Empowering
the Financial World

FIS

FIS Fixed Income Processing Suite (fka InTrader)

System and Organization Controls (SOC) for Service Organizations Report
for the period from January 1, 2022 to September 30, 2022

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 +1 312 602 8099

I. Report of Independent Service Auditors

To the Management and the Board of Directors of Fidelity Information Services, LLC:

Scope

We have examined Fidelity Information Services, LLC's (FIS) description of its FIS Fixed Income Processing Suite system (the "System") titled "Fidelity Information Services, LLC's Description of its System and Controls" for processing user entities' transactions ("description") throughout the period January 1, 2022 to September 30, 2022 (the "specified period") and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Fidelity Information Services, LLC's Assertion." The controls and control objectives included in the description are those that management of FIS believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in Section V of this report, "Other Information Provided by Fidelity Information Services, LLC" is presented by management of FIS to provide additional information and is not a part of FIS' description of its System made available to user entities during the specified period. Information about business continuity strategy, business continuity tactical overview and business continuity testing has not been subjected to the procedures applied in the examination of the description of the System and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the System and, accordingly, we express no opinion on it.

FIS uses FIS Computer Services, a subservice organization, for all of its infrastructure management services. The description in Section III of this report includes only the control objectives and related controls of FIS and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by FIS can be achieved only if complementary subservice organization controls assumed in the design of FIS' controls are suitably designed and operating effectively, along with the related controls at FIS. Our examination did not extend to controls of 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 certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of FIS' controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service organization's responsibilities
In Section II of this report, FIS has provided an assertion about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. FIS is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; selecting the criteria stated in the assertion; and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the specified period. 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:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion;
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- evaluating the overall presentation of the description, the suitability of the control objectives stated in the description, and the suitability of the criteria specified by the service organization in its assertion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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

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

Opinion
In our opinion, in all material respects, based on the criteria described in Fidelity Information Services, LLC's assertion:

a. The description fairly presents the FIS Fixed Income Processing Suite system that was designed and implemented throughout the period January 1, 2022 to September 30, 2022.
b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 2022 to September 30, 2022, and 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, 2022 to September 30, 2022.
c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period January 1, 2022 to September 30, 2022 if complementary subservice organization and user entity controls assumed in the design of Fidelity Information Services, LLC's controls operated effectively throughout the period January 1, 2022 to September 30, 2022.

Grant Thornton

Restricted use

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

Grant Thornton LLP

Chicago, Illinois
October 28, 2022

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

The SOC Logo is a proprietary trademark and service mark of the American Institute of Certified Public Accountants, which reserves all rights.

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

II. Fidelity Information Services, LLC’s Assertion

We have prepared the description of Fidelity Information Services, LLC’s (FIS) FIS Fixed Income Processing Suite system (the “System”) for processing user entities’ transactions throughout the period January 1, 2022 to September 30, 2022 (the “specified period”), for user entities of the System during some or all of the specified period, and their auditors who audit and report on such user entities’ financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the subservice organization and the user entities of the System themselves, when assessing the risks of material misstatements of the user entities’ financial statements.

FIS uses FIS Computer Services, a subservice organization, for all of its infrastructure management services. The description includes only the control objectives and related controls of FIS and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by FIS can be achieved only if the complementary subservice organization controls assumed in the design of FIS’ controls are suitably designed and operating effectively, along with the related controls at FIS. The description does not extend to the controls of the subservice organization.

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

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

A. The description fairly presents the System made available to user entities of the System during some or all of the specified period for processing their transactions as it relates to controls that are likely to be relevant to user entities’ internal control over financial reporting. The criteria we used in making this assertion were that the description:

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

      a. The type of services provided including, as appropriate, the classes of transactions processed;

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

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

d. How the system captures and addresses significant events and conditions other than transactions;

e. The process used to prepare reports or other information for user entities of the system;

f. Services performed by a subservice organization, if any, including whether the inclusive method or carve-out method has been used in relation to them;

g. The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the service organization’s controls; and

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

2. Includes relevant details of changes to FIS’ system during the specified period.

3. Does not omit or distort information relevant to FIS’ system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the System that each individual user entity of the System and its auditor may consider important in its own particular environment.

B. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the specified period to achieve those control objectives if the subservice organization and user entities applied the complementary controls assumed in the design of FIS’ controls throughout the specified period. The criteria we used in making this assertion were that:

1. The risks that threaten the achievement of the control objectives stated in the description have been identified by management of FIS;

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

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

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

A. About FIS

Fidelity Information Services, LLC (FIS or the “Company”) is a leading provider of technology solutions for financial institutions and businesses of all sizes and across any industry globally. We enable the movement of commerce by unlocking the financial technology that powers the world’s economy. Our employees are dedicated to advancing the way the world pays, banks and invests through our trusted innovation, system performance and flexible architecture. 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 member of the Fortune 500® and the Standard & Poor’s 500® Index. To learn more, visit www.fisglobal.com. Follow FIS on Facebook, LinkedIn and Twitter (@FISGlobal).

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.

B. 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. This 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 service commitments FIS makes with respect to any of the trust services categories (e.g., security, availability, confidentiality, processing integrity, or privacy), 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 the activities of 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 and Chief Executive Officer. The Chairman 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 Company 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.

C. Overview

FIS Fixed Income Processing Suite (fka FIS InTrader) is a leading integrated solution used by U.S. banks, thrifts and credit unions to effectively manage their institutions' investment portfolio, funding, and safekeeping activities. FIS provides FIS Fixed Income Processing Suite Application Service Provider (ASP) processing services for 33 customers. ASP hardware resides in the Hopkins, Minnesota, datacenter and is administered and monitored by FIS Fixed Income Processing Suite personnel according to established policies and procedures. Customers access FIS Fixed Income Processing Suite ASP through a Virtual Private Network (VPN) connection or Private IP (PIP) circuits.

FIS Fixed Income Processing Suite provides Remote Systems Administration (RSM) services for three (3) customers. There are six different levels of remote systems administration that a customer can select, ranging from monitoring and advising, to system, database and network administration. Generally, hardware is located at a customer's facility and is accessed and administered remotely by RSM personnel according to the level of service contracted by the customer. This report covers RSM customers that are at level 5 or level 6.

FIS Fixed Income Processing Suite operations are under the direction of the FIS Fixed Income Processing Suite General Manager, Vice Presidents, and functional level managers. FIS Fixed Income Processing Suite employs a staff of approximately 80 employees and is supported by the major functional areas listed below:

Sales and Marketing is responsible for sales, sales support, account management and marketing of FIS Fixed Income Processing Suite products.

Customer Service is responsible for customer support and customer issue tracking.

Quality Assurance (QA) is responsible for testing of application maintenance and enhancements.

Data Center Services is responsible for technical services, computer operations, and production support. Facility responsibilities are now under FIS Facilities. LAN/WAN responsibilities are now under FIS Networking.

Product Development is responsible for new application development, maintenance and enhancements to existing products.

Professional Services is responsible for providing professional services to current customers including conversions, installation support and customer training.

Information Security is responsible for overseeing information security controls and responding to customer related information security questionnaires.

Customer Information Risk Assessment Security Program

Many FIS Fixed Income Processing Suite customers are institutions that are regulated by one of the following federal agencies: Federal Banking Agencies (FBA), Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC) and Federal Reserve Board (FRB). These organizations require that FIS establish standards for safeguarding non-public customer information. As a service provider, FIS maintains non-public customer information by or on behalf of FIS Fixed Income Processing Suite customers, and must establish comparable standards.

FIS Fixed Income Processing Suite Senior Management is responsible for approving and enforcing the Customer Information Risk Assessment Security Program (CIRASP). The program defines information security requirements for FIS Fixed Income Processing Suite, the data center, contractors, vendors, clients and all third-party personnel. FIS Fixed Income Processing Suite Senior Management reviews the CIRASP at least once per calendar year and updates the CIRASP as required.

FIS Fixed Income Processing Suite Application

FIS Fixed Income Processing Suite is an integrated solution for bank treasury and portfolio management, clearance and settlement. FIS Fixed Income Processing Suite offers trading and sales, investment portfolio, safekeeping, funding and correspondent services. System input is online with automatic printing of confirmations after each transaction entry. FIS Fixed Income Processing Suite also provides numerous reports, on-line displays, and alerts necessary to manage these lines of business.

FIS Fixed Income Processing Suite ASP provides FIS Fixed Income Processing Suite customers with the ability to outsource the administration of their UNIX and FIS Fixed Income Processing Suite environments. FIS Fixed Income Processing Suite RSM, similar to FIS Fixed Income Processing Suite ASP, provides FIS Fixed Income Processing Suite customers the ability to outsource the administration of their UNIX and FIS Fixed Income Processing Suite environments, but still provide their own physical security of the UNIX server. FIS Fixed Income Processing Suite RSM and ASP allows the customer to focus on their core business and not be concerned with the costs and complexities of running and maintaining a UNIX based system.

