers, firewalls and intrusion prevention systems (IPS), and passive countermeasures such as Intrusion Detection Systems (IDSs) and a security incident and event management (SIEM) system to facilitate data gathering, notification, analysis, and interpretation. Additionally, internal portions of the network have been segmented to restrict access between internal workstations and production applications across the Company's major Data Centers.

The Intrusion Detection System and Intrusion Prevention System (IDS/IPS) software is automatically configured to monitor the network perimeter and to intercede and/or provide alert notifications to appropriate personnel. Alert notifications identified are logged, tracked, and resolved.

Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent for each week.

The Information Security Department utilizes a combination of commercial and custom tools to conduct vulnerability scans and security tests to detect malware and/or other potential security vulnerabilities. Identified vulnerabilities are tracked and reported to management based on their risk rating.

The Company conducts web-application and/or network penetration testing on an annual basis for FIS-owned internet facing applications and FIS-owned/managed infrastructure. Information Security is responsible for performing vulnerability scans and penetration tests. Vulnerabilities identified within scans and penetration tests are documented and communicated to responsible parties. Upon notification that a vulnerability has been corrected, a validation scanning or testing is performed.

The Company has implemented an array of protections and procedures to secure the internal network from intrusion. IDS and IPS systems have been deployed across the Company's major Data Centers, with alerts notifying relevant personnel for investigation and resolution if established security-related events are triggered through a SIEM. Company personnel review the alerts and key indicators and may perform corrective action to the environment.

Alerts are configured to detect and notify the Information Security Team of key security events such as potential attacks and suspicious activities. There are defined procedures to investigate and respond to such events. Response activities are reported, logged, retained, and assigned for resolution within a ticketing system.

Network monitoring systems are deployed and are actively running on the Company's network to log events and detect anomalous activities. Tools are used to monitor Data Centers' network platforms and devices, service connections, data transmission errors and retransmissions, average response times, usage statistics, and downtime. Monitoring tools, including scripts developed by Company personnel, trigger automated warning messages which are displayed on consoles monitored by operations personnel as well as automated e-mails, which are sent to operations personnel, depending on the severity of the event. Incidents and alerts are managed and reported through the Company's central

incident tracking system to assist in prompt investigation and resolution of incidents and alerts. Alarms and automatic messages are also produced to indicate the status of certain key events or jobs.

For high-severity incidents, a root cause analysis is prepared and is reviewed by operations management. Based on the root cause analysis, change requests are prepared, and the Company's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution.

Daily reports are produced and detail changes made to processing parameters. These reports provide operations personnel with a method to monitor parameter changes which are introduced into the batch processing structures. Operations personnel also monitor changes in executed jobs each business day to help ensure changes were authorized and expected. Unexpected events are investigated and resolved.

The process for clients and external users to inform the entity of possible availability issues, security breaches, and other incidents, including complaints, is posted on FIS' intranet site.

FIS Incident Management policies and procedures exist for issues which have the potential to affect clients. Status meetings occur to discuss client impact issues, in which the issues are weighted by their criticality, with the most critical issues receiving the most immediate attention. The incident owner for these issues provides an update to the audience regarding the extent of the client impact, short-term resolution/workaround, root cause information, and timeframe for permanent resolution.

The Incident Management team performs an assessment based on established criteria for meeting requests and gathers the authorized teams from within the organization to help troubleshoot or communicate about the issues. Post Incident Reviews (PIRs) can be requested by any person within FIS and are typically requested for reasons such as processing issues, problems requiring multiple changes, system standstill, etc.

When a security incident is identified, the FIS Security Incident Response Team (FSIRT) is engaged to analyze, coordinate, investigate, and respond to events and mitigate the impact. Specific actions are assigned to relevant Company resources and the FSIRT reviews actions taken to validate that problems are addressed. The incident response plan also addresses escalation and client notification.

The Incident Management Department maintains established Incident Report (IR) and PIR standards. One does not dictate the need for the other; however, IRs can be created as the result of an action item from a PIR. The IR is a summary document which is distributed both internally and externally for the purposes of communication or clarification of the impact, root cause, resolution, and long-term prevention of an incident. The PIR process provides an opportunity for interested parties to discuss critical issues for the purpose of clarifying and reviewing the incident, while identifying potential improvements.

The Vulnerability Governance Committee has been established to provide ongoing measurement and monitoring of the risk-rating methodology, to perform scenario analysis, and to implement changes as needed to address the risk tolerance and prioritization for identified network and application vulnerabilities. This committee meets monthly and maintains meeting minutes, action items, and follows up on any open action items.

Data Classification and Protection

The Company has established a Data Classification and Handling Standard which addresses data retention to help ensure that confidential client information is retained to meet the Company's confidentiality commitments and system requirements. Additionally, the Company's Data Protection Policy states that client information that has exceeded its retention period is security purged, destroyed, or overwritten in accordance with business requirements and client specifications.

Change Management

The Change Management Department is responsible for providing oversight and for maintaining the practices FIS uses to perform and regulate production environment changes. The Change Management

Department practices are designed to facilitate consistent service delivery to FIS clients by reducing the potential for negative impact caused by the introduction of change into the production environment.

The Company has implemented a formal Business Project Management Methodology (BPM) in support of the Systems Development Life Cycle (SDLC) methodology which governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology. The Business Project Management Methodology (BPM) includes a framework for evaluating risk, confirming availability and performance requirements, and confirming project conformance to architecture and security standards, including the classification of data and the appropriate treatment of information in the event of a loss of security. In addition, the Company has a Change Authorization Policy which defines change management requirements and responsibilities related to the change process, steps to be performed throughout the change process, and required authorizations to confirm that changes are complete and authorized.

The Patch Management Policy details recommended actions and outlines a minimum recommended timeframe for implementation of routine security patches. A formal process is documented to rank patches according to their level of vulnerability and enables the reviewers to prioritize and apply those patches deemed critical in a more timely fashion.

Managing change is a systematic approach to implementing system software, infrastructure, application, and database changes. The Company has developed a standard change process which includes key control points to confirm that all changes (including, but not limited to software, hardware, network, firewalls, application configuration changes, etc.) are controlled and managed in a consistent manner. Control points of the FIS change process include steps to confirm changes are properly authorized by management, documented by the implementation teams, and approved by relevant stakeholders before the change is migrated to the production environment. These approvals may include affirmation that appropriate quality control steps have been taken prior to implementation.

Requests for changes, system maintenance, and supplier maintenance are standardized and are subject to documented change management procedures. Changes are categorized and are ranked according to priority, and procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their requests. Changes are assigned one of four risk ratings (low, medium, high, and very high/critical). Validation/test and approval requirements are driven by these ratings. Low and medium risk changes are small in size and scope, use established processes, and have no or low potential for negative client impact. High and critical risk changes are moderate to high in scope and size, have complex implementation requirements, and have moderate to high potential for negative client impact. Changes involving high and critical levels of risk require an endorsement from management or a quality control function that the change is ready for production. Change Management provides the final approval on risk assessment and the request itself.

FIS utilizes the Case Management System (CMS) and ServiceNow to track and document changes to the production environments. Source code and production environments include controls designed to restrict the ability to access and modify production source code and to migrate changes into the production environment to authorized personnel. These controls are designed to confirm that the change process is consistently followed.

All changes to the hardware, servers, operating systems, and supporting infrastructure (including job schedules and network security devices) at the Technology Center locations require initial authorization, testing (when required), approval from clients (when required), and migration approval from authorized personnel to confirm that changes introduced into production are authorized. Weekly change meetings are held to review changes related to security made to production systems.

Separate libraries for the test and production environments for servers, operating systems, and supporting infrastructure located at the Technology Center locations have been established. Logical access to these environments is restricted based on job responsibility to prevent unauthorized access.

Reactive Emergency changes are those that are not planned but are required to initiate immediate corrective action within the production environment. These changes include those necessary to correct a production application problem, changes to programs necessitated by environmental/network

problems, and changes necessary to correct other errors. In accordance with the Change Authorization Policy, emergency changes are tracked via a Case Management System (CMS) or ServiceNow ticket and require after-the-fact approval. To complete a reactive emergency change, the on-call or designated support or development personnel develops the authorized change and then requests that it be migrated into production. Tools and processes exist to migrate an emergency change into the production environment. Change records documenting the emergency action taken are required to be submitted for approval to Change Management within two business days of the change.

Production Library Controls

Access to promote changes into production at the Technology Centers is limited to appropriate individuals without development responsibilities. On-call personnel and personnel who support ongoing operations and production are granted access to the production environment to troubleshoot and remedy problems which occur based on business need and business approval.

Source Code Management Tools

FIS uses a variety of source code management tools, depending upon the platform and application. The source code management tools used by FIS help protect the integrity of production code through the use of check-in and check-out features. These tools confirm that conflicts do not occur on changes when multiple staff members are involved in a development project. Source code management practices also help to control when changes are migrated into the production environment, as approvals are required to be obtained by authorized personnel before the change is allowed to be migrated into production. This process is controlled either through an automated link to the tracking system which does not allow changes to be migrated into production without documented approvals or through an application librarian function. Application teams that do not utilize automation to migrate code into production utilize a librarian function. The librarian is responsible for migrating changes into the production environment after approvals have been obtained. Logical access to the source code management tools utilized at the Technology Centers locations is restricted to appropriate personnel based on job responsibilities.

Recovery Procedures

The Business Continuity and Disaster Recovery Plan is tested on at least an annual basis, and any issues are documented and resolved. In addition, incremental backups for the in-scope servers and databases are configured to be performed daily and full backups for the in-scope servers and databases are configured to be performed weekly. Any issues are researched and resolved in accordance with the Company's Backup and Restoration policies. Data restore testing is performed on at least an annual basis to verify the integrity of the backup data.

E. Principal Service Commitments and System Requirements

FIS designs its processes and procedures related to user entities to meet its objectives for its FIS Technology Centers system. Those objectives are based on the service commitments that FIS makes to user entities; the laws and regulations that govern the provision of the FIS Technology Centers system; and the financial, operational, and compliance requirements that FIS has established for the services. The security commitments to user entities are documented and communicated in contracts and other agreements. FIS' principal service commitments include, but are not limited to, the following:

- Protection of user entities' information against unauthorized access, modification, or disclosure;
- Providing for the availability of services supporting user accounts;
- Use of encryption technologies to protect customer data both at rest and in transit; and
- Conduct standards dictating security, availability, and privacy standards.

FIS establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in FIS' system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected.

F. Additional Information about Management's Description

FIS' applicable Trust Services Criteria and related controls are included within Section IV of this report, "Description of the Trust Services Category, Criteria, Fidelity Information Services, LLC's Related Controls, and the Independent Service Auditor's Description of Tests and Results." Although the applicable Trust Services Criteria and related controls are presented within Section IV, they are, nevertheless, an integral part of the Company's description of its system as described within this section.

G. Non-Applicable Trust Services Criteria

There were no non-applicable Trust Services Criteria noted.

