Service Organization Control 1 Report on the Description of the IT General Controls System of Voya Services Company as it relates to Voya Retirement Insurance and Annuity Company and Voya Institutional Plan Services, LLC

For the Period October 1, 2015 to September 30, 2016 with the Independent Service Auditor’s Report Including Tests Performed and Results Thereof
Voya Services Company as it relates to
Voya Retirement Insurance and Annuity Company
and Voya Institutional Plan Services, LLC

IT General Controls

Service Organization Control 1 Report on the Description of the IT General Controls System
for the Period October 1, 2015 to September 30, 2016

Table of Contents

SECTION I – MANAGEMENT ASSERTION OF VOYA SERVICES COMPANY.................................1
SECTION I – MANAGEMENT ASSERTION OF INTERNATIONAL BUSINESS MACHINES
CORPORATION (IBM) ON ITS CONTROLS FOR VOYA SERVICES COMPANY AS IT
RELATES TO VOYA RETIREMENT INSURANCE AND ANNUITY COMPANY (VRIAC)...............3
SECTION II – INDEPENDENT SERVICE AUDITOR’S REPORT.........................................................5
SECTION III – DESCRIPTION OF IT GENERAL CONTROLS SYSTEM OF VOYA SERVICES
COMPANY ..................................................................................................................................................8

GENERAL DESCRIPTION OF OPERATIONS .................................................................................8
General Overview ..................................................................................................................................8
Scope of This Report ............................................................................................................................8

DESCRIPTION OF CONTROL ENVIRONMENT ..............................................................................9
Management’s Philosophy and Operating Style .................................................................................9
Organizational Structure .....................................................................................................................10
Oversight by the Board of Directors .................................................................................................10
Assignment of Authority and Responsibility ......................................................................................11

DESCRIPTION OF INFORMATION TECHNOLOGY ENVIRONMENT .............................................13
Logical Access ....................................................................................................................................15
Change Management ..........................................................................................................................17
Physical Access ..................................................................................................................................19
Job Processing .................................................................................................................................20
Data Backups ....................................................................................................................................21

SUBSERVICE ORGANIZATION .........................................................................................................22

SECTION IV – DESCRIPTION OF CONTROL OBJECTIVES, CONTROLS, TESTS AND
RESULTS OF TESTS (DESCRIPTION OF TESTS AND RESULTS) ....................................................23

PURPOSE AND SCOPE OF REPORT .................................................................................................23
CONTROL ENVIRONMENT COMPONENTS ......................................................................................23
TESTING PERFORMED AND RESULTS OF TESTS WHEN USING THE WORK OF
MANAGEMENT ........................................................................................................................................24
TESTING OF INFORMATION PRODUCED BY THE ENTITY ............................................................24
INFORMATION TECHNOLOGY GENERAL CONTROLS

Control Objective 1: Logical Access ................................................................. 25
Control Objective 2: Change Management ....................................................... 33
Control Objective 3: Physical Access ............................................................... 36
Control Objective 4: Job Processing ................................................................. 39
Control Objective 5: Data Backups ................................................................. 41
SECTION I

Management Assertion of Voya Services Company
Management Assertion of International Business Machines Corporation (IBM) on its Controls for Voya Services Company as it relates to Voya Retirement Insurance and Annuity Company (VRIAC)
SECTION I – MANAGEMENT ASSERTION OF VOYA SERVICES COMPANY

November 21, 2016

We have prepared the accompanying IT General Controls System (Description) of Voya Services Company as it relates to Voya Retirement Insurance and Annuity Company (VRIAC) and Voya Institutional Plan Services, LLC (VIPS), (collectively, “the Company” or “Voya”) (Service Organization) for users of system during some or all of the period October 1, 2015 to September 30, 2016 (user entities), and their independent auditors who have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by such user entities themselves, when assessing the risks of material misstatements of user entities’ financial statements. International Business Machines Corporation (IBM) is an independent service organization that provides certain computer operations and infrastructure support services (the Services) to VRIAC that constitute part of our IT General Controls System. The Description includes a description of IBM’s services, including controls of IBM relevant to the control objectives stated in the Description. IBM has provided the accompanying assertion titled, “Management Assertion of International Business Machines Corporation (IBM) on its Controls for Voya Services Company as it relates to Voya Retirement Insurance and Annuity Company (VRIAC)” about the fairness of the presentation of the portion of the Description relevant to the services provided by IBM. The management of the Company confirms, to the best of its knowledge and belief, that:

1. The Description fairly presents the IT General Controls System (System) made available to user entities during the period October 1, 2015 to September 30, 2016 for processing their transactions. The criteria we used in making this assertion were that the Description:

   (a) presents how the System made available to user entities was designed and implemented, including:

      • the types of services provided.
      • the procedures, within both automated and manual systems, by which those services are provided to user entities.
      • the related supporting information; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
      • how the System captures and addresses significant events and conditions.
      • the process used to prepare reports or other information provided to user entities.
      • specified control objectives and controls designed to achieve those objectives.
      • other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to the services provided.