FIS Fixed Income Processing Suite is a fully integrated application that maintains security positions and computes profit and loss (traded and settled). FIS Fixed Income Processing Suite maintains payment/delivery information, calculates and prepares accounting entries, produces regulatory reports and provides all necessary settlement and safekeeping reporting. FIS Fixed Income Processing Suite trading supports a wide variety of domestic and foreign fixed income and money market securities, including Treasury bills, bonds and notes, issues of government agencies, municipalities and corporations, certificates of deposit, commercial paper, and bankers' acceptances.

Security portfolios and positions for both the user and its customers are updated in real time as transactions are entered. There is a daily "accounting run" where settled positions are posted, income and expense is accrued, amortized, and accreted, and amounts are interfaced to the clients' general ledger and DDA systems. Several reports are generated during this accounting run to assist users in balancing and reconciling these interfaces.

Parameters are configured by the customer to determine how transactions (sales and trades) are processed and reported. All sales to a customer create a customer holding. A parameter on the customer determines whether their holdings should be included in Investment Portfolio reporting. A parameter on the Delivery method determines whether the holding is held in the user institution's safekeeping, and thereby whether it should be included in Safekeeping reporting. Subsequent to the initial sale, all or part of the holding may be moved in or out of custody, and therefore in or out of Safekeeping reporting.

All trades in FIS Fixed Income Processing Suite have a Customer, Portfolio, Security, Payment, and Delivery method. Parameters on individual business entities determine further processing. All trades create or update a Position for the user institution. Parameters on the portfolio indicate whether it is an issued money-market transaction, a Fed Fund, a Repurchase Agreement, or a secondary market securities trade. Parameters on the portfolio indicate whether it is a Trading account or an Investment Portfolio account, and thereby whether or not it is included in the user institution's Investment Portfolio reporting.

Scope

This report has been prepared to provide information on the FIS Fixed Income Processing Suite (ASP and RSM) system that may be relevant to the system of internal control of FIS Fixed Income Processing Suite's clients. This report, when combined with an understanding of the controls in place at user entities, is intended to assist in the understanding of FIS' controls related to the FIS Fixed Income Processing Suite (ASP and RSM) system.

This report covers both the FIS Fixed Income Processing Suite ASP and RSM delivery methods for the FIS Fixed Income Processing Suite product line. It is important that users of this report determine the specific product delivery method and configuration items for their specific use of FIS Fixed Income Processing Suite when assessing the testing and results included herein. In addition, there are six different levels of remote systems administration that a customer can select. This report covers RSM customers that are at level 5 or level 6.

The servers and databases are housed at the Hopkins Data Center (Hopkins, MN). The scope of this report is limited to the following applications:

Application/Tool	Supporting FIS Technology Center	Platform	Database
FIS Fixed Income Processing Suite ASP	Hopkins Data Center - Part of FIS Computer Services Voorhees Data Center – Part of FIS Computer Services	Oracle, Solaris	Progress
FIS Fixed Income Processing Suite RSM	Hopkins Data Center - Part of FIS Computer Services Voorhees Data Center – Part of FIS Computer Services	Oracle, Solaris	Progress

FIS Fixed Income Processing Suite uses FIS Computer Services as a subservice organization. A separate SOC 1 Type 2 report titled "FIS Computer Services" encompasses the underlying Information Technology (IT) general computing controls (GCC) environment for the FIS Fixed Income Processing Suite operations. The GCC report is available for users of this report and contains controls relating to physical security, environmental protection, logical access, system processing, change management, and backup and recovery. Additionally, a separate SOC 2 Type 2 report titled "FIS Computer Services Data Center Managed Hosting and FS-Cloud Applications" is available to provide users with information about the FIS Computer Services controls intended to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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*), including controls relating to Enterprise Policies, Standards and Communications; and Network Security.

Application Systems Development

Control Objective 1: Controls provide reasonable assurance that development of new FIS Fixed Income Processing Suite releases are documented, tested, and approved prior to migration into production.

1. FIS Fixed Income Processing Suite's Planning,
2. Execution, and
3. Release Management.

Planning

Backlog Management – The Product Backlog is a list of known requirements for application enhancements based on the FIS Fixed Income Processing Suite product roadmap. Responsibility for continuously populating, prioritizing, and otherwise maintaining the Backlog is held by Product Management and includes senior management representation.

Project Formalization and Initiation – Product Release planning is managed in regularly scheduled meetings with representation of stakeholders from Development, Client Services, Product Management, Operations, Quality Assurance and documentation. This process includes establishing content targets, documentation deliverables and schedules.

Risk Management – In the planning phase, any known risks are identified and documented along with any necessary mitigation plan.

Execution

Scrum-based Design, Development and Testing – Scrum teams made up of Product Owners, Developers and SQA specialists select and groom top priority requirements (stories) from the Product Backlog to fill a short-term development cycle known as a sprint. The team works together to understand user requirements, outline a functional and technical approach and establish acceptance criteria for validating effective execution. The team sizes the effort required for each story to establish the functional content of the sprint. During the sprint, daily collaboration within the team continues and each member contributes to the development, documentation and testing of each enhancement. Upon completion of each sprint, the enhancements are formally documented and demonstrated for stakeholders in the business unit whose feedback is collected as additional Backlog content.

- Software produced in the sprint undergoes a peer review process before being checked into the main code branch of the source code control system.
- At the close of the release cycle, a final application build is generated from the main code branch. This build represents the enhancements developed over several sprints for the Scrum teams participating in the release. The final build is delivered to the SQA department for a full regression test.

Impact Analysis – as software changes are made in the course of Scrum team activities, analysis is conducted to assess the potential downstream impact to consumers of the application data or services. This analysis is documented and shared with stakeholders internally and externally.

Documentation – Enhancements completed in a release cycle are reviewed by the Documentation department. FIS Fixed Income Processing Suite product documentation is updated to reflect software changes made to the product as necessary.

Security Management – At the end of each release development cycle, the code-base is subjected to a third-party security/vulnerability scan.

Release Management

Project Management – Each new release of FIS Fixed Income Processing Suite has an associated project folder in a document repository which contains release related documentation including: project schedule, scrum team turnover documents, risk and metric reports, release notes and announcements, and meeting notes from regular release stakeholder meetings.

Regression Testing – Each release undergoes a final phase of regression testing.

Analysis and Measurement – Metrics for each release are captured via queries within FIS Fixed Income Processing Suite's issue tracking system. The results are posted and reviewed by release stakeholders for each release.

Application Change Management

Control Objective 2: Controls provide reasonable assurance that FIS Fixed Income Processing Suite maintenance requests, including direct data changes, are documented, authorized, tested, and approved prior to migration into production.

A formal process is utilized for initiating, approving, completing, testing and implementing application maintenance requests, custom programming requests and government regulatory requirements. Customer Support personnel enter requests for application system changes into an on-line ticketing system. These requests are initiated in connection with problems encountered with an application or with specific user needs. Those items relating to applications are routed to appropriate programming personnel. Open items are monitored through a weekly status meeting and various reports.

Product Development is responsible for the design of the database structure best suited for the applications, FIS' operating environment, and anticipated future requirements by FIS. The establishment, issuance, and enforcement of change control and development standards are in place for data record design, incorporation of data and use of database files. These standards follow the same process as application change management.

When items are received by programming, the manager assigns the requests to an appropriate programming project leader or programmer for review. If the programmer needs more information to complete the request, the programmer will contact the initiator for additional information. Developers and SQA specialists work together as a team to lay out and execute a technical-development and testing approach to each remediation item, consulting with Product Management as needed. All application program modifications are made to copies of production versions in separate test libraries. Application programmers may not modify production versions of source code.

ASP Program Testing and Transfer to Production

FIS maintains separate environments for maintenance and custom programming, development, QA, regression testing, beta and acceptance testing, and production. The scope and method of unit, functional, and acceptance testing is determined and executed by the programming and SQA staff working as a team. Upon completion of the remediation, software is peer reviewed and checked into the main code-branch. A build of the application is then created and delivered to SQA for regression testing. Upon completion of the regression testing process with qualifying success, the build is prepared for a move into production.

Separate libraries are also maintained for job control, implemented as UNIX scripts. Test versions are used throughout the development and testing process and follow a similar path before movement into production.

Approval is required from the QA department on each standard software change to application programs and non-application software changes. Custom software changes require approvals from a Professional Services Manager/Supervisor. In addition, a representative from the customer must approve the custom software change. A formal policy is consistently followed to promote application programs and scripts into production to help outline that all controls are followed. Production Support, Unix Systems, or Network Services will not promote any change that does not meet stated policy requirements and are the only authorized personnel with the ability to move new and modified programs into production libraries and directories.