H. Changes to the System During the Specified Period

There were no changes that are likely to affect report users' understanding of how the FIS Technology Centers system is used to provide the service during the specified period.

I. System Incidents

There were no system incidents identified by management during the specified period that were the result of controls that were not suitably designed or operating effectively that management is aware of. There were also not any incidents during the specified period that resulted in a significant failure in the achievement of one or more of the Company's service commitments and/or system requirements that management is aware of.

J. Subservice Organizations

The Company utilizes a subservice organization to perform certain functions to improve operating and administrative effectiveness. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the subservice organization described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at this subservice organization.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organization and are necessary to achieve specific control objectives, along with the associated subservice organization, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organization. Each user entity's internal control over financial reporting must be evaluated in conjunction with the Company's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Subservice Organization	Service(s) Provided and Complementary Subservice Organization Controls	Criterion Addressed
Digital Realty	Digital Realty is responsible for hosting services and for managing infrastructure services and operations. The following control areas are critical to achieving the applicable control objectives: • Controls provide reasonable assurance that physical access to the Data Center is restricted to properly authorized individuals. • Controls provide reasonable assurance that the physical environment is monitored and protected from disruptive events.	CC 6.4*

Subservice Organization	Service(s) Provided and Complementary Subservice Organization Controls	Criterion Addressed
	In addition, the Company has identified the following Control Activity to help monitor the subservice organization: • A documented vendor management policy defines requirements for vendor management activities including due diligence, ongoing monitoring, and oversight of third-party relationships. The Digital Realty SOC report is reviewed on an annual basis.	

* The achievement of design and operating effectiveness related to this Trust Services Criterion assumes that complementary controls at this subservice organization that support this criterion are in place and are operating effectively.

K. User Entity Controls

The Company's controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company's service commitments and system requirements to be achieved based on the applicable trust services criteria solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related testing detailed in Section IV of this report, taking into account the related complementary user entity controls identified within the table below, where applicable. Complementary user entity controls and their associated criteria are included within the table below.

Management has highlighted criterion in which complementary user entity controls were assumed in the design of the Company's system with an asterisk. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control environment to determine if the identified complementary user entity controls have been implemented and are operating effectively.

Furthermore, the table below includes suggested control considerations that the Company believes each user organization should consider in developing their internal controls or planning their audits that are relevant to the Company's controls detailed in this report, however, such control considerations are not required to achieve design or operating effectiveness for the Company's service commitments and system requirements based on the applicable trust services criteria. The following list of suggested control activities is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user entity. Accordingly, this list does not allege to be, and is not, a complete listing of all the control activities which provide a basis for the assertions underlying the control environments for the Company's user entities.

User Entity Controls	Associated Criteria
Controls should be established to perform penetration testing on all client-owned internet facing applications and client-owned/managed infrastructure.	CC 2.1*, CC 2.2, CC 3.1, CC 3.2, CC 3.3, CC 3.4, CC 4.1, CC 4.2, CC 5.1*, CC 5.3, CC 6.1*, CC 6.6*, CC 6.7*, CC 6.8*, CC 7.1*, CC 7.2*, CC 7.3*, CC 7.4*
Controls should be established to notify FIS of changes made to each user entity's authorized technical or administrative contact information in a timely manner.	CC 2.2*, CC 2.3*, CC 5.2*, CC 6.2*, CC 6.3*, CC 7.3*, CC 7.4*
Controls should be established to notify FIS of unusual activity, violations, and/or security breaches identified.	CC 2.3*, CC 7.3*, CC 7.4*

User Entity Controls	Associated Criteria
Controls should be established to restrict physical and logical access to authorized personnel for systems sending data to and receiving data from FIS.	CC 5.2*, CC 6.1*, CC 6.2*, CC 6.3*, CC 6.4*, CC 6.6*, CC 6.7*, CC 6.8*
Controls should be established to supervise, manage, and monitor the use of FIS' services by user entity personnel. Among the access controls which should be considered are the following items: • An individual with sufficient authority and accountability should be assigned to the security function; • Passwords should be kept confidential, should be changed on a regular basis, and should be in conformity with user entity policies; • Access to subsystems and sensitive transactions should be restricted to authorized individuals; • Procedures to communicate, monitor, and approve security requests should be established and followed; • Transferred and terminated users should be removed completely, accurately, and timely; and • User access should be periodically reviewed and maintained.	CC 5.2*, CC 6.1*, CC 6.2*, CC 6.3*, CC 6.4*, CC 6.6*, CC 6.7*, CC 6.8*
Controls should be established to review, test, and approve requested changes made to production systems and configurations.	CC 5.2*, CC 8.1*
Controls should be established to review system access on a periodic basis to help ensure access is appropriate.	CC 5.2*, CC 6.2*, CC 6.3*

* This is a complementary control and is required to achieve design and operating effectiveness for this particular criterion.

IV. Description of the Trust Services Category, Criteria, Fidelity Information Services, LLC's Related Controls, and the Independent Service Auditor's Description of Tests and Results

A. Types and Descriptions of the Tests of Operating Effectiveness

This report, when combined with an understanding of the controls at user entities and the subservice organization, is intended to provide user entities of the Company's System, those prospective user entities, practitioners providing services to such user entities, and other specified parties with information about the control features of the Company's System. The description is intended to provide users with information about the System. Our examination was limited to the applicable trust services criteria and related controls specified by the Company in Sections III and IV of the report and did not extend to the controls in effect at user entities and the subservice organization. It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user entity to assess the total internal control environment. If internal control is not effective at user entities, the Company's controls may not compensate for such weaknesses.

The Company's system of internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by the Company. In planning the nature, timing, and extent of our testing of the controls to achieve the Company's service commitments and system requirements based on the applicable trust services criteria, we considered aspects of the Company's control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Type	Description
Inquiry	Inquired of appropriate personnel and corroborated with management
Observation	Observed the application, performance, or existence of the control
Inspection	Inspected documents, records, or other evidence indicating performance of the control
Reperformance	Reperformed the control, or processing of the application control, for accuracy of its operation

In addition, when using information produced (or provided by) the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

B. Trust Service Category, Criteria, and Controls

The trust services criteria relevant to security address that information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the Company's ability to achieve its service commitments and system requirements.

COMMON CRITERIA

CRITERIA GROUP 1: Control Environment		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	
	5	An annual program has been implemented to communicate the Company's Code of Conduct, security policies and practices, and procedures for submitting complaints and/or non-ethical behavior to employees. As part of the program, each employee must confirm his/her understanding of and compliance with the Company's Code of Conduct and security policies on an annual basis. (A)
	6	Consequences for non-compliance of job responsibility and security policies, up to and including termination, are addressed within the FIS Employee Handbook which is made available to employees on the intranet.
	2	Managers are required to perform performance appraisals of employees annually to confirm that skilled personnel are in place to achieve objectives.
	8	The Information Security Department is responsible for reviewing, updating, and issuing security policies.
	13	Company employees are required to participate in annual security awareness training, which includes information regarding the process to notify members of the Information Security Department of possible security breaches and the limitation on the user of information systems.
	1	The Company uses a formal structure for employee assignments which includes written job descriptions that contain job requirements, job related competencies, and business and professional competencies.
	4	The Company’s new employees and contractors must sign a statement signifying that they have read, understand, and will follow the security policies and the Company’s Code of Conduct.
	71	An Acceptable Use Policy establishes the requirements regarding the proper use of the Company’s systems/data/resources.
CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
	11	The Board of Directors is responsible for overseeing the Business Continuity Management System which monitors the integrity of the Business Continuity Policies. Specific responsibilities are outlined within the Business Continuity Policy.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the “Restricted Use” section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 1: Control Environment		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	10	A Charter has been adopted by the Company's Board of Directors to assist the Board and its committees in the exercise of their responsibilities. The Charter requires the establishment of an Audit Committee to oversee the functions of Internal Audit and requires sufficient members to be independent from management.
	7	The Chief Audit Executive reports directly to the Audit Committee of the Board both functionally and administratively.
	9	The Company's organizational structure provides the framework for defining key areas of authority and responsibility, as well as for establishing lines of reporting. The Company is designed as a vertical structure with business lines reporting upward to the CEO. The Chief Compliance Officer and the Chief Risk Officer report independently from operations.
	72	The Vulnerability Governance Committee has been established to provide ongoing measurement and monitoring of the risk-rating methodology, to perform scenario analysis, and to implement changes as needed to address the risk tolerance and prioritization for identified network and application vulnerabilities. This committee meets quarterly and maintains meeting minutes, action items, and follows up on open action items.
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
	72	The Vulnerability Governance Committee has been established to provide ongoing measurement and monitoring of the risk-rating methodology, to perform scenario analysis, and to implement changes as needed to address the risk tolerance and prioritization for identified network and application vulnerabilities. This committee meets quarterly and maintains meeting minutes, action items, and follows up on open action items.
	31	The Vendor Risk Management Policy requires that vendors who have access to confidential data or who perform a managed service related to the operation of the System be reviewed based on the vendor's classification. Based on the vendor classification, the Company either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 Type II reports, or the third party is subjected to continuous monitoring controls.
	9	The Company's organizational structure provides the framework for defining key areas of authority and responsibility, as well as for establishing lines of reporting. The Company is designed as a vertical structure with business lines reporting upward to the CEO. The Chief Compliance Officer and the Chief Risk Officer report independently from operations.
	8	The Information Security Department is responsible for reviewing, updating, and issuing security policies.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 1: Control Environment		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	1	The Company uses a formal structure for employee assignments which includes written job descriptions that contain job requirements, job related competencies, and business and professional competencies.
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
	15	Background checks are performed for all new contractors.
	14	New personnel background checks include, but are not limited to, a criminal record review, a credit check, an education verification, and a drug test, where applicable.
	5	An annual program has been implemented to communicate the Company's Code of Conduct, security policies and practices, and procedures for submitting complaints and/or non-ethical behavior to employees. As part of the program, each employee must confirm his/her understanding of and compliance with the Company's Code of Conduct and security policies on an annual basis. (A)
	6	Consequences for non-compliance of job responsibility and security policies, up to and including termination, are addressed within the FIS Employee Handbook which is made available to employees on the intranet.
	2	Managers are required to perform performance appraisals of employees annually to confirm that skilled personnel are in place to achieve objectives.
	8	The Information Security Department is responsible for reviewing, updating, and issuing security policies.
	13	Company employees are required to participate in annual security awareness training, which includes information regarding the process to notify members of the Information Security Department of possible security breaches and the limitation on the user of information systems.
	1	The Company uses a formal structure for employee assignments which includes written job descriptions that contain job requirements, job related competencies, and business and professional competencies.
CC 1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
	69	Internal audits are performed based on a risk-based assessment plan for the environments.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the “Restricted Use” section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 1: Control Environment		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	6	Consequences for non-compliance of job responsibility and security policies, up to and including termination, are addressed within the FIS Employee Handbook which is made available to employees on the intranet.
	9	The Company's organizational structure provides the framework for defining key areas of authority and responsibility, as well as for establishing lines of reporting. The Company is designed as a vertical structure with business lines reporting upward to the CEO. The Chief Compliance Officer and the Chief Risk Officer report independently from operations.
	2	Managers are required to perform performance appraisals of employees annually to confirm that skilled personnel are in place to achieve objectives.
	8	The Information Security Department is responsible for reviewing, updating, and issuing security policies.
	1	The Company uses a formal structure for employee assignments which includes written job descriptions that contain job requirements, job related competencies, and business and professional competencies.