   (b) does not omit or distort information relevant to the scope of the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities and their independent auditors, and may not, therefore, include every aspect of the System that each individual user entity and its independent auditor may consider important in the user entity’s own particular environment.
2. The Description includes relevant details of changes to the System during the period from October 1, 2015 to September 30, 2016.

3. The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period October 1, 2015 to September 30, 2016 to achieve those control objectives. The criteria we used in making this assertion were that:

   (a) the risks that threaten the achievement of the control objectives stated in the Description have been identified by management;

   (b) the controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent those control objectives stated in the Description from being achieved; and

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

Voya Services Company
SECTION I – MANAGEMENT ASSERTION OF INTERNATIONAL BUSINESS MACHINES CORPORATION (IBM) ON ITS CONTROLS FOR VOYA SERVICES COMPANY AS IT RELATES TO VOYA RETIREMENT INSURANCE AND ANNUITY COMPANY (VRIAC)

November 21, 2016

The accompanying Description of IT General Controls System of Voya Services Company as it relates to VRIAC controls that are managed by Voya Services Company and the related technology support services used to administer centrally managed controls (Description) prepared by Voya Services Company management includes a description of certain managed services provided by IBM Global Technology Services (IBM) related to certain of those Services for Voya Services Company as it relates to VRIAC during some or all of the period from October 1, 2015 to September 30, 2016. This is intended only for Voya Services Company as it relates to VRIAC, user entities of Voya Services Company as it relates to VRIAC’s system and the independent auditors of user entities who have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by user entities themselves, to understand the nature of the controls that are the subject of this report and any role the IBM controls may play in such user entities’ overall control structures when assessing the risks of material misstatements of user entities’ financial statements.

Because of inherent limitations, controls at IBM may not prevent or detect all failures of controls to operate as designed or intended; in addition, these controls are designed for common needs of multiple customers and may not include all aspects of controls that an individual customer may consider important for its own needs. Furthermore, we make no projection of any conclusions, based on our assertion, to future periods.

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

a. a portion of the Description that describes IBM controls designed and operated by IBM as part of its common controls for multiple customers (the IBM Controls) fairly presents those aspects of the controls that we believe are likely to be relevant to user entities in assessing their own controls during some or all of the period October 1, 2015 to September 30, 2016. The criteria we used in making this assertion were that the description of the IBM Controls:

(1) presents how the controls were designed and implemented, including:

• the types of services provided that are the subject of the IBM Controls;
• the procedures, within both automated and manual systems, by which those services are provided to the extent they relate to the IBM Controls;
• how the IBM Controls capture and address significant events and conditions;
• the process used by IBM to prepare reports or other information provided to Voya Services Company as it relates to VRIAC to the extent related to the IBM Controls; and
• certain other aspects of the IBM control environment, risk assessment process, information and communication processes, control activities and monitoring controls that we believe are relevant to the IBM Controls; provided however, that the description of the IBM Controls was prepared to meet the common needs of a broad range of user entities and the independent auditors of user entities, and may not, therefore, include every aspect of the IBM Controls that each individual user entity
and its auditor may consider important in the user entity’s own particular environment.

(2) at the level of detail provided in the Description, and subject to the accuracy of Voya Services Company as it relates to VRIAC assertion regarding the IT General Controls System, does not omit or distort information relevant to the scope of the IBM services, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the IBM services and the IT General Controls System and may not, therefore, include every aspect of the IBM services that any individual user entity of the IBM services or IT General Controls System or its independent auditors may consider important in the user entity’s own particular environment.

b. the Description includes relevant details of changes to IBM’s description of the IBM Controls during the period from October 1, 2015 to September 30, 2016.