An application change that is of high priority and cannot wait for the regularly scheduled move cycle becomes a "Hot Move" or an emergency change. Prior to being moved into production, "Hot Moves" are processed through the QA Department. Additionally, signoff must be obtained from any other alternate department manager.

If Computer Operations identifies a problem requiring a change, it is considered an after-hours emergency change. Computer Operations first pages the person on-call and enters an incident ticket. If there is no response to the page, Computer Operations follows the normal escalation procedures in place for their department. The person on-call researches the issue. If they are able to resolve the issue, they do so by placing a software program into a temporary directory that allows the customer's processing to complete. The contents of the temporary directory will automatically be deleted when processing is complete and, if necessary, a permanent change will be developed, which follows the change management process identified above. Once the problem is resolved, the on-call person resolving the issue updates the incident ticket and sends a summarizing e-mail to an internal distribution list. The distribution list includes senior level and management level personnel. Customer Support will contact the client with any information that affects a missed deadline or next day processing.

ASP Data Change Management

FIS Fixed Income Processing Suite personnel are not authorized to originate or change data input by users without management and user approval. When data repair requests are made, FIS will evaluate the nature of the request and determine if a Data Repair Utility (DRU) can be developed to correct the data without interruption to the processing environment. The DRU Utility allows FIS to create a program to repair data, without having direct access to data. The DRU is a program that corrects historical data.

When FIS determines that a customer specific DRU needs to be created and executed, approval is required from an authorized customer representative. When FIS identifies a need to develop and execute a DRU against multiple customer environments, FIS Customer Support will send a notification explaining the need for the change and the nature of the repair to all customers affected before executing the DRU. In all instances, the DRU program source code is reviewed and approved by the FIS Fixed Income Processing Suite QA, Professional Services or Technical Manager prior to implementing the DRU. An e-mail notification is also sent to either a Development Manager or Professional Services Manager informing them when the change is being implemented.

RSM Application System Maintenance

RSM customers may request available FIS Fixed Income Processing Suite patch and release upgrades, shell script modifications and data changes at any point in time. The customer is responsible for requesting all changes. FIS Fixed Income Processing Suite personnel notify customers of the availability of new FIS Fixed Income Processing Suite patches, releases and shell scripts as they occur. Each customer is responsible for designating personnel that are authorized to request and approve FIS Fixed Income Processing Suite modifications. These requests are submitted to RSM personnel and entered into a formal change request form. Patch, release, data and shell script changes are initiated through requests from authorized customer personnel.

Patches and shell scripts are electronically delivered to the customer. New releases of FIS Fixed Income Processing Suite are delivered to a customer through a DVD. Patch and release documentation are updated and communicated to the client as appropriate. After the change is received by the customer, it is loaded onto the customer's server in the test environment. Exceptions to this rule can be requested by the customer to place a critical change directly into the production environment; however, a formal request must be submitted. New FIS Fixed Income Processing Suite releases will always be installed in a non-production environment without exception.

Once a patch, release and shell script change has been tested and approved to be promoted by a user, the change will be promoted into production. The change is moved through the users' unique change control script. The change control script contains specific information to a user's environment, including the release and patch level and all shell scripts. After a change is determined to be valid and authorized, the change control script is executed. A log of all moves is recorded in the change control script and an e-mail is sent to notify the customer of the completion of the move.

Operations Procedures

Control Objective 3: Controls provide reasonable assurance that processing (FIS Fixed Income Processing Suite nightly accounting runs), including backups, is scheduled appropriately and deviations from scheduled processing are identified and resolved.

Operations

The Computer Operations Department is responsible for the operation of the 24 hours per day data center that supports Application Service Provider (ASP) production processing. Telecommunications lines and/or VPN tunnels are maintained between FIS and all of its user organizations. FIS utilizes various Oracle servers using the Solaris operating system environment to support the majority of FIS Fixed Income Processing Suite ASP product line processing.

Remote Systems Management (RSM) is available from the Hopkins operations center. RSM provides FIS Fixed Income Processing Suite customers with the ability to outsource the administration of their UNIX and FIS Fixed Income Processing Suite environments. RSM allows the customer to focus on their core business and not be concerned with the costs and complexities of running and maintaining a UNIX based system. The RSM customers own and host the equipment used in the RSM environment.

In the FIS Fixed Income Processing Suite ASP and RSM environment, Computer Operations procedures, which have been developed and are available on-line on the company intranet and updated on a periodic basis, include normal operations and anticipated exceptions. Operators complete on-line incident reports for unusual situations that occur during the shift. These incidents are assigned to the proper support organization for follow-up and resolution. The majority of computer jobs are scheduled for execution via CA (Computer Associates), Inc.'s AutoSys product. Only authorized personnel have the ability to schedule or modify jobs within the AutoSys product.

Operations personnel monitor and produce daily Service Center and Statistics reports, which are reviewed for service interruptions, performance monitoring and capacity planning. Monthly system availability reports are also produced as part of the above reporting. The design of FIS' systems and programs minimize actions required by the Operations staff, which helps to reduce the risk of error. Daily database monitoring is performed for each customer and reported on a monthly basis. This monitoring consists of a file system summary, CPU utilization, and a summary of the accounting runs processing time.

Backup and Off-site Storage

FIS Fixed Income Processing Suite ASP utilizes an automated tape management system (Veritas) for control of tape retention and backup. Procedures have been developed to regularly backup and store off-site files critical for the continuity of computer operations. Access to make changes to the Veritas backup schedule software is restricted to IT Operations personnel. The following tape backups are performed on a daily or weekly basis:

- FIS Fixed Income Processing Suite production libraries, including source and object code;
- FIS Fixed Income Processing Suite customer-specific system preferences, data files and report files; and
- UNIX operating system settings and configurations.

Unix Systems is responsible for archiving the ASP database annually and daily database monitoring. At year-end, FIS makes a copy of the ASP database structure, which it provides to the ASP users. In the RSM environment, data is archived to a user's media as requested by the user. FIS Fixed Income Processing Suite personnel must manually initiate and monitor the archiving process. Any changes to the archival schedule are subject to the RSM internal change control process as discussed in the System Software section. File restores may be requested by an authorized RSM user contact. Tape backups and restores are monitored by operations personnel via an automated e-mail and errors are documented and communicated to authorized personnel for follow-up.

RSM backup tape schedules are determined and agreed upon for each RSM customer. Responsibilities for customer tape backups are documented and available to Operations personnel. Each RSM customer has backup hardware and a unique schedule, which is managed using an automated process.

Backups are tested for recoverability for those servers located in the Hopkins, MN datacenter by the normal recovering of information for customers per their request.

System Software

Control Objective 4: Controls provide reasonable assurance that modifications to critical FIS Fixed Income Processing Suite system software are documented and approved prior to migration into production.

FIS utilizes a broad array of system software products in support of the development, maintenance and operation of automated services. All system software products are evaluated prior to acquisition. System software is obtained from reputable vendors to help provide stability and maximum availability. Data center services personnel apply vendor issued modifications to system software on a quarterly basis and implement new releases, as they become available.

If a new version of system software is required due to a release of FIS Fixed Income Processing Suite, the new system software will be promoted through the normal release process of Development, QA and Production. Data center personnel apply vendor-issued modifications to system software and implement new releases of FIS Fixed Income Processing Suite as they become available and as requested by the RSM customer.

Modifications to system software products are required for various reasons, some of which are summarized below:

Type	Typical Cause or Origin
New system software product	Departmental, operational or application generated requirement
New releases or updates of system software	Vendor release and application requirement
Correction of system software problems	As required

Regardless of type, all modifications related to system software are originated by or routed to the data center services department. Based on available staffing and FIS Fixed Income Processing Suite software product(s) impacted, a member of the data center services staff is assigned responsibility for evaluating the modification.

Access to directories containing UNIX system software is restricted to authorized data center services personnel. These libraries must be accessed through signing on with a user profile with root authority.

FIS Fixed Income Processing Suite ASP

Authorization and approval of all modifications to ASP-related system software by Information Systems management is required before modifications are made. System software changes must be submitted to a Change Advisory Board (CAB) for approval before implementation in production and added to the CAB Calendar. Data center services supervisory personnel and the responsible data center services employee jointly determine the scope of system software testing.

FIS Fixed Income Processing Suite RSM

Authorization and approval of all modifications to system software by the appropriate RSM customer is required before modifications are made. Technical Services supervisory personnel and the appropriate RSM customer jointly determine the scope of system software testing, which is performed by the RSM customer. System Software changes follow the change management process noted in the Application change management section noted above.

Data Transmissions

Control Objective 5: Controls provide reasonable assurance that data transmissions between FIS and its client organizations are complete, accurate and secured in accordance with client specifications.