CRITERIA GROUP 2: Communication and Information		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
CC 2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	
	35	The Intrusion Detection System and Intrusion Prevention System (IDS/IPS) software is automatically configured to monitor the network perimeter and to intercede and/or provide alert notifications to appropriate personnel. Alert logs are reconciled and tracked for all business days.
	33	Network monitoring systems are deployed and are actively running on the Company's network to log events and to detect anomalous activities.
	18	The Information Security Department utilizes a combination of commercial and custom tools to conduct vulnerability scans and security tests to detect malware and/or other potential security vulnerabilities. Identified vulnerabilities are tracked and reported to management based on their risk rating.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 2: Communication and Information		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	34	The Company conducts web-application and/or network penetration testing on an annual basis for FIS-owned internet facing applications and FIS-owned/managed infrastructure.
	32	During the annual risk assessment process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors which may threaten the achievement of business objectives and/or impact security. The potential threats to system objectives are updated based on these reviews.
	8	The Information Security Department is responsible for reviewing, updating, and issuing security policies.
	1	The Company uses a formal structure for employee assignments which includes written job descriptions that contain job requirements, job related competencies, and business and professional competencies.
	69	Internal audits are performed based on a risk-based assessment plan for the environments.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
	39	FIS security changes are communicated to both internal and external users on the FIS Client Portal.
	12	Either a member of the Legal Department and/or a member of the Procurement Department is responsible for the review of all third-party contracts and for confirming that any third-party contracts include applicable security practices and commitments.
	37	The Company's security commitments and customer responsibilities, which include responsibilities for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are described on the FIS website and within system documentation.
	38	A description of the Company's products and services, including boundaries and commitments, is documented and communicated to internal and external users through the FIS website and/or Client Portal.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 2: Communication and Information		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	20	Management monitors employees' compliance with the code of conduct through monitoring of customer and employee complaints and through the use of an anonymous third-party-administered ethics hotline. The results of the compliance and code of conduct monitoring are communicated to the Audit Committee on a quarterly basis.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	5	An annual program has been implemented to communicate the Company's Code of Conduct, security policies and practices, and procedures for submitting complaints and/or non-ethical behavior to employees. As part of the program, each employee must confirm his/her understanding of and compliance with the Company's Code of Conduct and security policies on an annual basis. (A)
	3	The Information Security Department or the Corporate Privacy Department is responsible for monitoring the integrity of security policies, including the Records Management Policy. Specific responsibilities are outlined within the Information Security Policy and are communicated on the FIS and Me intranet.
	8	The Information Security Department is responsible for reviewing, updating, and issuing security policies.
	13	Company employees are required to participate in annual security awareness training, which includes information regarding the process to notify members of the Information Security Department of possible security breaches and the limitation on the user of information systems.
	1	The Company uses a formal structure for employee assignments which includes written job descriptions that contain job requirements, job related competencies, and business and professional competencies.
	4	The Company's new employees and contractors must sign a statement signifying that they have read, understand, and will follow the security policies and the Company's Code of Conduct.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	
	39	FIS security changes are communicated to both internal and external users on the FIS Client Portal.
	3	The Information Security Department or the Corporate Privacy Department is responsible for monitoring the integrity of security policies, including the Records Management Policy. Specific responsibilities are outlined within the Information Security Policy and are communicated on the FIS and Me intranet.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 2: Communication and Information		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	12	Either a member of the Legal Department and/or a member of the Procurement Department is responsible for the review of all third-party contracts and for confirming that any third-party contracts include applicable security practices and commitments.
	37	The Company's security commitments and customer responsibilities, which include responsibilities for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are described on the FIS website and within system documentation.
	38	A description of the Company's products and services, including boundaries and commitments, is documented and communicated to internal and external users through the FIS website and/or Client Portal.
	20	Management monitors employees' compliance with the code of conduct through monitoring of customer and employee complaints and through the use of an anonymous third-party-administered ethics hotline. The results of the compliance and code of conduct monitoring are communicated to the Audit Committee on a quarterly basis.

CRITERIA GROUP 3: Risk Assessment		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
CC 3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	8	The Information Security Department is responsible for reviewing, updating, and issuing security policies.
	1	The Company uses a formal structure for employee assignments which includes written job descriptions that contain job requirements, job related competencies, and business and professional competencies.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 3: Risk Assessment		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	32	During the annual risk assessment process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors which may threaten the achievement of business objectives and/or impact security. The potential threats to system objectives are updated based on these reviews.
CC 3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	32	During the annual risk assessment process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors which may threaten the achievement of business objectives and/or impact security. The potential threats to system objectives are updated based on these reviews.
	31	The Vendor Risk Management Policy requires that vendors who have access to confidential data or who perform a managed service related to the operation of the System be reviewed based on the vendor's classification. Based on the vendor classification, the Company either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 Type II reports, or the third party is subjected to continuous monitoring controls.
CC 3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	
	40	The Company's annual risk assessment includes an assessment of fraud risk and considers opportunities for unauthorized acquisition, use, or disposal of assets; altering the Company's reporting records; committing other inappropriate acts; and the threats and vulnerabilities which could arise specifically from the use of IT and access to information.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	32	During the annual risk assessment process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors which may threaten the achievement of business objectives and/or impact security. The potential threats to system objectives are updated based on these reviews.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 3: Risk Assessment		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	9	The Company's organizational structure provides the framework for defining key areas of authority and responsibility, as well as for establishing lines of reporting. The Company is designed as a vertical structure with business lines reporting upward to the CEO. The Chief Compliance Officer and the Chief Risk Officer report independently from operations.
	8	The Information Security Department is responsible for reviewing, updating, and issuing security policies.
	32	During the annual risk assessment process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors which may threaten the achievement of business objectives and/or impact security. The potential threats to system objectives are updated based on these reviews.
	31	The Vendor Risk Management Policy requires that vendors who have access to confidential data or who perform a managed service related to the operation of the System be reviewed based on the vendor's classification. Based on the vendor classification, the Company either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 Type II reports, or the third party is subjected to continuous monitoring controls.

CRITERIA GROUP 4: Monitoring Activities		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
CC 4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	
	35	The Intrusion Detection System and Intrusion Prevention System (IDS/IPS) software is automatically configured to monitor the network perimeter and to intercede and/or provide alert notifications to appropriate personnel. Alert logs are reconciled and tracked for all business days.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 4: Monitoring Activities		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	33	Network monitoring systems are deployed and are actively running on the Company's network to log events and to detect anomalous activities.
	18	The Information Security Department utilizes a combination of commercial and custom tools to conduct vulnerability scans and security tests to detect malware and/or other potential security vulnerabilities. Identified vulnerabilities are tracked and reported to management based on their risk rating.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	34	The Company conducts web-application and/or network penetration testing on an annual basis for FIS-owned internet facing applications and FIS-owned/managed infrastructure.
	69	Internal audits are performed based on a risk-based assessment plan for the environments.
CC 4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	
	36	When an incident is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and is tracked to resolution.
	35	The Intrusion Detection System and Intrusion Prevention System (IDS/IPS) software is automatically configured to monitor the network perimeter and to intercede and/or provide alert notifications to appropriate personnel. Alert logs are reconciled and tracked for all business days.
	33	Network monitoring systems are deployed and are actively running on the Company's network to log events and to detect anomalous activities.
	18	The Information Security Department utilizes a combination of commercial and custom tools to conduct vulnerability scans and security tests to detect malware and/or other potential security vulnerabilities. Identified vulnerabilities are tracked and reported to management based on their risk rating.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 4: Monitoring Activities		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	34	The Company conducts web-application and/or network penetration testing on an annual basis for FIS-owned internet facing applications and FIS-owned/managed infrastructure.
	6	Consequences for non-compliance of job responsibility and security policies, up to and including termination, are addressed within the FIS Employee Handbook which is made available to employees on the intranet.
	69	Internal audits are performed based on a risk-based assessment plan for the environments.

CRITERIA GROUP 5: Control Activities		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
CC 5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	
	35	The Intrusion Detection System and Intrusion Prevention System (IDS/IPS) software is automatically configured to monitor the network perimeter and to intercede and/or provide alert notifications to appropriate personnel. Alert logs are reconciled and tracked for all business days.
	33	Network monitoring systems are deployed and are actively running on the Company's network to log events and to detect anomalous activities.
	18	The Information Security Department utilizes a combination of commercial and custom tools to conduct vulnerability scans and security tests to detect malware and/or other potential security vulnerabilities. Identified vulnerabilities are tracked and reported to management based on their risk rating.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	34	The Company conducts web-application and/or network penetration testing on an annual basis for FIS-owned internet facing applications and FIS-owned/managed infrastructure.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 5: Control Activities		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	9	The Company's organizational structure provides the framework for defining key areas of authority and responsibility, as well as for establishing lines of reporting. The Company is designed as a vertical structure with business lines reporting upward to the CEO. The Chief Compliance Officer and the Chief Risk Officer report independently from operations.
	8	The Information Security Department is responsible for reviewing, updating, and issuing security policies.
	32	During the annual risk assessment process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors which may threaten the achievement of business objectives and/or impact security. The potential threats to system objectives are updated based on these reviews.
CC 5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	
	22	The Company has implemented a formal Business Project Management Methodology (BPMM) in support of the Systems Development Life Cycle (SDLC) methodology which governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology. The Business Project Management Methodology (BPMM) includes a framework for evaluating risk, confirming availability and performance requirements, and confirming project conformance to architecture and security standards, including the classification of data and the appropriate treatment of information in the event of a loss of security.
	49	In accordance with the Change Authorization Policy, all changes made to FIS infrastructure, applications and services must be authorized by appropriate levels of management through a defined change management process.
	50	Separate libraries for test and production environments have been established.
	51	Access to promote changes into production is limited to appropriate individuals without development responsibilities.
	52	Logical access to schedule and execute jobs is limited to automated interfaces and authorized personnel based on job responsibilities.
	42	The use of group or shared IDs is not permitted unless approved by management.
	43	Privileged access rights to the servers, operating systems, and supporting systems and infrastructure, including the ability to make changes to logical access rights, are restricted based on job responsibilities.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 5: Control Activities		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	48	In accordance with the Change Authorization Policy, emergency changes are tracked via a ticket system and require after the fact approval.
	73	The FIS Enterprise Identity and Access Management Policy forces users to select long passwords and passphrases, including spaces and all printable characters; and employs automated tools to assist the user in selecting strong passwords and authenticators.
	74	The Encryption Policy and Standard requires that passwords must be encrypted at rest and in motion.
	53	A manual request from an authorized client requestor or approval from authorized FIS personnel must be received before a new client user is set up for the servers, operating systems, and supporting infrastructure.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	
	35	The Intrusion Detection System and Intrusion Prevention System (IDS/IPS) software is automatically configured to monitor the network perimeter and to intercede and/or provide alert notifications to appropriate personnel. Alert logs are reconciled and tracked for all business days.
	33	Network monitoring systems are deployed and are actively running on the Company's network to log events and to detect anomalous activities.
	18	The Information Security Department utilizes a combination of commercial and custom tools to conduct vulnerability scans and security tests to detect malware and/or other potential security vulnerabilities. Identified vulnerabilities are tracked and reported to management based on their risk rating.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	34	The Company conducts web-application and/or network penetration testing on an annual basis for FIS-owned internet facing applications and FIS-owned/managed infrastructure.
	36	When an incident is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and is tracked to resolution.
	2	Managers are required to perform performance appraisals of employees annually to confirm that skilled personnel are in place to achieve objectives.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 5: Control Activities		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	3	The Information Security Department or the Corporate Privacy Department is responsible for monitoring the integrity of security policies, including the Records Management Policy. Specific responsibilities are outlined within the Information Security Policy and are communicated on the FIS and Me intranet.
	8	The Information Security Department is responsible for reviewing, updating, and issuing security policies.
	1	The Company uses a formal structure for employee assignments which includes written job descriptions that contain job requirements, job related competencies, and business and professional competencies.