c. The IBM Controls related to the combined control objectives specified by Voya Services Company and stated in the Description that relate to the IBM Services were suitably designed and operated effectively throughout the period October 1, 2015 to September 30, 2016 to achieve those control objectives; provided, that “effectively” for these purposes means effectively for purposes of achieving the IBM control objectives relating to the IBM Controls. The criteria we used in making this assertion were that the IBM Controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority. The assertions and other statements contained herein do not (i) amend any agreement between IBM and any customer or user organization or their respective rights and obligations under any agreement to which the controls described herein relate or create any rights or causes of action under any such agreement or otherwise, or (ii) substitute for any independent analysis or verifications otherwise required of a user entity or its representatives. IBM makes no assertion, representation or warranty regarding (i) the adequacy of controls required by the customer under any such agreement or otherwise or any controls other than the IBM Controls or (ii) the adequacy, effectiveness or significance of the System or the design or effectiveness of IBM Controls with respect to ultimate assessments of control risk at user entities, which are dependent on their interaction with the controls and other factors present at or implemented by individual user entities. User entities retain ultimate authority and responsibility for determining whether controls used or implemented by them are relevant to or sufficient for their needs.

International Business Machines Corporation
SECTION II

Independent Service Auditor’s Report
SECTION II – INDEPENDENT SERVICE AUDITOR’S REPORT

To the Management and Board of Directors of Voya Services Company

Scope
We have examined Voya Services Company as it relates to Voya Retirement Insurance and Annuity Company’s (VRIAC) and Voya Institutional Plan Services, LLC’s (VIPS) (collectively, “the Company” or “Voya”) accompanying Description of the IT General Controls System for the processing of user entities’ transactions throughout the period October 1, 2015 to September 30, 2016 (Description) and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description. International Business Machines Corporation (IBM) is an independent service organization that provides certain computer operations and infrastructure support services to Voya Services Company as it relates to VRIAC that constitute part of the IT General Controls System. The Company’s Description includes a description of IBM’s services, including controls of IBM relevant to the control objectives stated in the Description.

The Company’s responsibilities
The Company has provided the accompanying assertion titled, “Management Assertion of Voya Services Company” (Voya Services Company Assertion) about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related control objectives stated in the Description. The Company is responsible for preparing the Description and the Voya Services Company Assertion, including the completeness, accuracy, and method of presentation of the Description and the Voya Services Company 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 Voya Services Company Assertion, and designing, implementing, and documenting controls to achieve the related control objectives stated in the Description.

IBM’s responsibilities
IBM has provided the accompanying assertion titled, “Management Assertion of International Business Machines Corporation (IBM) on its Controls for Voya Services Company as it relates to Voya Retirement Insurance and Annuity Company (VRIAC)” (IBM Assertion) about the fairness of the presentation of the portion of the Description related to certain computer operations and infrastructure support services and suitability of the design and operating effectiveness of IBM’s controls described therein to achieve relevant portions of the related control objectives stated in the Description. IBM is responsible for preparing the IBM Assertion, including its completeness, accuracy and method of presentation, providing the services as described in the Description, selecting the criteria stated in the IBM Assertion, and implementing and documenting controls to achieve the Description either wholly or in conjunction with controls implemented by Voya.

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 described therein to achieve the related control objectives stated in the Description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about
whether, in all material respects, the Description is fairly presented and the controls described therein are suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period October 1, 2015 to September 30, 2016.

An examination of a description of a service organization’s system and the suitability of the design and operating effectiveness of the service and subservice organizations’ controls described therein to achieve the related control objectives stated in the Description involves performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives. Our procedures included 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. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives were achieved. An examination engagement of this type also includes evaluating the overall presentation of the Description, the suitability of the control objectives, and the suitability of the criteria specified by the service and subservice organizations and described in the Voya Services Company Assertion and IBM Assertion (Assertions). We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations
The Description is prepared to meet the common needs of a broad range of user entities and their independent auditors 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 or subservice organization may not prevent, or detect and correct, all errors or omissions in Information Technology General Controls services supporting the processing or reporting of user entities’ transactions for the applications described in Section III provided to user entities. 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 or subservice organization may become ineffective or fail.