FIS Private IP (PIP) circuits and/or VPN tunnels are used to connect customers to the FIS facilities. Internet Protocol Security (IPsec) for the PIP network is available for users in the event of dedicated network circuit data transmission disruptions. The FIS Fixed Income Processing Suite application contains built-in edit/validation checks to help ensure that complete, accurate and valid data is entered into FIS Fixed Income Processing Suite. From the point of entry, this information is directly interfaced with FIS' internal systems. All user paths have been identified and are controlled by the user's internal system identifier. The establishment and utilization of this internal system identifier provides for proper and authorized user access into the data center's production system. All FIS Fixed Income Processing Suite ASP and RSM connections are routed through redundant firewalls, located at the Hopkins Data Center.

FIS Fixed Income Processing Suite operations support personnel are not responsible for balancing user input and related output. As one of the last steps in the daily maintenance process, operations support personnel are responsible for verifying that production processing is complete for both the ASP and RSM environments. The CA AutoSys scheduler automatically creates a receipt acknowledgement for successful completion of data file transmissions. Operations support personnel monitor the receipt of successful completions, log failed transmissions and work to successfully complete failed data file transmissions.

FIS Fixed Income Processing Suite provides customers with the ability to print daily reports and access information daily. Each customer is provided its own Progress database to store information. ASP customers only have access to their Progress database and are restricted from viewing any information in other customer databases. Any report or data transmissions to FIS Fixed Income Processing Suite ASP and RSM customers are made via IBM's Connect:Direct product. Connect:Direct provides secure data delivery based on transfer technology that includes protection against network interruptions and automated validation checks of transmissions.

Policies are defined for assigning and removing resources to the FIS Fixed Income Processing Suite environment. FIS requests to add or remove logical access to the FIS Fixed Income Processing Suite environment must have an approved on-line System Access Request form. FIS access to modify the file transfer process is limited to FIS Technical Support personnel.

Logical Security Administration

Control Objective 6: Controls provide reasonable assurance that logical access to programs and data is restricted to properly authorized individuals.

FIS Fixed Income Processing Suite ASP User Administration

In the FIS Fixed Income Processing Suite ASP environment, clients control creating user ID's and passwords for new FIS Fixed Income Processing Suite users, resetting existing passwords and can further restrict password configuration and expiration rules. These rules control such parameters as password minimum length, number of upper and lower-case characters, minimum password age, password expiration and maximum failed login attempts. Policies are defined for assigning and removing FIS resources to FIS Fixed Income Processing Suite ASP. FIS requests to add or remove logical access to the FIS Fixed Income Processing Suite ASP environment must have an approved on-line System Access Request form.

FIS Fixed Income Processing Suite RSM User Administration

For RSM customers, clients control creating user ID's for FIS Fixed Income Processing Suite users. For those RSM customers that require FIS to create user ID's for FIS Fixed Income Processing Suite users, policies are defined for assigning and removing user IDs and passwords to FIS Fixed Income Processing Suite users. New users or changes to client access levels are made by RSM personnel only after receipt of a request from a pre-approved client contact. Two separate administrators set-up new users; one for UNIX and one for the FIS Fixed Income Processing Suite application. RSM customers must provide written notification to FIS for the removal of UNIX user IDs. Passwords must be constructed to meet FIS' policy requirements.

UNIX Security

FIS Fixed Income Processing Suite passwords are configured via a correspondence between LDAP and Active Directory. Access to sensitive UNIX directories is restricted to appropriate FIS Fixed Income Processing Suite personnel and is aligned with personnel job responsibilities. Access to "root" through SUDO is restricted to appropriate FIS Fixed Income Processing Suite personnel is aligned with personnel job responsibilities. System-generated monitoring reports of use of root authority are reviewed by the Information Security Analyst. ASP users only have access to their progress database and are restricted from viewing any information in other user databases.

In the FIS Fixed Income Processing Suite RSM UNIX environment, access to data files and program files is restricted by native UNIX security and by FIS Fixed Income Processing Suite security. Access control is primarily achieved through the use of a user ID, which restricts access to only authorized personnel. Access to sensitive UNIX directories is restricted to appropriate FIS Fixed Income Processing Suite personnel and is aligned with personnel job responsibilities. Access to "root" through SUDO is restricted to appropriate FIS Fixed Income Processing Suite personnel and is aligned with personnel job responsibilities.

Network Security

An Internet Security policy has been developed and employees are required to acknowledge their understanding and acceptance of this policy via the Business Conduct and Compliance Program on an annual basis.

FIS utilizes its Internet connections to distribute various reports and data, via the FIS Fixed Income Processing Suite Portal, to its clients as well as to correspondent portfolio clients. Clients and correspondent portfolio clients log onto the FIS Fixed Income Processing Suite Portal using a unique login. All FIS Fixed Income Processing Suite ASP and RSM Private IP (PIP) circuits are routed through the Firewalls.

FIS utilizes Checkpoint Firewall Software on two redundant Hewlett-Packard (HP) Firewalls and a Cisco router to provide the capability to deny unauthorized access to the internal network. The firewall hardware and software were obtained from a reputable vendor that provides hardware and operating system software support as needed. All firewall software patches are evaluated prior to implementation in a separate testing environment. The firewall processor is physically located inside the data center where physical access is restricted by card access keys. Secure Socket Layers (SSL) security is utilized by the FIS Fixed Income Processing Suite Application. Additionally, a disclaimer-warning message is displayed at the beginning of each session.

Controls are in place to identify access guidelines, Internet services deployment, technical architecture, employee responsibilities, monitoring functions, and reporting of abnormal events. Daily reports are generated to monitor exceptions and violation reports. FIS enforces network passwords parameters to be in alignment with their Corporate Security Policy.

Data center services personnel perform support functions for the firewall. Access to the firewall is restricted to valid business users of FIS resources. Firewall configurations are backed-up daily and are sent offsite for storage.

Only appropriate personnel have the ability to make configuration changes to the firewall. On a weekly basis, FIS performs a high-level security scan against the network from the Internet to identify major vulnerabilities. Based on the scan, the appropriate remediation is taken to address any major vulnerabilities.

Description of Application Controls

Note that for presentation purposes individual control objectives have not been listed for each key module of the FIS Fixed Income Processing Suite application as the controls are consistent across each of the modules. A single control objective has been utilized instead of repeating the same control objective for each key module. Results are reported in Section IV of the report. Also note that the User Control Considerations of this report are critical to the achievement of the control objectives noted below.

FIS Fixed Income Processing Suite System

Control Objective 7: Controls provide reasonable assurance that input transactions are accurate, complete, and valid.

The FIS Fixed Income Processing Suite system contains built-in edit/validation checks to help ensure that complete, accurate and valid data is entered into FIS Fixed Income Processing Suite. Incomplete, inaccurate and invalid user input is handled in one of three ways:

- If the incomplete, inaccurate or invalid input will cause FIS Fixed Income Processing Suite to malfunction, or it is clearly unreasonable, FIS Fixed Income Processing Suite will display a message on the screen describing the error, and will not commit the transaction to the database until the error is corrected.
- If the incomplete, inaccurate or invalid input will not cause FIS Fixed Income Processing Suite to malfunction, but it appears unreasonable from a business standpoint, FIS Fixed Income Processing Suite will display a warning message and ask the user to take action and verify the input.
- If the incomplete, inaccurate or invalid input will not cause FIS Fixed Income Processing Suite to malfunction, but it is a case where someone else in the organization should review or complete the input, an “Alarm” is sent to another designated user on the network for review or completion. These “Alarms” are configured by the user organization.

Exceptions within the application during processing cause a message to be displayed on the user’s screen which describes the exception. The user organization is responsible for data input, edit, processing, balancing and output distribution controls at each of their independent locations.

Exceptions during processing within the database are recorded in a database log, which records in plain ASCII text each time a user logs in, logs out, or encounters a database error. Other ASCII text logs are maintained by the application itself. Offline processes such as the confirmation queue maintain their own application log.

Maintenance to key database files is recorded within the database. An audit report (File Maintenance History Report) is automatically generated by the FIS Fixed Income Processing Suite application on a nightly basis and lists any changes to customer data. The user making the change, the date and time, and the before and after values of each modified field are recorded and may be displayed using the “File Maintenance History” function. In the case of trading, when a trade is corrected, a complete snapshot of the important elements of the trade prior to correction is stored in the “oldtrade” table. When a trade is displayed using the standard function the values in these tables are compared and a listing of changed values is presented.

Each user is granted “permission” to the functions to which they are to be enabled by a user system administrator. They may only perform those functions. The user ID which they used to log into the application is compared to a table of allowed functions, and only those functions are presented to that user within their menus.

The Accounting Run keeps an ASCII log. In addition, it records its current step within the database. If an error occurs during the application processing of the accounting run, a message is displayed to the operator. The operator can refer to the logs for more detail. Since the current step is recorded within the database, the accounting run can be restarted and it automatically skips to the point at which it failed earlier. If the accounting run fails during non-application processing (such as the database housekeeping portions), the logs indicate what was occurring when the failure occurred, and the nature of the failure.