CRITERIA GROUP 6: Logical and Physical Access Controls		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	
	17	A master list of FIS system components is maintained, accounting for additions and removals, for management's use.
	54	Logical access to the backup application is restricted to appropriate employees based on job function.
	55	Back-up tapes are encrypted during the back-up process (when feasible), are rotated/transmitted offsite, and are transported in locked containers via a secured courier truck for the data centers.
	24	Laptops used to access the Company's network are encrypted in accordance with Company policy.
	57	The Encryption Architecture Review Committee (EARC) performs a review of the encryption technologies in place. Any identified issues are researched and resolved.
	35	The Intrusion Detection System and Intrusion Prevention System (IDS/IPS) software is automatically configured to monitor the network perimeter and to intercede and/or provide alert notifications to appropriate personnel. Alert logs are reconciled and tracked for all business days.
	60	Servers are built according to documented build standards.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 6: Logical and Physical Access Controls		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	59	Direct access to the in-scope databases is restricted to appropriate personnel based on job function.
	58	Privileged access is governed via a password vault. Users must first log in with their usernames and passwords. Logging on the password vault is enabled to track individuals accessing privileged accounts.
	21	FIS Company policy requires that the Reporting Manager records the employee and contractor termination in the HR system and access is removed within five business days of separation. Automated jobs are configured to run every 15 minutes to disable Active Directory access. (B)
	41	A valid username and password set in accordance with Company policy, including password length, expiration, history, complexity and number of failed login attempts are required to access the in-scope systems. (B)
	23	Remote access to network resources, including mobile access, is controlled through the use of SecurID tokens and/or a Virtual Private Network (VPN), subject to password security settings, to create encrypted private communications when remotely accessing network resources. Users are granted VPN access based on management approval.
	52	Logical access to schedule and execute jobs is limited to automated interfaces and authorized personnel based on job responsibilities.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	43	Privileged access rights to the servers, operating systems, and supporting systems and infrastructure, including the ability to make changes to logical access rights, are restricted based on job responsibilities.
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
	44	Logical access to the FIS network is requested and approved by management based on business need and job responsibilities.
	45	Logical access for FIS users to in-scope applications, servers and databases is requested and approved by management based upon business need and job responsibilities.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the “Restricted Use” section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 6: Logical and Physical Access Controls		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	46	Logical access for FIS users to supporting infrastructure (e.g., firewalls and network devices) is requested and approved by management based upon business need and job responsibilities.
	47	Logical access is reviewed by management on a quarterly basis to validate that user access levels for in-scope servers, operating systems, databases, and supporting infrastructure is appropriate.
	42	The use of group or shared IDs is not permitted unless approved by management.
	21	FIS Company policy requires that the Reporting Manager records the employee and contractor termination in the HR system and access is removed within five business days of separation. Automated jobs are configured to run every 15 minutes to disable Active Directory access. (B)
	53	A manual request from an authorized client requestor or approval from authorized FIS personnel must be received before a new client user is set up for the servers, operating systems, and supporting infrastructure.
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
	42	The use of group or shared IDs is not permitted unless approved by management.
	21	FIS Company policy requires that the Reporting Manager records the employee and contractor termination in the HR system and access is removed within five business days of separation. Automated jobs are configured to run every 15 minutes to disable Active Directory access. (B)
	44	Logical access to the FIS network is requested and approved by management based on business need and job responsibilities.
	45	Logical access for FIS users to in-scope applications, servers and databases is requested and approved by management based upon business need and job responsibilities.
	46	Logical access for FIS users to supporting infrastructure (e.g., firewalls and network devices) is requested and approved by management based upon business need and job responsibilities.
	47	Logical access is reviewed by management on a quarterly basis to validate that user access levels for in-scope servers, operating systems, databases, and supporting infrastructure is appropriate.
	53	A manual request from an authorized client requestor or approval from authorized FIS personnel must be received before a new client user is set up for the servers, operating systems, and supporting infrastructure.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 6: Logical and Physical Access Controls		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	
	61	Physical access is granted based upon job responsibility, according to a defined process, which requires management approval to validate that employee access is commensurate with job responsibilities.
	63	Physical access of terminated employees is removed within one business day following notification from Human Resources or management.
	62	The ability to implement changes to physical access rights is limited to defined administrative personnel to prevent unauthorized changes.
	70	Badge access readers restrict access to all external access points.
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
	64	Company policies state that client information that has exceeded its retention period is securely purged, destroyed, or overwritten in accordance with business requirements and client specifications.
	27	The Company has established a Data Classification and Handling Standard which addresses data retention and disposal to help ensure that confidential client information is retained and disposed to meet the Company's confidentiality commitments and system requirements.
	25	Data Loss Protection (DLP) software is enabled to prevent unauthorized data removal through removable media, except where required by approved business need.
	75	Company policy stipulates that any records containing personal information, regardless of the method of storage (e.g., electronic, portable media, or paper-based), be disposed of in a secure manner or securely sanitized prior to reuse to help prevent loss, theft, misuse, and/or unauthorized access.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
	26	Network devices (e.g., routers, switches, firewalls) are deployed and are maintained to detect and prevent threats to the Company's environment.
	52	Logical access to schedule and execute jobs is limited to automated interfaces and authorized personnel based on job responsibilities.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 6: Logical and Physical Access Controls		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	35	The Intrusion Detection System and Intrusion Prevention System (IDS/IPS) software is automatically configured to monitor the network perimeter and to intercede and/or provide alert notifications to appropriate personnel. Alert logs are reconciled and tracked for all business days.
	33	Network monitoring systems are deployed and are actively running on the Company's network to log events and to detect anomalous activities.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	54	Logical access to the backup application is restricted to appropriate employees based on job function.
	21	FIS Company policy requires that the Reporting Manager records the employee and contractor termination in the HR system and access is removed within five business days of separation. Automated jobs are configured to run every 15 minutes to disable Active Directory access. (B)
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
	56	Company policy states that transmissions of electronic information is encrypted as the default setting over public networks via secure transmission protocols (e.g., HTTPS, SFTP, VPN, and TLS) and that system data is encrypted at rest.
	52	Logical access to schedule and execute jobs is limited to automated interfaces and authorized personnel based on job responsibilities.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	54	Logical access to the backup application is restricted to appropriate employees based on job function.
	55	Back-up tapes are encrypted during the back-up process (when feasible), are rotated/transmitted offsite, and are transported in locked containers via a secured courier truck for the data centers.
	24	Laptops used to access the Company's network are encrypted in accordance with Company policy.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 6: Logical and Physical Access Controls		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	25	Data Loss Protection (DLP) software is enabled to prevent unauthorized data removal through removable media, except where required by approved business need.
	59	Direct access to the in-scope databases is restricted to appropriate personnel based on job function.
	58	Privileged access is governed via a password vault. Users must first log in with their usernames and passwords. Logging on the password vault is enabled to track individuals accessing privileged accounts.
	21	FIS Company policy requires that the Reporting Manager records the employee and contractor termination in the HR system and access is removed within five business days of separation. Automated jobs are configured to run every 15 minutes to disable Active Directory access. (B)
	23	Remote access to network resources, including mobile access, is controlled through the use of SecurID tokens and/or a Virtual Private Network (VPN), subject to password security settings, to create encrypted private communications when remotely accessing network resources. Users are granted VPN access based on management approval.
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	
	28	Antivirus software is implemented and is updated to help protect programs, data, and other information resources from viruses and malware.
	51	Access to promote changes into production is limited to appropriate individuals without development responsibilities.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	60	Servers are built according to documented build standards.
	58	Privileged access is governed via a password vault. Users must first log in with their usernames and passwords. Logging on the password vault is enabled to track individuals accessing privileged accounts.
	43	Privileged access rights to the servers, operating systems, and supporting systems and infrastructure, including the ability to make changes to logical access rights, are restricted based on job responsibilities.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 6: Logical and Physical Access Controls		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	21	FIS Company policy requires that the Reporting Manager records the employee and contractor termination in the HR system and access is removed within five business days of separation. Automated jobs are configured to run every 15 minutes to disable Active Directory access. (B)

CRITERIA GROUP 7: System Operations		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	
	18	The Information Security Department utilizes a combination of commercial and custom tools to conduct vulnerability scans and security tests to detect malware and/or other potential security vulnerabilities. Identified vulnerabilities are tracked and reported to management based on their risk rating.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	34	The Company conducts web-application and/or network penetration testing on an annual basis for FIS-owned internet facing applications and FIS-owned/managed infrastructure.
CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	
	18	The Information Security Department utilizes a combination of commercial and custom tools to conduct vulnerability scans and security tests to detect malware and/or other potential security vulnerabilities. Identified vulnerabilities are tracked and reported to management based on their risk rating.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 7: System Operations		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	34	The Company conducts web-application and/or network penetration testing on an annual basis for FIS-owned internet facing applications and FIS-owned/managed infrastructure.
CC 7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	
	29	For all instances of unauthorized use or disclosure of personal information, the affected information is appropriately identified.
	30	Security incidents are evaluated to determine whether the incident could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws and regulations.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	36	When an incident is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and is tracked to resolution.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	
	68	Data restore testing is performed on at least an annual basis to verify the integrity of the backup data.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	36	When an incident is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and is tracked to resolution.
	16	Clients are notified if the FIS Security Incident Response Team (FSIRT) determines that a specific, direct client impact related to security incidents has occurred.
	29	For all instances of unauthorized use or disclosure of personal information, the affected information is appropriately identified.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the “Restricted Use” section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 7: System Operations		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	30	Security incidents are evaluated to determine whether the incident could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws and regulations.
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	
	67	The Business Continuity and Disaster Recovery Plan is tested on at least an annual basis, and any issues are documented and tracked for resolution.
	66	Incremental and full backups for the in-scope servers and databases are configured to be performed based upon pre-defined frequency. Any issues are researched and resolved in accordance with the Company's Backup and Restoration policies.
	19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.
	68	Data restore testing is performed on at least an annual basis to verify the integrity of the backup data.
	16	Clients are notified if the FIS Security Incident Response Team (FSIRT) determines that a specific, direct client impact related to security incidents has occurred.