Opinion
In our opinion, in all material respects, based on the criteria described in Voya’s Assertion:

a. the Description fairly presents the Company’s IT General Controls System that was designed and implemented throughout the period October 1, 2015 to September 30, 2016;

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 October 1, 2015 to September 30, 2016;

c. the controls of Voya Services Company and IBM tested were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period October 1, 2015 to September 30, 2016.
Description of tests of controls
The specific controls tested and the nature, timing, and results of those tests are listed in the accompanying Description of Control Objectives, Controls, Tests and Results of Tests. (Description of Tests and Results)

Restricted use
This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of the Company, user entities of the Company’s IT General Controls System during some or all of the period October 1, 2015 to September 30, 2016, and the independent auditors of such user entities, who 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 misstatements of user entities’ financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Ernst & Young LLP

November 21, 2016
Atlanta, Georgia, United States of America
SECTION III

Description of the IT General Controls System of Voya Services Company
SECTION III – DESCRIPTION OF IT GENERAL CONTROLS SYSTEM OF VOYA SERVICES COMPANY

GENERAL DESCRIPTION OF OPERATIONS

General Overview

VRIAC, VIPS and Voya Services Company (collectively referred to as “the Company” or “Voya”) are part of Voya Financial, Inc. (Voya Financial), and provides a full range of retirement plan services to businesses and corporations, educational institutions, state and local governments and non-profit organizations.

The Company provides recordkeeping, and administration services to over 35,000 Plan Sponsors in the Corporate and Tax Exempt (e.g., Health, Education and Government) (TEM) sectors as part of Voya Financial’s Retirement division. These plans are established under sections 401(a)/ (k) (referred to as Corporate throughout this report), 403(b)(1)/ (7) and 457 (referred to as TEM throughout the report) of the Internal Revenue Code.

As of September 30, 2016, the Company had over $334 billion of assets under management and administration.

Primary operations for the Company are located in Windsor, Connecticut, Braintree, Massachusetts, and Jacksonville, Florida with data centers supporting applications in this report in Jacksonville, Florida and Minneapolis, Minnesota. The Company also maintains primary Retirement Readiness Service Centers (RRSC) in Windsor, Connecticut, Jacksonville, Florida and Des Moines, Iowa.

Scope of This Report

This report describes the Company’s Information Technology General Controls (ITGC) for Logical Access, Change Management, Physical Access, Job Processing and Data Backups, in support of the applications relevant to the following Service Organization Control (SOC 1) reports issued by the Company:

<table>
<thead>
<tr>
<th>Voya Entity</th>
<th>SOC 1 Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voya Retirement Insurance and Annuity Company</td>
<td>Contract and Plan Administration Services for the EASE Omni Platform</td>
</tr>
<tr>
<td>Voya Retirement Insurance and Annuity Company</td>
<td>Contract Administration Services for the ACES Platform</td>
</tr>
<tr>
<td>Voya Institutional Plan Services, LLC</td>
<td>Institutional Defined Contribution Services</td>
</tr>
<tr>
<td>Voya Institutional Plan Services, LLC</td>
<td>Institutional Defined Benefit Plan Services</td>
</tr>
</tbody>
</table>

The Company uses IBM as a subservice organization to perform various controls relevant to the administration of the ACES platform for VRIAC. These controls are included in scope of this report and only relate to VRIAC Contract Administration Services for the ACES Platform.
DESCRIPTION OF CONTROL ENVIRONMENT

The overall attitude, awareness, and actions of the Board of Directors, management, and others reflect the importance of the control environment, risk assessment, information and communication, and monitoring within the organization as described in the following:

- Management’s Philosophy and Operating Style
- Organizational Structure
- Oversight by the Board of Directors
- Assignment of Authority and Responsibility; including
  - Chief Financial Officer
  - Compliance
  - Corporate Audit Services
  - Financial Control Risk
  - Human Resources’ Policies and Practices
  - Information Technology
  - Legal
  - Operational Risk Management
  - Technology Risk and Security

Management’s Philosophy and Operating Style

Management is committed to providing quality, accurate, and timely service to customers. Employees follow detailed workflow practices and internal control procedures to strive to achieve the highest standards of customer satisfaction.

Adherence to policies and procedures is monitored by senior management. The philosophy of senior management is to manage and control risk through a hierarchy of control policies, procedures and management processes which reinforce the internal controls. Management is challenged to assess and monitor risk that could affect the Company’s ability to provide reliable transaction processing. These efforts include, but are not limited to identifying, assessing and managing risks associated with implementing new technologies and business products, integrating new personnel, and addressing regulatory, industry, or other the Company initiatives.
To help align business strategies and goals with operating performance, management is committed to maintaining effective communication with all personnel. Management, across all functions, discusses the status of current customer processing, organizational structure and other matters of interest and concern. Issues or suggestions identified by personnel, or independent reviews are readily brought to the attention of management to be addressed and resolved.

Organizational Structure

The organizational structure provides an overall framework for planning, directing, and controlling operations. Authority and responsibility assigned within the organizational structure is designed to provide adequate staffing, segregation of duties, efficiency of operations, and adequate concentration of knowledge and skills.