FIS Fixed Income Processing Suite 16.0 has the ability to restrict a non-system administrator from modifying his/her own functional permissions (Tree Permissions) and Trading Permissions via the System Information function field, “Change Own Perms”. New installations of FIS Fixed Income Processing Suite will have this field defaulted to “N”, meaning the user is not allowed to change his/her own permissions. Each customer has the ability to modify the settings to be in alignment with their environment and therefore this functionality may not be utilized by all customers.

FIS Fixed Income Processing Suite System Conversions

Control Objective 8: Controls provide reasonable assurance that for new FIS Fixed Income Processing Suite ASP migrations, the application is configured in accordance with user specifications during the implementation phase.

FIS utilizes a detailed technical approach for conducting a controlled transition from a financial institution’s current processor to FIS Fixed Income Processing Suite ASP. Subsequent to receiving a signed contract from the FIS Sales area, the Professional Services group is responsible for implementing a controlled transition to the FIS Fixed Income Processing Suite ASP processing environment. A detailed Project Plan or Project Report is used to track that all of the tasks are accurately articulated to successfully complete the conversion process.

The assigned FIS conversion representative conducts an information gathering session with the converting client referred to as the ‘first call’. During the first call, the key components of the conversion process are discussed and decisions are made by the client as to the direction in which the client wants to proceed. Subsequent to the first call, a project plan is developed and is provided to the client to document the entire conversion process. To accomplish the objectives of the conversion and to facilitate project planning and management, the conversion process to the FIS Fixed Income Processing Suite ASP environment is performed as a series of five primary tasks:

- Task 1 - Obtain executed contract from Sales;
- Task 2 - Develop project plan or project report containing a timeline for the implementation effort;
- Task 3 - Execute project plan until all defined tasks are completed;
- Task 4 - Conduct go/no-go meeting with customer prior to first production use; and
- Task 5 - Upon customer acceptance, execute live conversion to production.

A conversion date is agreed to between the customer and FIS. FIS’ Change Management approves the scheduling of the event and place it on the change calendar. The implementation plan is reviewed internally at FIS with the affected departments that are performing the task.

Following the completion of user acceptance testing, the customer meets with FIS representatives during a “go/no-go” meeting to discuss the results of the testing. The customer may request additional modifications to the FIS Fixed Income Processing Suite functionality at this meeting and their decision to go-live is based on the relative importance of these modifications. If the application satisfies the customer’s current needs, the customer will decide to go-live with the conversion and allow FIS to address the additional modifications in a subsequent release.

Upon successful completion of the conversion process, the FIS Fixed Income Processing Suite Answerline area assumes responsibility for ongoing client service and support. Professional Services performs a "turn-over" of support to FIS Fixed Income Processing Suite Answerline and this is typically done 30 days after the customer has been in production.

Management noted that the circumstances what would warrant the operation of control activities 1, 2, 3, and 4 of this control objective did not occur during the specified period and therefore the controls did not operate during the specified period.

D. Additional Information about Management's Description

FIS' control objectives and related control activities are included in Section IV of this report, "Fidelity Information Services, LLC's Control Objectives and Related Controls and the Independent Service Auditor's Description of Tests of Controls and Results." Although the control objectives and related control activities are presented in Section IV, they are, nevertheless, an integral part of FIS' description of its system as described in this section.

E. Subservice Organizations

FIS 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 FIS 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 FIS' 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	Associated Control Objective(s)
FIS Computer Services	FIS Computer Services is responsible for infrastructure management services. The following control groupings are critical to achieving the applicable control objectives: • Controls provide reasonable assurance that physical access to the data centers is restricted to authorized personnel. • Controls provide reasonable assurance that environmental protection mechanisms are in place and are maintained on a periodic basis. • Controls provide reasonable assurance that logical access is restricted to authorized FIS personnel. • Controls provide reasonable assurance that system processing is authorized and executed in a complete and timely manner and that processing deviations are identified and resolved. • Controls provide reasonable assurance that changes to in-scope systems are performed according to defined procedures that include testing and approval prior to promotion to the production environment.	Control Objectives 1*, 2*, 3*, 4*, 5*, 6*, 7*, and 8

Subservice Organization	Service(s) Provided and Complementary Subservice Organization Controls	Associated Control Objective(s)
	• Controls provide reasonable assurance that data is backed up and available for restoration in the event of processing errors and/or unexpected processing interruptions in accordance with the Company's Backup and Restoration policies. In addition, the Company has identified the following controls to help monitor the subservice organization: • SOC 1 and SOC 2 examinations are performed over the FIS Computer Services. Management monitors the results of the SOC reports.	

* The achievement of design and operating effectiveness for this particular control objective assumes that complementary controls at this subservice organization are in place and are operating effectively to support and achieve this control objective.

F. Complementary User Entity Controls

FIS' controls relating to the system cover only a portion of the overall internal control structure of each user entity of FIS' system. It is not feasible for the control objectives to be solely achieved by FIS. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with FIS' controls and related testing detailed in Section IV of this report, taking into account the related complementary user entity controls identified in the table below, where applicable. Complementary user entity controls and their associated control objective(s) are included within the table below.

In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine if the identified complementary user entity controls have been implemented and are operating effectively.

Complementary User Entity Controls	Associated Control Objective(s)
User entities are responsible for ensuring that FIS is provided with accurate and up-to-date contact information for change authorization, emergency notification, and problem escalation.	Control Objective 2
User entities are responsible for ensuring that custom changes are tested prior to approving for release to production environment.	Control Objective 2
User entities are responsible for controls over user entity owned server-based data files transmitted between FIS and the user and stored on the user entities' equipment.	Control Objective 5
User entities are responsible for instituting local policies to guide their users in the overriding of "soft" flags, indicators or warnings identified by the FIS Fixed Income Processing Suite application during the data entry process.	Control Objective 5
User entities are responsible for setting up and maintaining security using the security module within the FIS Fixed Income Processing Suite application, which includes administrating application access and password parameters.	Control Objective 6

Complementary User Entity Controls	Associated Control Objective(s)
User entities are responsible for performing periodic reviews of system access levels granted to determine whether access remains commensurate with job responsibilities. In addition, user entities are responsible for reviewing audit trail reports generated from the FIS Fixed Income Processing Suite application to monitor and verify that the processing of transactions is performed by authorized individuals.	Control Objective 6
User entities are responsible for configuring the System Information function field to align with their information security policies. FIS Fixed Income Processing Suite version 16.0 and greater has the ability to restrict a non-system administrator from modifying his/her own functional permissions (Tree Permissions) and Trading Permissions via the System Information function field, “Change Own Perms”. New installations of FIS Fixed Income Processing Suite version 16.0 and greater will have this field defaulted to “N”, meaning the user is not allowed to change his/her own permissions. Each customer has the ability to modify the settings to be in alignment with their environment, and therefore, use of this functionality is solely the responsibility of user organizations.	Control Objective 8
User entities are responsible for the completeness and accuracy of data transmissions with FIS.	Control Objective 7
User entities are responsible for retrieving and reviewing the nightly application output print files.	Control Objective 7
User entities are responsible for reconciling and determining that its records are in balance to help assess the integrity of their ledgers and system reports. The FIS Fixed Income Processing Suite application produces balancing reports that should be reviewed and reconciled on a daily basis by the user entity. We recommend the reconciliation be performed by a person independent of the origination and posting functions.	Control Objective 7
User entities are responsible for implementing controls to determine if transactions are appropriately authorized.	Control Objective 7
User entities are responsible for implementing controls to determine if accuracy of price information.	Control Objective 7
User entities are responsible for reviewing applicable daily activity reports and investigating the basis for the use of backdating of transactions.	Control Objective 7
User entities are responsible for periodically testing or otherwise verifying key calculations and processes as appropriate to determine the accuracy of FIS Fixed Income Processing Suite’s processing.	Control Objective 7

Complementary User Entity Controls	Associated Control Objective(s)
User entities are responsible for determining when to begin using FIS Fixed Income Processing Suite's nightly transmissions in their production environment during a conversion to FIS Fixed Income Processing Suite ASP. (ASP Specific)	Control Objective 8
RSM user entities are responsible for providing FIS a list of users authorized to request and approve FIS Fixed Income Processing Suite modifications. Any modifications to the listing of authorized requesters must be submitted by an authorized individual to FIS. (RSM Specific)	Control Objective 2
Backups complete on a nightly basis as outlined in the data processing service agreement between FIS and the RSM user entities. Based on the agreement, either FIS or the customer will be responsible for managing the backup process. The service agreement will also note who is responsible for ensuring the tapes are regularly removed and stored offsite. (RSM Specific)	Control Objective 3
RSM user entities are responsible for testing any operating system patches or releases. The user entity can make changes directly to their own server or can request FIS to assist in the process; however, the user entity is solely responsible for testing these changes. (RSM Specific)	Control Objective 4
RSM user entities are responsible for providing FIS a list of users authorized to request and approve FIS Fixed Income Processing Suite modifications. Any modifications to the listing of authorized requesters must be submitted by an authorized individual to FIS. (RSM Specific)	Control Objective 4
RSM user entities with servers located at the user site are responsible for logical security of users that the user organization adds to the server; including SYS ADMIN and high-level access (i.e., root). Any changes made by user personnel to the FIS Fixed Income Processing Suite RSM environment are not covered by this report and are not the responsibility of FIS. (RSM Specific)	Control Objective 6
RSM user entities are responsible for providing timely written notification of changes to authorized security administrators and removal requests for UNIX user ID's. (RSM Specific)	Control Objective 6

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

A. Types and Descriptions of the Tests of Operating Effectiveness Provided by the Independent Service Auditor

This report, when combined with an understanding of the controls at user entities and the subservice organization, is intended to assist auditors in planning the audit of user entities' financial statements or user entities' internal control over financial reporting and in assessing control risk for assertions in user entities' financial statements that may be affected by controls at FIS.