CRITERIA GROUP 8: Change Management		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	
	65	Logical access to the source code is restricted to appropriate personnel based on job responsibilities.
	17	A master list of FIS system components is maintained, accounting for additions and removals, for management's use.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the “Restricted Use” section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 8: Change Management		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	22	The Company has implemented a formal Business Project Management Methodology (BPMM) in support of the Systems Development Life Cycle (SDLC) methodology which governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology. The Business Project Management Methodology (BPMM) includes a framework for evaluating risk, confirming availability and performance requirements, and confirming project conformance to architecture and security standards, including the classification of data and the appropriate treatment of information in the event of a loss of security.
	49	In accordance with the Change Authorization Policy, all changes made to FIS infrastructure, applications and services must be authorized by appropriate levels of management through a defined change management process.
	50	Separate libraries for test and production environments have been established.
	51	Access to promote changes into production is limited to appropriate individuals without development responsibilities.
	60	Servers are built according to documented build standards.
	48	In accordance with the Change Authorization Policy, emergency changes are tracked via a ticket system and require after the fact approval.

CRITERIA GROUP 9: Risk Mitigation		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	
	11	The Board of Directors is responsible for overseeing the Business Continuity Management System which monitors the integrity of the Business Continuity Policies. Specific responsibilities are outlined within the Business Continuity Policy.
	67	The Business Continuity and Disaster Recovery Plan is tested on at least an annual basis, and any issues are documented and tracked for resolution.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the “Restricted Use” section of the accompanying Report of Independent Service Auditors.

CRITERIA GROUP 9: Risk Mitigation		
Ref.	**Applicable Trust Services Criteria**	
	#	**Company Control**
	66	Incremental and full backups for the in-scope servers and databases are configured to be performed based upon pre-defined frequency. Any issues are researched and resolved in accordance with the Company's Backup and Restoration policies.
	68	Data restore testing is performed on at least an annual basis to verify the integrity of the backup data.
	32	During the annual risk assessment process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors which may threaten the achievement of business objectives and/or impact security. The potential threats to system objectives are updated based on these reviews.
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	
	16	Clients are notified if the FIS Security Incident Response Team (FSIRT) determines that a specific, direct client impact related to security incidents has occurred.
	32	During the annual risk assessment process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors which may threaten the achievement of business objectives and/or impact security. The potential threats to system objectives are updated based on these reviews.
	31	The Vendor Risk Management Policy requires that vendors who have access to confidential data or who perform a managed service related to the operation of the System be reviewed based on the vendor's classification. Based on the vendor classification, the Company either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 Type II reports, or the third party is subjected to continuous monitoring controls.

(A) The Service Auditor noted that that this control or a portion of this control did not operate during the specified period; therefore, this control could not be tested for operating effectiveness. Refer to Section IV C for additional details.
(B) Exceptions noted. Refer to Section IV C for additional details.

This report is intended solely for the specified parties identified in the "Restricted Use" section of the accompanying Report of Independent Service Auditors.

C. Controls, Tests Performed and Results of Testing

Control Activity		Tests Performed By Service Auditor	Results of Testing
1	The Company uses a formal structure for employee assignments which includes written job descriptions that contain job requirements, job related competencies, and business and professional competencies.	**Inspection:** Inspected the job descriptions for a sample of active employees to determine that the Company used a formal structure for employee assignments which included written job descriptions that contained job requirements, job related competencies, and business and professional competencies.	No exceptions noted.
2	Managers are required to perform performance appraisals of employees annually to confirm that skilled personnel are in place to achieve objectives.	**Inspection:** Inspected the performance appraisal completion records for a sample of active employees to determine that managers completed a performance appraisal of employees during the specified period to confirm that skilled personnel were in place to achieve objectives.	No exceptions noted.
3	The Information Security Department or the Corporate Privacy Department is responsible for monitoring the integrity of security policies, including the Records Management Policy. Specific responsibilities are outlined within the Information Security Policy and are communicated on the FIS and Me intranet.	**Inquiry:** Inquired of Risk Analyst II to determine that throughout the specified period, Information Security Policy and the Records Management Policy the Information Security Policy was communicated on the FIS and Me intranet.	No exceptions noted
		Observation: Observed the FIS intranet site to determine that the Information Security Policy and the Records Management Policy was made available to employees on the intranet.	No exceptions noted
		Inspection: Inspected the Information Security Policy and the Records Management Policy to determine that the Information Security Department or the Corporate Privacy Department was responsible for monitoring the integrity of security policies, including the Records Management Policy. Further, determined that specific responsibilities were outlined within the Information Security Policy and were communicated on the FIS and Me intranet.	No exceptions noted