Voya has organized a separate IT department to perform centralized system support functions for all user divisions, including functions such as application development, information security, network administration, and network security.

The IT organization reports to the operations unit of Voya. The IT organization is led by the Chief Information Officer (CIO), who reports to the business unit Chief Operations Officer.

The following areas report directly to the CIO:

- Analytics & Data Management – Responsible for business information and architecture, business intelligence and analytics, data integration and orchestration services, data management and data quality, and application database support
- Digital Delivery Services – Responsible for full system development for Individual Retirement and Voya Financial
- Enterprise Application Services – Responsible for IT service delivery for Finance, Human Resources (HR), Legal, Financial Risk, and Communications applications
- Enterprise Architecture – Responsible for integrated technology and roadmap planning, enterprise technology and standards, and architecture governance
- Retirement IT – Responsible for IT service delivery for Retirement Services applications
- Strategy & Delivery Office – Responsible for the management of strategic IT work portfolios and for leading the execution of IT projects across the organization
- Technology Risk and Security Management – Responsible for access management, security operations, security management and recovery services, risk management, IT controls, and security architecture and platforms
- Technology Services – Responsible for end-user services, network middleware and distributed systems engineering, operations, and service delivery

Oversight by the Board of Directors

The Board of Directors has general oversight responsibility for the business matters of the Company.
Assignment of Authority and Responsibility

The following departments are generally considered to be part of the control environment:

**Finance**
The Chief Financial Officer (CFO) leads the Retirement finance function. This responsibility includes the oversight of all financial activities including financial reporting, accounting policy and expense management, and product pricing review and analysis.

Financial Control Risk (FCR) is a component of the Voya Financial Controller’s organization. This department provides resources and methodologies related to internal control evaluation (testing) and awareness with primary emphasis on the controls over financial reporting for Voya’s legal entities that are subject to The Sarbanes-Oxley (SOX) Act of 2002 and the National Association of Insurance Commissioners Model Audit Rule (MAR). FCR's work and activities are performed on behalf of management and are executed in coordination with the activities of the external auditor, Internal Audit and Advisory Services (Internal Audit), and Operational Risk Management (ORM). FCR performs testing of internal controls over financial reporting for those areas that are in-scope for SOX and MAR; provides controls awareness/guidance on new process implementation or process redesign; and performs other functions at the request of management. FCR works with management to evaluate the design and effectiveness of controls while assisting in reducing risk to an acceptable, cost effective level.

**Compliance**
Designated Compliance Officers are accountable for developing and maintaining compliance standards. It is the responsibility of these Compliance Officers, working with internal legal counsel, to monitor the adherence to the Voya Financial Code of Business Conduct and Ethics and to assist employees in achieving the highest standards of integrity and business conduct.

Integrity is the key to continued success in all dealings with plan sponsors, participants, shareholders, employees, regulators and other business associates. All individuals, either employed or associated with the Company, are responsible for conducting themselves in compliance with the Voya Financial Code of Business Conduct and Ethics, other Company policies, and applicable laws and regulations.

**Internal Audit and Advisory Services**
Voya Financial's Internal Audit function provides independent objective assurance and consulting services designed to add value, improve operations and support the Voya Financial, Inc. Audit Committee of the Board of Directors (Audit Committee) in fulfilling its oversight role with the Company. Internal Audit employs a systematic, disciplined approach to evaluate and offer recommendations for improving the effectiveness and efficiency of risk management, control, and governance processes for the various businesses and legal entities that are a part of Voya Financial. Internal Audit independence and authority are granted in the form of an Audit Charter approved by the Audit Committee.

Internal Audit develops its audit plan using a risk-based approach. This approach enables Internal Audit to align its audit activity with the business objectives of the Company and the key value drivers of the organization. Audit effort is prioritized based on risk and regulatory requirements. The annual audit plan is approved by the Audit Committee and communicated to Company management.

Results and conclusions of audit work are reviewed with operating and financial management responsible for the activity being evaluated. Audit reports include an opinion on the adequacy of internal controls for the activities within the scope of the audit, audit findings and recommendations, as well as management’s
corrective action plans with due dates. Corrective action plans are monitored in a centralized application, and each remediation effort is validated by Internal Audit before a finding is considered closed.

Periodic reports summarizing audit activity, audit results and status of management’s corrective action plans are presented to the Audit Committee and management.