Our examination was limited to the control objectives and related controls specified by FIS 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 user entity and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess the internal control environment. If the internal controls are not effective at a user entity, FIS' controls may not compensate for such weaknesses.

FIS' system of internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by FIS. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by FIS, we considered aspects of FIS' control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used within 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

Inquiries were performed for substantially all controls in Section IV, and, therefore, inquiries were not separately listed as a test for every control.

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. Control Objectives, Control Activities, Tests Performed and Results of Testing

Control Objective 1

Controls provide reasonable assurance that development of new FIS Fixed Income Processing Suite releases are documented, tested, and approved prior to migration into production.

Control Activity		Tests Performed By Service Auditor	Results of Testing
1-1	FIS Fixed Income Processing Suite uses a Software Development Life Cycle policy that includes the following phases: 1. Planning 2. Execution 3. Release Management	**Inspection:** Inspected the FIS Fixed Income Processing Suite Software Development Process Life Cycle policy to determine that it included standards for planning, execution, and release management, as well as the responsibilities for each phase.	No exceptions noted.
1-2	Enhancements for new releases of FIS Fixed Income Processing Suite include a project plan, functional turnover document, testing and approval prior to migration into production.	**Inspection:** Inspected the supporting documentation for a sample of new FIS Fixed Income Processing Suite enhancements to determine that for each selected enhancement, a project plan was documented.	No exceptions noted.
		Inspection: Inspected the supporting documentation for a sample of new FIS Fixed Income Processing Suite enhancements to determine that for each selected enhancement, a functional turnover document was created.	No exceptions noted.
		Inspection: Inspected the supporting documentation for a sample of new FIS Fixed Income Processing Suite enhancements to determine that for each selected enhancement, testing was performed and results were documented.	No exceptions noted.
		Inspection: Inspected the supporting documentation for a sample of new FIS Fixed Income Processing Suite enhancements to determine that for each selected enhancement, appropriate personnel approved the enhancement prior to migration into production.	No exceptions noted.

Control Objective 2

Controls provide reasonable assurance that FIS Fixed Income Processing Suite maintenance requests, including direct data changes, are documented, authorized, tested, and approved prior to migration into production.

Control Activity		Tests Performed By Service Auditor	Results of Testing
2-1	FIS Fixed Income Processing Suite ASP Move Procedure is in place to govern that application maintenance, "Hot Moves" and custom changes are documented, authorized, tested and approved prior to migration into production.	**Inspection:** Inspected the FIS Fixed Income Processing Suite ASP Move Procedure to determine that the policy included processes for documenting, authorizing, testing, approving, and implementing application maintenance, "Hot Moves" and custom changes.	No exceptions noted.
2-2	ASP change control and development standards are in place for data record design, incorporation of data, and use of database files.	**Inspection:** Inspected the FIS Fixed Income Processing Suite Agile SDLC, ABL Programming Standards, and FIS Fixed Income Processing Suite Database Schema Change Standards to determine that the policies included the process for data record design, incorporation of data, and use of database files.	No exceptions noted.
2-3	FIS Fixed Income Processing Suite ASP custom changes are documented, authorized, tested, and approved prior to migration into production.	**Inspection:** Inspected the tickets for a sample of FIS Fixed Income Processing Suite ASP custom changes to determine that each change was documented, authorized, tested, and approved prior to migration into production.	No exceptions noted.
2-4	FIS Fixed Income Processing Suite ASP application standard changes are documented, authorized, tested and approved prior to migration into production.	**Inspection:** Inspected the tickets for a sample of ASP application standard changes to determine that each selected change was documented, authorized, tested, and approved prior to migration into production.	No exceptions noted.
2-5	If the FIS Fixed Income Processing Suite ASP application change is a custom program move that affects the customer, a customer sign-off is required prior to migration into production.	**Inspection:** Inspected the tickets for a sample of ASP custom program moves to determine that for each selected custom program move, a customer sign-off was received prior to migration into production, if applicable.	No exceptions noted.

Control Objective 2

Controls provide reasonable assurance that FIS Fixed Income Processing Suite maintenance requests, including direct data changes, are documented, authorized, tested, and approved prior to migration into production.

Control Activity		Tests Performed By Service Auditor	Results of Testing
2-6	Only authorized personnel have access to promote FIS Fixed Income Processing Suite ASP programs into production libraries and directories.	**Inspection:** Inspected the sudoers file to determine that only authorized personnel had access to promote FIS Fixed Income Processing Suite ASP programs into production libraries and directories.	No exceptions noted.
2-7	If an FIS Fixed Income Processing Suite ASP application change is classified as a "Hot Move", the change must be tested and approved by the QA Department.	**Inspection:** Inspected the tickets for a sample of "Hot Move" emergency changes to determine that each selected emergency change was tested and approved by the QA Department.	No exceptions noted.
2-8	If the FIS Fixed Income Processing Suite ASP Data Repair Utility (DRU) is required for multiple customer environments, the DRU program source code is reviewed and approved by FIS Management. To create and execute a customer specific DRU, approval is required from FIS Management and an authorized customer representative.	**Inspection:** Inspected the tickets for a sample of DRU changes to determine that each selected DRU change was approved by FIS Management and, if necessary, an authorized customer representative.	No exceptions noted.
2-9	The Change Control and Version Control Policies include procedures for initiating, approving, completing, testing and implementing FIS Fixed Income Processing Suite RSM application maintenance requests, custom programming requests, data, and government regulatory requirements.	**Inspection:** Inspected the Change Control and Version Control Policies to determine that the procedures included processes for initiating, approving, completing, testing, and implementing FIS Fixed Income Processing Suite RSM application maintenance requests, custom programming requests, data, and government regulatory requirements.	No exceptions noted.

Control Objective 2

Controls provide reasonable assurance that FIS Fixed Income Processing Suite maintenance requests, including direct data changes, are documented, authorized, tested, and approved prior to migration into production.

Control Activity		Tests Performed By Service Auditor	Results of Testing
2-10	FIS Fixed Income Processing Suite RSM maintenance requests must originate from the customer.	**Inspection:** Inspected the tickets for a sample of FIS Fixed Income Processing Suite RSM maintenance requests implemented into production, to determine that each selected request originated from the customer.	No exceptions noted.
2-11	FIS Fixed Income Processing Suite RSM maintenance requests require approval from an authorized customer approver prior to migration into production.	**Inspection:** Inspected the tickets for a sample of FIS Fixed Income Processing Suite RSM maintenance requests to determine that each selected maintenance request included the approval from an authorized customer personnel prior to migration into production.	No exceptions noted.
2-12	Authorized users within the Production Control Group have access to promote FIS Fixed Income Processing Suite RSM programs into production libraries and directories.	**Inspection:** Inspected the sudoers file to determine that only authorized users within the Production Control Group had access to promote FIS Fixed Income Processing Suite RSM programs into production libraries and directories.	No exceptions noted.

Control Objective 3

Controls provide reasonable assurance that processing (FIS Fixed Income Processing Suite nightly accounting runs), including backups, is scheduled appropriately and deviations from scheduled processing are identified and resolved.