Control Activity		Tests Performed By Service Auditor	Results of Testing
4	The Company's new employees and contractors must sign a statement signifying that they have read, understand, and will follow the security policies and the Company's Code of Conduct.	**Inspection:** Inspected the signed statement for a sample of new employees and contractors to determine that the Company's new employees and contractors signed a statement signifying that they had read, understood, and would follow the security policies and the Company's Code of Conduct.	No exceptions noted.
5	An annual program has been implemented to communicate the Company's Code of Conduct, security policies and practices, and procedures for submitting complaints and/or non-ethical behavior to employees. As part of the program, each employee must confirm his/her understanding of and compliance with the Company's Code of Conduct and security policies on an annual basis.	**Inspection:** Inspected the Company's annual compliance program to determine that an annual program was implemented to communicate the Company's Code of Conduct, security policies and practices, and procedures for submitting complaints and/or non-ethical behavior.	No exceptions noted.
		Inspection: Inspected the Code of Conduct signoff documentation for a sample of employees to determine that as part of the program, each employee confirmed his/her understanding of and compliance with the Code of Conduct and security policies, within the last calendar year.	The Service Auditor noted that this control activity did not operate during the specified period, as the annual signoff did not occur during the specified period. Therefore, this control activity could not be tested for operating effectiveness.
		Inspection: Inspected the Company's annual compliance program implemented to communicate the Company's Code of Conduct, security policies and practices, and procedures for submitting complaints and/or non-ethical behavior produced by the Risk Analyst to determine that the annual program was not performed within the specified period and scheduled to be performed annually at the end of the calendar year.	No exceptions noted.
6	Consequences for non-compliance of job responsibility and security policies, up to and including termination, are addressed within the FIS Employee Handbook which is made available to employees on the intranet.	**Inquiry:** Inquired of the Risk Analyst II to determine that throughout the specified period, the FIS Employee Handbook was made available to employees on the intranet.	No exceptions noted.
		Observation: Observed the FIS intranet site to determine that the FIS Employee Handbook was made available to employees on the intranet.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
		Inspection: Inspected the FIS Employee Handbook to determine that consequences for non-compliance of job responsibility and security policies, up to and including termination, were addressed.	No exceptions noted.
7	The Chief Audit Executive reports directly to the Audit Committee of the Board both functionally and administratively.	**Inspection:** Inspected the Audit Committee Charter to determine that the Chief Audit Executive reported directly to the Audit Committee of the Board both functionally and administratively.	No exceptions noted.
8	The Information Security Department is responsible for reviewing, updating, and issuing security policies.	**Inspection:** Inspected the Information Security Policy and the Policy Management Policy to determine that the Information Security Department was responsible for reviewing, updating, and issuing the security policies.	No exceptions noted
9	The Company's organizational structure provides the framework for defining key areas of authority and responsibility, as well as for establishing lines of reporting. The Company is designed as a vertical structure with business lines reporting upward to the CEO. The Chief Compliance Officer and the Chief Risk Officer report independently from operations.	**Inspection:** Inspected the FIS Colleague Finder to determine that the Company's organizational structure provided the framework for defining key areas of authority and responsibility, as well as for establishing lines of reporting. Further, determined that the Company was designed as a vertical structure with business lines reporting upward to the CEO. And that the Chief Compliance Officer and the Chief Risk Officer reported independently from operations.	No exceptions noted.
10	A Charter has been adopted by the Company's Board of Directors to assist the Board and its committees in the exercise of their responsibilities. The Charter requires the establishment of an Audit Committee to oversee the functions of Internal Audit and requires sufficient members to be independent from management.	**Inspection:** Inspected the Company's Charter to determine that a Charter had been adopted by the Company's Board of Directors to assist the Board and its committees in the exercise of their responsibilities. Further, determined that the Charter required the establishment of an Audit Committee to oversee the functions of Internal Audit and required sufficient members to be independent from management.	No exceptions noted.
11	The Board of Directors is responsible for overseeing the Business Continuity Management System which monitors the integrity of the Business Continuity Policies. Specific responsibilities are outlined within the Business Continuity Policy.	**Inspection:** Inspected the Business Continuity Policy to determine that the Board of Directors was responsible for overseeing the Business Continuity Management System which monitored the integrity of the Business Continuity Policies. Additionally, determined that specific responsibilities were outlined within the Business Continuity Policy.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
12	Either a member of the Legal Department and/or a member of the Procurement Department is responsible for the review of all third-party contracts and for confirming that any third-party contracts include applicable security practices and commitments.	**Inspection:** Inspected the contracts and supporting review evidence for a sample of new third-party contracts to determine that a member of the Legal Department and/or Procurement Department reviewed all third-party contracts and confirmed that any third-party contracts included applicable security practices and commitments.	No exceptions noted.
13	Company employees are required to participate in annual security awareness training, which includes information regarding the process to notify members of the Information Security Department of possible security breaches and the limitation on the user of information systems.	**Inspection:** Inspected the security awareness training completion records for a sample of active employees to determine that company employees participated in annual security awareness training.	No exceptions noted.
		Inspection: Inspected the security awareness training materials to determine that security awareness training included information regarding the process to notify members of the Information Security Department of possible security breaches and the limitation on the user of information systems.	No exceptions noted.
14	New personnel background checks include, but are not limited to, a criminal record review, a credit check, an education verification, and a drug test, where applicable.	**Inspection:** Inspected the background screening documentation for a sample of new employees to determine that new personnel background checks included, but was not limited to, a criminal record review, a credit check, an education verification, and a drug test, where applicable.	No exceptions noted.
15	Background checks are performed for all new contractors.	**Inspection:** Inspected the pre-screening documentation for a sample of new contractors to determine that a background check was performed for new contractors.	No exceptions noted.
16	Clients are notified if the FIS Security Incident Response Team (FSIRT) determines that a specific, direct client impact related to security incidents has occurred.	**Inspection:** Inspected the client notifications for a sample of incidents which directly impacted clients' data to determine that clients were notified if the FIS Security Incident Response Team (FSIRT) determined that a specific, direct client impact related to security incidents had occurred for each selected incident.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
17	A master list of FIS system components is maintained, accounting for additions and removals, for management's use.	**Inquiry:** Inquired of the Risk Analyst to determine that throughout the specified period, a master list of FIS system components was maintained, accounting for additions and removals, for management's use.	No exceptions noted
		Observation: Observed the listing of FIS system components in the Single Technology Asset Repository (STAR) system to determine that a master list of FIS system components was maintained, accounting for additions and removals, for management's use.	No exceptions noted
18	The Information Security Department utilizes a combination of commercial and custom tools to conduct vulnerability scans and security tests to detect malware and/or other potential security vulnerabilities. Identified vulnerabilities are tracked and reported to management based on their risk rating.	**Inquiry:** Inquired of the Risk Analyst to determine that throughout the specified period, the Information Security Department utilized a combination of commercial and custom tools to conduct vulnerability scans and security tests to detect malware and/or other potential security vulnerabilities. Further, determined that identified vulnerabilities were automatically tracked and reported to management based on their risk rating.	No exceptions noted.
		Observation: Observed the commercial tools used to conduct internal and external network scanning to determine that the Information Security Department utilized a combination of commercial and custom tools to conduct vulnerability scans and security tests to detect malware and/or other potential security vulnerabilities. Further, observed the vulnerability management dashboard to determine that identified vulnerabilities were automatically tracked and reported to management based on their risk rating.	No exceptions noted.
19	Management monitors vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly or every other week cadence.	**Inspection:** Inspected the compliance metrics email reports for a sample of weeks to determine that management monitored vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on a weekly cadence.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
		Inspection: Inspected the compliance metrics email reports for a sample of bi-weeks to determine that management monitored vulnerability management reporting, risk ratings, remediation priorities, escalation of past-due vulnerabilities, end of life devices, and remediation projects related to passwords, FTP, and transmission encryption, through e-mails sent on an every other week cadence.	No exceptions noted.
20	Management monitors employees' compliance with the code of conduct through monitoring of customer and employee complaints and through the use of an anonymous third-party-administered ethics hotline. The results of the compliance and code of conduct monitoring are communicated to the Audit Committee on a quarterly basis.	**Inquiry:** Inquired of the Risk Analyst II to determine that throughout the specified period, an active ethics hotline existed and was available for use.	No exceptions noted.
		Observation: Observed the third-party-administered ethics hotline on the intranet and any other publicly available source to determine that an active ethics hotline existed and was available for use.	No exceptions noted.
		Inspection: Inspected the Audit Committee meeting minutes for a sample of quarters to determine that management monitored employees' compliance with the code of conduct through monitoring of customer and employee complaints and through the use of an anonymous third-party-administered hotline, and that the results of the compliance and code of conduct monitoring were communicated to the Audit Committee.	No exceptions noted.
21	FIS Company policy requires that the Reporting Manager records the employee and contractor termination in the HR system and access is removed within five business days of separation. Automated jobs are configured to run every 15 minutes to disable Active Directory access.	**Inspection:** Inspected the FIS Enterprise Identity and Access Management Policy to determine that the policy required the Reporting Manager to record the employee and contractor termination in the HR system.	No exceptions noted.
		Inspection: Inspected the automated job set up between Active Directory and the HR system to determine that jobs were configured to be run every 15 minutes to disable Active Directory Access.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
		Inspection: Inspected the Active Directory Activity Log for a sample of terminated employees and contractors to determine that the termination date was recorded in the HR system timely so that Active Directory access could be disabled within five business days.	No exceptions noted.
		Inspection: Inspected all daily job logs between Active Directory and the HR system for pre dated terminations to determine that all jobs ran successfully to disable Active Directory access.	Exception noted. The Service Auditor noted that 1 out of 274 daily batch jobs did not run successfully and did not change users status' to "terminated".
		Inspection: Inspected all job logs between Active Directory and the HR system for all user access changes to determine that all jobs ran successfully every 15 minutes to disable Active Directory access.	No exceptions noted.
22	The Company has implemented a formal Business Project Management Methodology (BPMM) in support of the Systems Development Life Cycle (SDLC) methodology which governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology. The Business Project Management Methodology (BPMM) includes a framework for evaluating risk, confirming availability and performance requirements, and confirming project conformance to architecture and security standards, including the classification of data and the appropriate treatment of information in the event of a loss of security.	**Inspection:** Inspected the Business Project Management Methodology to determine that the Company had implemented a formal Business Project Management Methodology (BPMM) in support of the Systems Development Life Cycle (SDLC) methodology which governed the development, acquisition, implementation, and maintenance of computerized information systems and related technology. Further, determined that the BPMM included a framework for evaluating risk, confirming availability and performance requirements, and confirming project conformance to architecture and security standards, including the classification of data and appropriate treatment of information in the event of a loss of security.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
23	Remote access to network resources, including mobile access, is controlled through the use of SecurID tokens and/or a Virtual Private Network (VPN), subject to password security settings, to create encrypted private communications when remotely accessing network resources. Users are granted VPN access based on management approval.	**Inquiry:** Inquired of the Risk Analyst to determine that throughout the specified period, remote access was controlled through the use of SecurID tokens and/or a Virtual Private Network (VPN), subject to password security settings, to create encrypted private communications when remotely accessing network resources.	No exceptions noted.
		Observation: Observed the process for remotely accessing network resources, including mobile access to determine that remote access was controlled through the use of SecurID tokens and/or a Virtual Private Network (VPN), subject to password security settings, to create encrypted private communications when remotely accessing network resources.	No exceptions noted.
		Inspection: Inspected the management approval forms for a sample of employees granted VPN access to determine that remote access was granted based on management approval.	No exceptions noted.
24	Laptops used to access the Company's network are encrypted in accordance with Company policy.	**Inspection:** Inspected the Company's End-User Device Encryption Standard to determine that Company policy required that laptops be encrypted to access the Company's network.	No exceptions noted.
		Inspection: Inspected the encryption settings related for a sample of laptops to determine that each laptop was encrypted to access the Company's network.	No exceptions noted.
25	Data Loss Protection (DLP) software is enabled to prevent unauthorized data removal through removable media, except where required by approved business need.	**Inquiry:** Inquired of the IT Security Analyst Specialist to determine that throughout the specified period, DLP software was enabled to prevent unauthorized data removal through removable media, except where required by approved business need.	No exceptions noted.
		Observation: Observed the system configuration management console to determine that DLP software was distributed automatically to computers on the Company's Network to prevent unauthorized data removal through removable media.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
		Inspection: Inspected the approval forms for a sample of users without DLP software enabled to determine that management approved the DLP exception.	No exceptions noted.
26	Network devices (e.g., routers, switches, firewalls) are deployed and are maintained to detect and prevent threats to the Company's environment.	**Inspection:** Inspected the network diagram to determine that network devices (e.g., routers, switches, firewalls) were documented and maintained to detect and prevent threats to the Company's environment.	No exceptions noted.
		Inspection: Inspected the logging configurations, NTP configurations, and password policies for a sample of network devices (e.g. routers, switches, firewalls) to determine that network devices were deployed and maintained to detect and prevent threats to the Company's environment.	No exceptions noted.
27	The Company has established a Data Classification and Handling Standard which addresses data retention and disposal to help ensure that confidential client information is retained and disposed to meet the Company's confidentiality commitments and system requirements.	**Inspection:** Inspected the Company's Data Classification and Handling Standard to determine that the Company had established a Data Classification and Handling Standard which addressed data retention and disposal to help ensure that confidential client information was retained and disposed to meet the Company's confidentiality commitments and system requirements.	No exceptions noted
28	Antivirus software is implemented and is updated to help protect programs, data, and other information resources from viruses and malware.	**Inquiry:** Inquired of the Risk Analyst to determine that throughout the specified period, the antivirus software was implemented and updated to help protect programs, data, and other information resources from viruses and malware.	No exceptions noted.
		Inspection: Inspected the antivirus policy management console's configurations to determine that antivirus software was implemented and was updated to help protect programs, data, and other information resources from viruses and malware.	No exceptions noted.
29	For all instances of unauthorized use or disclosure of personal information, the affected information is appropriately identified.	**Inspection:** Inspected the incident and reporting documentation for a sample of unauthorized use or disclosure of personal information to determine that the affected information was appropriately identified.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
30	Security incidents are evaluated to determine whether the incident could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws and regulations.	**Inspection:** Inspected the incident ticket and supporting documentation for a sample of security incidents to determine that security incidents were evaluated to determine whether the incident could or did result in the unauthorized disclosure or use of personal information and whether there had been a failure to comply with applicable laws and regulations.	No exceptions noted.
31	The Vendor Risk Management Policy requires that vendors who have access to confidential data or who perform a managed service related to the operation of the System be reviewed based on the vendor's classification. Based on the vendor classification, the Company either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 Type II reports, or the third party is subjected to continuous monitoring controls.	**Inspection:** Inspected the Vendor Risk Management Policy to determine that the policy required vendors who had access to confidential data or who performed a managed service related to the operation of the System be reviewed based on the vendor's classification.	No exceptions noted.
		Inspection: Inspected the vendor review documentation for a sample of vendors to determine that based on the vendor classification, the Company either performed a vendor security assessment of the third party, reviewed the third party's System and Organization Control reports such as SOC 2 Type II reports, or the third party was subjected to continuous monitoring controls.	No exceptions noted.
32	During the annual risk assessment process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors which may threaten the achievement of business objectives and/or impact security. The potential threats to system objectives are updated based on these reviews.	**Inspection:** Inspected the annual risk assessment documentation to determine that risk management personnel identified changes to business objectives, commitments and requirements, internal operations, and external factors which threatened the achievement of business objectives and/or impact security. Further determined that the potential threats to system objectives were updated based on these reviews.	No exceptions noted.
33	Network monitoring systems are deployed and are actively running on the Company's network to log events and to detect anomalous activities.	**Inquiry:** Inquired of the IT Security Manager to determine that throughout the specified period, network monitoring systems were deployed and were actively running on the Company's network to log events and to detect anomalous activities.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
		Observation: Observed the network monitoring tool to determine that network monitoring systems were deployed and were actively running on the Company's network to log events and to detect anomalous activities.	No exceptions noted.
34	The Company conducts web-application and/or network penetration testing on an annual basis for FIS-owned internet facing applications and FIS-owned/managed infrastructure.	**Inspection:** Inspected the penetration summary for a sample of web-application and networks to determine that the Company conducted testing on an annual basis for FIS-owned internet facing applications and FIS-owned/managed infrastructure.	No exceptions noted.
35	The Intrusion Detection System and Intrusion Prevention System (IDS/IPS) software is automatically configured to monitor the network perimeter and to intercede and/or provide alert notifications to appropriate personnel. Alert logs are reconciled and tracked for all business days.	**Inquiry:** Inquired of the IT Security Manager to determine that throughout the specified period, the Intrusion Detection System and Intrusion Prevention System (IPS/IDS) software was automatically configured to monitor the network perimeter and to intercede and/or provide alert notifications to appropriate personnel. Further determined that alert logs were reconciled and tracked for all business days.	No exceptions noted.
		Observation: Observed the IPS/IDS software configurations to determine that the (IDS/IPS) software was automatically configured to monitor the network perimeter and to intercede and/or provide alert notifications to appropriate personnel.	No exceptions noted.
		Inspection: Inspected the IDS/IPS automatic ticket configurations to determine that alert notifications were automatically created into SNOW tickets.	No exceptions noted.
		Inspection: Inspected the reconciliation reports for a sample of days to determine that alert logs were reconciled and tracked for all business days.	No exceptions noted.
36	When an incident is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and is tracked to resolution.	**Inspection:** Inspected the incident ticket for a sample of incidents to determine that when an incident was detected or reported, a defined incident management process was initiated by appropriate personnel and included a root cause analysis and was tracked to resolution.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
37	The Company's security commitments and customer responsibilities, which include responsibilities for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, are described on the FIS website and within system documentation.	**Inquiry:** Inquired of the Risk Analyst II to determine that throughout the specified period, the Company's security commitments and customer responsibilities, which include responsibilities for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, were described on the FIS website and within system documentation.	No exceptions noted.
		Observation: Observed the FIS Client Portal and FIS Ethics Helpline to determine that the Company's security commitments and customer responsibilities, which include responsibilities for reporting operational failures, incidents, problems, concerns and complaints, and the process for doing so, were described on the FIS website and within system documentation.	No exceptions noted.
38	A description of the Company's products and services, including boundaries and commitments, is documented and communicated to internal and external users through the FIS website and/or Client Portal.	**Inquiry:** Inquired of the Risk Analyst II to determine that throughout the specified period, a description of the Company's products and services, including boundaries and commitments, was documented and communicated to internal and external users through the FIS website and/or Client Portal.	No exceptions noted.
		Observation: Observed the FIS Client Portal to determine that a description of the Company's products and services, including boundaries and commitments, was documented and communicated to internal and external users through the FIS website and/or Client Portal.	No exceptions noted.
39	FIS security changes are communicated to both internal and external users on the FIS Client Portal.	**Inquiry:** Inquired of the Risk Analyst II to determine that throughout the specified period, FIS security changes were communicated to both internal and external users on the FIS Client Portal.	No exceptions noted.
		Observation: Observed the FIS Client Portal to determine that FIS security changes were communicated to both internal and external users on the FIS Client Portal.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
40	The Company's annual risk assessment includes an assessment of fraud risk and considers opportunities for unauthorized acquisition, use, or disposal of assets; altering the Company's reporting records; committing other inappropriate acts; and the threats and vulnerabilities which could arise specifically from the use of IT and access to information.	**Inspection:** Inspected the annual risk assessment results to determine that the Company's annual risk assessment included an assessment of fraud risk and considered opportunities for unauthorized acquisition, use, or disposal of assets; altering the Company's reporting records; committing other inappropriate acts; and the threats and vulnerabilities which could arise specifically from the use of IT and access to information.	No exceptions noted.
41	A valid username and password set in accordance with Company policy, including password length, expiration, history, complexity and number of failed login attempts are required to access the in-scope systems.	**Inspection:** Inspected the RACF and ACF2 Mainframe password parameters to determine that a valid username and password set in accordance with Company policy, including password length, expiration, history, complexity and number of failed login attempts were required to access the servers, operating systems, and supporting infrastructure.	No exceptions noted.
		Inspection: Inspected the UNIX/Linux user authentication settings to determine that user access is granted through multi-factor authentication through BoKs.	No exceptions noted.
		Inspection: Inspected the Windows password parameters to determine that a valid username and password set in accordance with Company policy, including password length, expiration, history, complexity and number of failed login attempts were required to access the servers, operating systems, and supporting infrastructure.	No exceptions noted.
		Inspection: Inspected the HP Nonstop and Enscribe HP password parameters to determine that a valid username and password set in accordance with Company policy, including password length, expiration, history, complexity and number of failed login attempts were required to access the servers, operating systems, and supporting infrastructure.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
		Inspection: Inspected the SQL and Windows authentication credentials to determine that the server authentication required both SQL Server and Windows credentials and password parameters included a valid username and passwords were set in accordance with Company policy, including password length, expiration, history, complexity and number of failed login attempts were required to access the servers, operating systems, and supporting infrastructure.	No exceptions noted.
		Inspection: Inspected the Oracle password parameters to determine that a valid username and password set in accordance with Company policy, including password length, expiration, history, complexity and number of failed login attempts were required to access the servers, operating systems, and supporting infrastructure.	No exceptions noted.
		Inspection: Inspected the Unisys/DMSII password parameters to determine that a valid username and password set in accordance with Company policy, including password length, expiration, history, complexity and number of failed login attempts were required to access the servers, operating systems, and supporting infrastructure.	No exceptions noted.
		Inspection: Inspected the IBM i password parameters to determine that a valid username and password set in accordance with Company policy, including password length, expiration, history, complexity and number of failed login attempts were required to access the servers, operating systems, and supporting infrastructure.	Exception noted. The Service Auditor noted that password complexity requirements were not configured as part of the IBM i password.
42	The use of group or shared IDs is not permitted unless approved by management.	**Inspection:** Inspected the system generated user listings for in-scope systems to determine that the use of group or shared IDs was not permitted unless approved by management.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
43	Privileged access rights to the servers, operating systems, and supporting systems and infrastructure, including the ability to make changes to logical access rights, are restricted based on job responsibilities.	**Inspection:** Inspected the system-generated listing of users with privileged access rights for a sample of servers, operating systems, and databases to determine that access rights were restricted based on job responsibilities.	No exceptions noted.
		Inspection: Inspected the system-generated listing of users with privileged access rights to supporting systems and infrastructure (including access to modify transmission protocols, network device configurations and firewall rule settings) to determine that access rights were restricted based on job responsibilities.	No exceptions noted.
44	Logical access to the FIS network is requested and approved by management based on business need and job responsibilities.	**Inspection:** Inspected new hire forms for a sample of new hires granted logical access to the FIS network to determine that logical access was requested and approved by management based upon business need or job responsibilities.	No exceptions noted.
45	Logical access for FIS users to in-scope applications, servers and databases is requested and approved by management based upon business need and job responsibilities.	**Inspection:** Inspected the access request ticket for a sample of new hires that were granted logical access to the FIS in-scope applications, servers and databases to determine that logical access was requested and approved by management based upon business need or job responsibilities.	No exceptions noted.
46	Logical access for FIS users to supporting infrastructure (e.g., firewalls and network devices) is requested and approved by management based upon business need and job responsibilities.	**Inspection:** Inspected the access request ticket for a sample of new hires that were granted logical access to the supporting infrastructure (e.g., firewalls and network devices) to determine that logical access was requested and approved by management based upon business need or job responsibilities.	No exceptions noted.
47	Logical access is reviewed by management on a quarterly basis to validate that user access levels for in-scope servers, operating systems, databases, and supporting infrastructure is appropriate.	**Inspection:** Inspected the access request ticket for a sample of new hires that were granted logical access to the supporting infrastructure (e.g., firewalls and network devices) to determine that logical access was requested and approved by management based upon business need or job responsibilities.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
48	In accordance with the Change Authorization Policy, emergency changes are tracked via a ticket system and require after the fact approval.	**Inspection:** Inspected the change tickets for a sample of emergency changes to determine that they were tracked via a ticket system and required after the fact approval, in accordance with the Change Authorization Policy.	No exceptions noted.
49	In accordance with the Change Authorization Policy, all changes made to FIS infrastructure, applications and services must be authorized by appropriate levels of management through a defined change management process.	**Inspection:** Inspected the ticket documentation for a sample of changes to determine that all changes made to FIS infrastructure, applications and services were authorized by appropriate levels of management through a defined change management process.	No exceptions noted.
50	Separate libraries for test and production environments have been established.	**Inquiry:** Inquired of the Risk Analyst II to determine that throughout the specified period, separate libraries for test and production environments were established.	No exceptions noted.
		Observation: Observed the separate environments to determine that separate libraries for test and production environments were established.	No exceptions noted.
51	Access to promote changes into production is limited to appropriate individuals without development responsibilities.	**Inspection:** Inspected the HP Nonstop user access listing to determine that access to promote changes into production was limited to appropriate individuals without development responsibilities.	No exceptions noted.
		Inspection: Inspected the Unisys and DMSII user access listing to determine that access to promote changes into production was limited to appropriate individuals without development responsibilities.	No exceptions noted.
		Inspection: Inspected the Linux Servers user access listing to determine that access to promote changes into production was limited to appropriate individuals without development responsibilities.	No exceptions noted.
		Inspection: Inspected the IBM i user access listing to determine that access to promote changes into production was limited to appropriate individuals without development responsibilities.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
		Inspection: Inspected the UNIX Servers user access listing to determine that access to promote changes into production was limited to appropriate individuals without development responsibilities.	No exceptions noted.
		Inspection: Inspected the Windows user access listing to determine that access to promote changes into production was limited to appropriate individuals without development responsibilities.	No exceptions noted.
		Inspection: Inspected the Mainframe user access listing to determine that access to promote changes into production was limited to appropriate individuals without development responsibilities.	No exceptions noted.
52	Logical access to schedule and execute jobs is limited to automated interfaces and authorized personnel based on job responsibilities.	**Inspection:** Inspected the user access listing to determine that logical access to schedule and execute jobs was limited to automated interfaces and authorized personnel based on job responsibilities.	No exceptions noted.
53	A manual request from an authorized client requestor or approval from authorized FIS personnel must be received before a new client user is set up for the servers, operating systems, and supporting infrastructure.	**Inspection:** Inspected the client request form for a sample of new client users to determine that the form originated from an authorized client requestor or approval from authorized FIS personnel was obtained before a new client user was set up for the servers, operating systems, and supporting infrastructure.	No exceptions noted.
54	Logical access to the backup application is restricted to appropriate employees based on job function.	**Inspection:** Inspected the user access listing to determine that logical access to the backup application was restricted to appropriate employees based on job function.	No exceptions noted.
55	Back-up tapes are encrypted during the back-up process (when feasible), are rotated/transmitted offsite, and are transported in locked containers via a secured courier truck for the data centers.	**Inquiry:** Inquired of the Risk Analyst II, to determine that throughout the specified period, back-up tapes were encrypted during the back-up process (when feasible), were rotated/transmitted offsite, and were transported in locked containers via a secured courier truck for the data centers.	No exceptions noted.
		Observation: Observed the backup configurations to determine that back-up tapes were encrypted during the back-up process.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
		Inspection: Inspected the Iron Mountain Service Agreement to determine that back-up tapes were transported in locked containers via a secured courier truck.	No exceptions noted.
		Inspection: Inspected the Iron Mountain reports for a sample of days to determine that back-up tapes were rotated/transmitted offsite for the data centers.	No exceptions noted.
56	Company policy states that transmissions of electronic information is encrypted as the default setting over public networks via secure transmission protocols (e.g., HTTPS, SFTP, VPN, and TLS) and that system data is encrypted at rest.	**Inspection:** Inspected the Encryption Policy to determine that transmissions of electronic information was encrypted as the default setting over public networks via secure transmission protocols (e.g., HTTPS, SFTP, VPN, and TLS) and that system data was encrypted at rest.	No exceptions noted.
57	The Encryption Architecture Review Committee (EARC) performs a review of the encryption technologies in place. Any identified issues are researched and resolved.	**Inspection:** Inspected the EARC Review Process documentation for a sample of encryption reviews to determine that a review was performed over encryption technologies in place and that any identified issues were researched and resolved.	No exceptions noted.
58	Privileged access is governed via a password vault. Users must first log in with their usernames and passwords. Logging on the password vault is enabled to track individuals accessing privileged accounts.	**Inquiry:** Inquired of the Risk Analyst II to determine that throughout the specified period, privileged access was governed via a password vault. Users must first log in with their usernames and passwords. Logging on the password vault was enabled to track individuals accessing privileged accounts.	No exceptions noted.
		Observation: Observed the password vaults to determine that privileged access was governed via a password vault. Users must first log in with their usernames and passwords. Logging on the password vault was enabled to track individuals accessing privileged accounts.	No exceptions noted.
59	Direct access to the in-scope databases is restricted to appropriate personnel based on job function.	**Inspection:** Inspected the user access listing to determine that direct access to the in-scope databases was restricted to appropriate personnel based on job function.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
60	Servers are built according to documented build standards.	**Inspection:** Inspected the Secure Configuration Policy to determine that servers were built according to documented build standards.	No exceptions noted.
		Inspection: Inspected the server build documentation for a sample of new server builds to determine that they were built according to documented build standards.	No exceptions noted.
61	Physical access is granted based upon job responsibility, according to a defined process, which requires management approval to validate that employee access is commensurate with job responsibilities.	**Inspection:** Inspected the access approval forms for a sample of users granted physical access to determine that user access was granted based upon job responsibility, according to a defined process, which required management approval to validate that employee access was commensurate with job responsibilities.	No exceptions noted.
62	The ability to implement changes to physical access rights is limited to defined administrative personnel to prevent unauthorized changes.	**Inspection:** Inspected the physical administrative access listings to determine that the ability to implement changes to physical access rights was limited to defined administrative personnel to prevent unauthorized changes.	No exceptions noted.
63	Physical access of terminated employees is removed within one business day following notification from Human Resources or management.	**Inspection:** Inspected the badge access disablement documentation for a sample of terminated employees to determine that physical access was removed within one business day following notification from Human Resources or management.	No exceptions noted.
64	Company policies state that client information that has exceeded its retention period is securely purged, destroyed, or overwritten in accordance with business requirements and client specifications.	**Inspection:** Inspected the Data Protection Policy to determine that Company policies state that client information that had exceeded its retention period was securely purged, destroyed, or overwritten in accordance with business requirements and client specifications.	No exceptions noted.
65	Logical access to the source code is restricted to appropriate personnel based on job responsibilities.	**Inspection:** Inspected the user access listings to determine that logical access to the source code was restricted to appropriate personnel based on job responsibilities.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
66	Incremental and full backups for the in-scope servers and databases are configured to be performed based upon pre-defined frequency. Any issues are researched and resolved in accordance with the Company's Backup and Restoration policies.	**Inspection:** Inspected the incremental and full backup up configurations to determine that backups for the in-scope servers and databases were configured to be performed based upon pre-defined frequency.	No exceptions noted.
		Inspection: Inspected the tickets for a sample of backup issues to determine that any issues were researched and resolved.	No exceptions noted.
67	The Business Continuity and Disaster Recovery Plan is tested on at least an annual basis, and any issues are documented and tracked for resolution.	**Inspection:** Inspected the Business Continuity and Disaster Recovery Plans to determine that each plan was tested on at least an annual basis and any issues were documented and resolved.	No exceptions noted.
68	Data restore testing is performed on at least an annual basis to verify the integrity of the backup data.	**Inspection:** Inspected the data restore testing results to determine that testing was performed on at least an annual basis to verify the integrity of the backup data.	No exceptions noted.
69	Internal audits are performed based on a risk-based assessment plan for the environments.	**Inspection:** Inspected the risk based assessment plan to determine that internal audits were scheduled based on a risk-based assessment plan for the environments.	No exceptions noted.
		Inspection: Inspected the internal audit reports/results to determine that internal audits were performed based on a risk-based assessment plan for the environments.	No exceptions noted.
70	Badge access readers restrict access to all external access points.	**Inquiry:** Inquired of the Risk Analyst II to determine that throughout the specified period, badge access readers restricted access to all external access points.	No exceptions noted.
		Observation: Observed the external access points to determine that badge access readers restricted access to all external access points.	No exceptions noted.
71	An Acceptable Use Policy establishes the requirements regarding the proper use of the Company's systems/data/resources.	**Inspection:** Inspected the Acceptable Use Policy to determine that an Acceptable Use Policy established the requirements regarding the proper use of the Company's systems/data/resources.	No exceptions noted.