Control Activity		Tests Performed By Service Auditor	Results of Testing
3-1	In the FIS Fixed Income Processing Suite ASP and RSM environment, Computer Operations procedures, which have been developed and are available on-line on the FIS intranet, include normal operations and anticipated exceptions.	**Inspection:** Inspected the Computer Operations procedures to determine that procedures were developed around normal operations and anticipated exceptions and were made available on-line on the FIS intranet.	No exceptions noted.
3-2	Operators complete online incident tickets for unusual situations that occur during the shift. These incident tickets are assigned to the proper support organization for follow-up and resolution.	**Inspection:** Inspected the tickets for a sample of incidents to determine that each selected incident was assigned to the proper support organization for follow-up and resolution.	No exceptions noted.
3-3	Operations personnel monitor a daily Service Center Report and Statistics report, which is reviewed for service interruptions, performance monitoring and capacity planning.	**Inspection:** Inspected the e-mail summary of the Service Center Report and Statistics report for a sample of days to determine that for each selected day, the Operations team reviewed the daily Service Center reports for service interruptions, performance monitoring, and capacity planning.	No exceptions noted.
3-4	Only authorized personnel have the ability to schedule or modify jobs within the AutoSys product.	**Inspection:** Inspected the listing of users with the ability to modify the AutoSys schedule for a sample of users to determine that for each selected user, access was restricted to authorized personnel.	No exceptions noted.
3-5	Procedures have been developed to regularly backup data and store off-site files critical for the continuity of computer operations.	**Inspection:** Inspected the ASP Backup Policy to determine that the policy was current and included tape backup frequencies and off-site storage durations.	No exceptions noted.

Control Objective 3

Controls provide reasonable assurance that processing (FIS Fixed Income Processing Suite nightly accounting runs), including backups, is scheduled appropriately and deviations from scheduled processing are identified and resolved.

Control Activity		Tests Performed By Service Auditor	Results of Testing
		Inspection: Inspected the backup settings configured within the backup software to determine that they complied with the Company policy.	No exceptions noted.
3-6	Access to make changes to the Veritas backup schedule software is restricted to IT Operations personnel.	**Inspection:** Inspected the sudoers file to determine that access to make changes to the Veritas backup schedule software was restricted to IT Operations personnel.	No exceptions noted.
3-7	The system is configured to perform ASP tape backups on a daily or weekly basis for the following: • FIS Fixed Income Processing Suite production libraries, including source and object code; • FIS Fixed Income Processing Suite customer-specific system preferences and data files; and • UNIX operating system settings and configurations.	**Observation:** Observed the backup configurations to determine that the system was configured to perform ASP tape backups on a daily or weekly basis for the following: • FIS Fixed Income Processing Suite production libraries, including source and object code; • FIS Fixed Income Processing Suite customer-specific system preferences and data files; and • UNIX operating system settings and configurations.	No exceptions noted.
3-8	Backup media is rotated to an off-site storage location on a daily basis (except Sundays).	**Inspection:** Inspected the off-site storage forms for a sample of days to determine that for each selected day, tapes were rotated to an off-site storage location.	No exceptions noted.
3-9	Backup media is rotated on-site from an off-site storage location on a daily basis.	**Inspection:** Inspected the on-site storage forms for a sample of days to determine that for each selected day, backup media was rotated on-site from an off-site storage location.	No exceptions noted.
3-10	Backups are tested for recoverability by the normal recovering of information for customers per their request.	**Observation:** Observed a file restore to determine that the files were able to be recovered per a client request.	No exceptions noted.

Control Objective 4

Controls provide reasonable assurance that modifications to critical FIS Fixed Income Processing Suite system software are documented and approved prior to migration into production.

Control Activity		Tests Performed By Service Auditor	Results of Testing
4-1	Authorization and approval of all ASP modifications to system software by Information Systems management is required before modifications are made.	**Inspection:** Inspected the tickets for a sample of ASP modifications to system software to determine that for each selected modification, Information Systems management approved the modification before the modification was made.	No exceptions noted.
4-2	High-Risk ASP system software changes must be submitted to the Change Advisory Board for approval prior to migration into production.	**Inspection:** Inspected the tickets for a sample of high-risk system software changes to determine that each selected change was submitted to the Change Advisory Board and approved prior to migration into production.	No exceptions noted.
4-3	All modifications to system software must be authorized and approved by the authorized RSM customer before modifications are made.	**Inspection:** Inspected the FIS Fixed Income Processing Suite Version Control Policy to determine that the RSM customer was responsible for testing any patch or operating system upgrade that occurred outside of a formal FIS Fixed Income Processing Suite release/patch.	No exceptions noted.
		Inspection: Inspected the tickets for a sample of RSM maintenance requests to determine that each selected maintenance request was documented and approved by an authorized RSM customer.	No exceptions noted.
4-4	FIS access to RSM and ASP directories containing UNIX system software is restricted to authorized Data Center Services personnel. These libraries must be accessed through signing on with a user profile with root authority.	**Inspection:** Inspected the sudoers file to determine that RSM and ASP directories containing UNIX system software was restricted to authorized FIS Data Center Services personnel.	No exceptions noted.

Control Objective 5

Controls provide reasonable assurance that data transmissions between FIS and its client organizations are complete, accurate and secured in accordance with client specifications.

Control Activity		Tests Performed By Service Auditor	Results of Testing
5-1	Operations support personnel are responsible for completing daily summary reports to evidence their monitoring of production processing. If an error occurs, the Operations support personnel updates the daily summary reports and creates a ticket.	**Inspection:** Inspected the Daily Summary Reports for a sample of days to determine that for each selected day, production processing was monitored by Operations personnel and tickets were created for incidents, if applicable.	No exceptions noted.
5-2	Customers only have access to their own Progress database and are restricted from viewing any information in other customer databases through virtual machine partitions and unique internal system identifiers.	**Observation:** Observed the database instances and authentication process to determine that customers only had access to their own Progress database and were restricted from viewing any information in other customer databases through virtual machine partitions and unique internal system identifiers.	No exceptions noted.
5-3	Connect: Direct provides data delivery based on transfer technology that includes protection against network interruptions and automated validation checks of transmissions.	**Observation:** Observed the data transmission configurations to determine the system included protection against network interruptions and automatically performed validation checks for transmissions.	No exceptions noted.
5-4	Policies are defined for assigning and removing FIS resources to the FIS Fixed Income Processing Suite environment.	**Inspection:** Inspected the Hopkins Facility & System Access Policy to determine that policies were defined for assigning and removing FIS resources to the FIS Fixed Income Processing Suite environment.	No exceptions noted.
5-5	FIS requests to add or remove logical access to the FIS Fixed Income Processing Suite environment must have an approved online System Access Request form.	**Inspection:** Inspected the tickets for a sample of new or removed logical access requests for the FIS Fixed Income Processing Suite environment to determine that for each selected request a System Access Request form was submitted and approved.	No exceptions noted.

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

Control Objective 5 Controls provide reasonable assurance that data transmissions between FIS and its client organizations are complete, accurate and secured in accordance with client specifications.			
Control Activity		Tests Performed By Service Auditor	Results of Testing
5-6	FIS access to modify the file transfer process is limited to Technical Support personnel.	**Inspection:** Inspected the sudoers file to determine that access to modify the file transfer process was restricted to FIS support personnel.	No exceptions noted.

Control Objective 6

Controls provide reasonable assurance that logical access to programs and data is restricted to properly authorized individuals.

Control Activity		Tests Performed By Service Auditor	Results of Testing
6-1	Policies are defined for assigning and removing FIS resources to the FIS Fixed Income Processing Suite ASP environment.	**Inspection:** Inspected the FIS Fixed Income Processing Suite Standards and Procedures to determine that policies were defined for assigning and removing FIS resources to the FIS Fixed Income Processing Suite ASP environment.	No exceptions noted.
6-2	FIS requests to add or remove logical access to the FIS Fixed Income Processing Suite environment must have a manager approved online System Access Request form.	**Inspection:** Inspected the tickets for a sample of new or removed logical access requests for the FIS Fixed Income Processing Suite environment to determine that for each selected request a System Access Request form was submitted and approved.	No exceptions noted.
6-3	Password parameters are configured within the FIS Fixed Income Processing Suite application for minimum password length and upper case and lower case complexity.	**Inspection:** Inspected the FIS Fixed Income Processing Suite password configurations to determine that password parameters were set to require a minimum length of 8 characters, minimum of 1 uppercase character, and a minimum of 1 lowercase character.	No exceptions noted.
6-4	Access to sensitive ASP UNIX directories is restricted to FIS Fixed Income Processing Suite personnel.	**Inspection:** Inspected the sudoers file to determine that access to sensitive ASP UNIX directories was restricted to FIS Fixed Income Processing Suite personnel.	No exceptions noted.
6-5	Access to “root” through sudo in the ASP environment is restricted to FIS Fixed Income Processing Suite personnel.	**Inspection:** Inspected the sudoers file to determine that access to “root” through sudo in the ASP environment was restricted to FIS Fixed Income Processing Suite personnel.	No exceptions noted.

Control Objective 6

Controls provide reasonable assurance that logical access to programs and data is restricted to properly authorized individuals.