Control Activity		Tests Performed By Service Auditor	Results of Testing
72	The Vulnerability Governance Committee has been established to provide ongoing measurement and monitoring of the risk-rating methodology, to perform scenario analysis, and to implement changes as needed to address the risk tolerance and prioritization for identified network and application vulnerabilities. This committee meets quarterly and maintains meeting minutes, action items, and follows up on open action items.	**Inspection:** Inspected the Vulnerability Governance Committee meeting minutes for a sample of quarters to determine that the committee met quarterly and maintained meeting minutes, action items, and follows up on open action items pertaining to the risk tolerance and prioritization for identified network and application vulnerabilities.	No exceptions noted.
73	The FIS Enterprise Identity and Access Management Policy forces users to select long passwords and passphrases, including spaces and all printable characters; and employs automated tools to assist the user in selecting strong passwords and authenticators.	**Inspection:** Inspected the FIS Enterprise Identity and Access Management Policy to determine that the policy forces users to select long passwords and passphrases, including spaces and all printable characters; and employs automated tools to assist the user in selecting strong passwords and authenticators.	No exceptions noted.
74	The Encryption Policy and Standard requires that passwords must be encrypted at rest and in motion.	**Inspection:** Inspected the Encryption Policy to determine that the policy and standard required that passwords must be encrypted at rest and in motion.	No exceptions noted.
75	Company policy stipulates that any records containing personal information, regardless of the method of storage (e.g., electronic, portable media, or paper-based), be disposed of in a secure manner or securely sanitized prior to reuse to help prevent loss, theft, misuse, and/or unauthorized access.	**Inspection:** Inspected the Information Classification and Handling Policy to determine that Company policy stipulated that any records containing personal information, regardless of the method of storage (e.g., electronic, portable media, or paper-based), be disposed of in a secure manner or securely sanitized prior to reuse to help prevent loss, theft, misuse, and/or unauthorized access.	No exceptions noted.