Control Activity		Tests Performed By Service Auditor	Results of Testing
6-6	ASP users only have access to their Progress database and are restricted from viewing any information in other user databases.	**Observation:** Observed the database instances and authentication process to determine that customers only had access to their own Progress database and were restricted from viewing any information in other customer databases through virtual machine partitions and unique internal system identifiers.	No exceptions noted.
6-7	New RSM users or changes to RSM user access levels are made by FIS Fixed Income Processing Suite personnel only after receipt of a request from a pre-approved client contact.	**Inspection:** Inspected the tickets for a sample of new or modified RSM users to determine that each selected request was made by pre-approved client contacts.	No exceptions noted.
6-8	RSM customers must provide written notification to FIS for the removal of UNIX user IDs.	**Inspection:** Inspected the tickets for a sample of RSM access removals to determine that each selected removal was requested by the customer.	No exceptions noted.
6-9	For RSM clients, access to sensitive UNIX directories is restricted to FIS Fixed Income Processing Suite personnel.	**Inspection:** Inspected the sudoers listing to determine that access to sensitive UNIX directories for RSM clients was restricted to FIS Fixed Income Processing Suite personnel for RSM clients.	No exceptions noted.
6-10	For RSM clients, access to "root" through sudo in the FIS Fixed Income Processing Suite environment is restricted to FIS Fixed Income Processing Suite personnel	**Inspection:** Inspected the sudoers listing to determine that access to "root" through sudo in the FIS Fixed Income Processing Suite environment for RSM clients was restricted to FIS Fixed Income Processing Suite personnel.	No exceptions noted.

Control Objective 7

Controls provide reasonable assurance that input transactions are accurate, complete, and valid.

Control Activity		Tests Performed By Service Auditor	Results of Testing
7-1	The FIS Fixed Income Processing Suite system contains the following built-in edit/validation checks: • invalid data types are detected and further processing of the transaction is prevented; • required fields must be completed prior to processing the transaction; • alarms are addressed prior to further processing of the transaction; and, • changes are captured on daily reports.	**Observation:** Observed the edit/validation checks for a Money Market, a Federal Funds, a Repurchase Agreement and a Secondary Market Securities transaction to determine that: • invalid data types were input to determine that the error was detected by the on-line system and that further processing of the transactions was prevented; • required fields were left blank to determine that blank fields were detected by the on-line system and that further processing of the transactions was prevented; • clearing of an Alarm was required for review or completion; and, • successful completion of a change appeared during nightly batch process on the necessary reports.	No exceptions noted.
7-2	An audit report (File Maintenance History Report) is automatically generated by the FIS Fixed Income Processing Suite application on a nightly basis and lists any changes to customer data.	**Inspection:** Inspected FIS Fixed Income Processing Suite audit reports for a sample of days to determine that for each selected day, changes in the customer service support environment were captured on an audit report (File Maintenance History Report).	No exceptions noted.
7-3	Each user is granted "permission" to the functions to which they are to be enabled by a system administrator. The user ID which they used to log into the operating system is compared to a table of allowed functions, and only those functions are presented to that user within their menus.	**Observation:** Observed the FIS Fixed Income Processing Suite user permissions to determine that FIS Fixed Income Processing Suite allowed users to access only those functions that they had been assigned by a system administrator.	No exceptions noted.

Control Objective 7

Controls provide reasonable assurance that input transactions are accurate, complete, and valid.

Control Activity		Tests Performed By Service Auditor	Results of Testing
7-4	FIS Fixed Income Processing Suite 16.0 has the ability to restrict a non-system administrator from modifying his/her own functional permissions (Tree Permissions) and Trading Permissions via the System Information function field, “Change Own Perms”.	**Observation:** Observed a user with non-system administrator access attempt to modify their access to determine that FIS Fixed Income Processing Suite 16.0 prevented the non-system administrator from changing her own permissions when the “Change Own Perms” field had been set to “N”.	No exceptions noted.
7-5	Operations personnel produce a daily Service Center Report and Statistics report, which is reviewed for service interruptions, performance monitoring and capacity planning.	**Inspection:** Inspected the e-mail summary of the Service Center Report and Statistics report for a sample of days to determine that for each selected day, the Operations team reviewed the daily Service Center reports for service interruptions, performance monitoring, and capacity planning.	No exceptions noted.
7-6	Operators complete online incident tickets for unusual situations that occur during the shift. These incidents tickets are assigned to the proper support organization for follow-up and resolution.	**Inspection:** Inspected the tickets for a sample of incidents to determine that each selected incident was assigned to the proper support organization for follow-up and resolution.	No exceptions noted.

Control Objective 8

Controls provide reasonable assurance that for new FIS Fixed Income Processing Suite ASP migrations, the application is configured in accordance with user specifications during the implementation phase.

Control Activity		Tests Performed By Service Auditor	Results of Testing
8-1	A detailed project plan is used to track and monitor that all critical tasks associated with the ASP conversions are successfully completed.	**Inspection:** Inspected the project plan for a sample of new ASP customers to determine that for each selected new ASP customer, the plan contained tasks associated with setup, testing, and conversion, and these tasks were tracked and monitored to completion.	No exceptions noted.
8-2	A signed contract is received from each new customer.	**Inspection:** Inspected the contract for a sample of new ASP customers to determine that for each selected new ASP customer, a signed contract was received.	No exceptions noted.
8-3	The new ASP customer provides authorization in writing (or e-mail) to acknowledge their authorization to go live.	**Inspection:** Inspected the customer 'Go/No Go' approval for a sample of new ASP customers to determine that for each selected new ASP customers, customers acknowledged their authorization to go live.	No exceptions noted.
8-4	The Major Events Committee meets to approve the scheduling of the conversion event.	**Inspection:** Inspected the change request forms for a sample of new ASP customers to determine that for each selected new ASP customer, the final conversion was approved by the Major Events Coordinator.	No exceptions noted.

V. Other Information Provided by Fidelity Information Services, LLC

The information in this section describing activities and controls is presented by FIS to provide additional information to its users and is not part of FIS' description of controls that may be relevant to the user's internal control as it relates to an audit of financial statements. Such information has not been subjected to the procedures applied in the examination of the description of FIS' operations on behalf of its users, and accordingly, we express no opinion on it.

A. Business Continuity Strategy

FIS Fixed Income Processing Suite has created and maintains a comprehensive Business Continuity Plan. This plan provides for crisis communications, employee relocation/remote workforce and recovery of critical client processing at its alternate data center including detail on the following:

- Duties and responsibilities of key personnel,
- Emergency response,
- Declaration of a disaster,
- Recovery of systems, programs, and data at the alternate data center,
- Backup and Restoration strategies and tactics, and
- Testing and continuing educational requirements.

B. Business Continuity Tactical Overview

Processing

The FIS Fixed Income Processing Suite application provides real-time ASP services involving frequent changes to client and internal databases, necessitating a robust point in time recovery that meets client needs.

FIS Fixed Income Processing Suite provides three service levels to accommodate client requirements for data processing recovery.

- Hot site
- Warm site
- Standard

Alternate Processing Environment

The FIS Fixed Income Processing Suite contingency processing environment is analogous to that of the primary production environment for each client. Both the production and contingency client environments are supported by Oracle server hardware.

Communications

FIS Fixed Income Processing Suite clients utilize a variety of communications methods. Client and vendor connectivity to both the primary and the alternate data centers is fully integrated into the basic client configuration. Connectivity over the Verizon MPLS network is monitored and managed by FIS Network Services, with primary and secondary circuits using diverse routes to FIS Fixed Income Processing Suite data centers and run through diverse geographic hubs, incoming T1 circuits, central routers and central switches. In addition, a diagnostic modem and line can be used for out-of-band management of the equipment and communications circuit. Client configurations may also include dedicated circuits, as well as VPN tunnels into each FIS location.

Internal communications between FIS Fixed Income Processing Suite's primary and alternate data centers is distributed over a dedicated high-speed connection.

Data Protection and Storage

At the conclusion of each weekday business cycle, a full tape media backup of primary system databases, Source and Object code is made at the production data center.

Tape media is encrypted and sent off-site daily for storage in a third-party firm's storage vault. Media is cycled back on a pre-determined schedule as well as by special request. The third-party firm's storage vault operation is audited on a regular basis.

C. Business Continuity Testing

FIS Fixed Income Processing Suite Testing

A testing program encompassing numerous components of the Continuity Plan is facilitated on an ongoing basis. These test procedures are designed to help assess, at varying frequencies determined appropriate by FIS Fixed Income Processing Suite management and Operations personnel, that internal processes critical to the FIS Fixed Income Processing Suite application are validated.

FIS Fixed Income Processing Suite participates in annual business continuity testing, and performs disaster recovery exercises throughout the year with individual clients.

FIS Fixed Income Processing Suite annually tests remote access involving critical support representatives.

Employees supporting FIS Fixed Income Processing Suite participate in an annual office-wide evacuation and remote workforce test exercising:

- Procedures for determining employee whereabouts and status;
- Activation of the Incident Management Team and crisis communications;
- Activation of the Employee Information Hotline and Business Continuity website; and
- Remote Workforce plans, with representative employees working from home or other alternate location for the remainder of the day.

Grant Thornton

This report is confidential. Unauthorized use of this report in whole or in part is strictly prohibited.