V. Other Information Provided by Fidelity Information Services, LLC

The information in this section describing activities and controls is presented by the Company to provide additional information to its users and is not part of the Company's description of controls. Such information has not been subjected to the procedures applied in the examination of the description of the Company's operations, and accordingly, we do not express an opinion on it.

A. Management's Responses to Testing Exceptions

Control Activity		Tests Performed By Service Auditor	Results of Testing
Applicable Trust Services Criteria: CC 6.1, CC 6.2, CC 6.3, CC 6.6, CC 6.7, CC 6.8			
21	FIS Company policy requires that the Reporting Manager records the employee and contractor termination in the HR system and access is removed within five business days of separation. Automated jobs are configured to run every 15 minutes to disable Active Directory access.	**Inspection:** Inspected all daily job logs between Active Directory and the HR system for pre dated terminations to determine that all jobs ran successfully to disable Active Directory access.	Exception noted. The Service Auditor noted that 1 out of 274 daily batch jobs did not run successfully and did not change user's status to "terminated".
Management's Response: Management acknowledges this exception. Management has disclosed the fact that Active Directory access was not automatically disabled within the expected five-day timeframe following a single maintenance window within the specified period. This exception was specific to the daily batch job which includes records of terminations which were communicated in advance of the date of termination. The Human Resources Information System (HRIS) team agrees that a single job was aborted and not rescheduled properly after routine maintenance was performed. The root cause was the impact created by the maintenance event. In the case of failure, these daily jobs will not re-run without manual intervention. This error was later identified, and the impacted records were processed accordingly. The impacted records had Active Directory access disabled after a total of 6 business days. FIS has multiple layers of controls in place which would have prevented the use of the access regardless of the fact that these user accounts remained active following the date of termination. At termination, each user would return all physical and logical access mechanisms (e.g., key cards, laptops, VPN tokens, etc.). Moving forward, following any scheduled maintenance, this job run is verified to have run successfully. Also, the HRIS team sends a nightly full file to the Active Directory (AD) team. The AD team completes a comparison between that file and the records within AD. Any identified differences are researched and resolved. No other outages occurred within the specified period. The control operated as described for the duration of the specified period otherwise.			

	Control Activity	Tests Performed By Service Auditor	Results of Testing
Applicable Trust Services Criteria: CC 6.1			
41	A valid username and password set in accordance with Company policy, including password length, expiration, history, complexity and number of failed login attempts are required to access the in-scope systems.	**Inspection:** Inspected the IBM i password parameters to determine that a valid username and password set in accordance with Company policy, including password length, expiration, history, complexity and number of failed login attempts were required to access the servers, operating systems, and supporting infrastructure.	Exception noted. The Service Auditor noted that password complexity requirements were not configured as part of the IBM i password.
Management's Response: Management acknowledges this exception. This deviation only relates to the (IBM i system in support of the ACBS application and is a direct result of the technical feasibility of the IBM i system. The ACBS application requires password complexity, but IBM i system ignores letter cases, effectively enforcing 2 (non case-sensitive letters and numbers) out of 4 (uppercase, lowercase, numbers, special characters) complexity requirements as defined in the FIS Policy. The application is developing a new password policy, requiring 3 out of 3 (letters, numbers, special characters). This change will affect the entire IBM i system, including the ACBS application, and direct IBM i log-ins. The result will mean that control will be compliant with the FIS Policy requirements. This update will be tested and deployed in stages. This change is expected to be completed by the end of Q2 2021.