**Human Resources’ Policies and Practices**

Policies and practices are in place related to hiring, training, evaluating, promoting, compensating, and terminating employees. All prospective employees are screened by the Human Resources (HR) Department, including background investigation and reference verification. Hiring policies include requiring the candidate to have obtained a minimum level of education and experience. Descriptions for all job classifications define job requirements and assist with properly managing employee workload. Final employment decisions are made by the department seeking to hire the individual.

Both formal and informal educational advancement opportunities are promoted, and employees are encouraged to take advantage of existing training programs. This training is designed to advance employees’ careers and provide employees with the skills necessary to provide quality service to customers.

For terminated employees, Voya manages the transition of a terminated employee’s existing projects, as well as access to facilities and business applications, in a manner appropriate to the termination.

**Information Technology**

Information Technology (IT) maintains and executes a framework of IT policies, procedures and controls that support and complement the business controls over the initiation, authorization, recording, processing and reporting of transactions. In addition, IT performs ongoing monitoring of the status of application and transaction processing by the Company’s systems.

**Legal**

The Voya Financial Legal Department has primary responsibility for providing legal services to Voya Financial including the Company. The legal services include advising the Company on legal issues relating to the development, sale and administration of the Company’s products and related services. Additionally, the Voya Financial Legal Department monitors legislative and regulatory activity that may potentially impact the Company.

**Operational Risk Management**

Retirement’s ORM function reports to the Chief Risk Officer of the Retirement business unit. ORM receives guidance and direction from Retirement management, as well as from Corporate Risk Management, to ensure operational risks are effectively managed by business management. ORM supports business management in making improved decisions when risks are involved. This entails advising management on existing and emerging risk exposures, developing and improving processes and related internal control design, tracking timely resolution of open issues, performing analysis of operational errors and conducting targeted risk assessments.

**Technology Risk and Security Management**

Technology Risk & Security Management (TRSM) is a part of IT that provides guidance and direction to Retirement and Information Technology management, to ensure information risks are effectively managed. Among its many responsibilities, TRSM acts as a liaison between the Company’s business units and its external auditor, to help ensure that internal IT control issues are addressed appropriately and timely. They also provide advice on developing and improving processes and related internal controls.
DESCRIPTION OF INFORMATION TECHNOLOGY ENVIRONMENT

Primary data centers supporting applications in this report are in Jacksonville, Florida and Minneapolis, Minnesota. The Company also uses IBM as a subservice organization to perform various controls relevant to the administration of the ACES platform for VRIAC at IBM’s Boulder, Colorado data center. This section provides information on the various aspects of computerized information systems controls, which include installing network, mainframe, and distributed (Windows and midrange) systems, maintaining the network and data centers, administering the operations of the data centers, securing the environment, and managing the operations of business application systems.

The IT general controls in this report only relate to the following primary applications addressed in the related SOC 1 reports for VIPS and VRIAC.

**ACES Administration Application (ACES)**
ACES is a mainframe engine. Information is entered through various on-line front-end applications and directly to ACES to support contract information, financial transactions, and non-financial transactions for Corporate and TEM business within VRIAC. Inquiry and data update access is available. The majority of transactions are stored on data collect files, which are processed in the batch cycle. There is limited real-time processing. This system is hosted by IBM in its Boulder, CO data center.

**AdminStation**
A module within the OmniPlus system, which is an html-based product developed by VIPS to manage plan-level configuration parameters of other applications and functions, such as job submissions (jsubs) and loans.

**EASE Omni**
EASE Omni is a daily-valued application that processes customer data relating to the Corporate and TEM markets within VRIAC. EASE Omni offers full Plan Sponsor and participant level plan administration. Functions supported by EASE Omni include transaction processing, record maintenance, and ad-hoc reporting. Its primary downstream interfaces include commissions systems, numerous financial reporting applications, as well as customer service platforms for the RRSCs, Voice Response Unit, and PWeb.

**Fund Operations Reporting and Control for the Enterprise (FORCE)**
FORCE is an enterprise application that supports the daily pricing of investment options offered in Voya products/plans. FORCE collects net asset value (NAV) and dividend data, and calculates accumulation unit value (AUV) data for the applicable investment options offered. FORCE is also used for the daily trading in the investment options offered within Voya’s products/plans. Trade instructions by shareholder account are provided to each of the investment companies.

**Fund Operations - Accounting**
Application module that processes daily accounting of trades / settlement, monthly allocation / accounting of asset based revenue, and calculation / reconciliation of fund company revenue.
**Fund Operations Pricing**
Application module that collects and processes pricing/dividend data for all investment options offered in Retirement Services, Annuity and Life products, and provides pricing data to Voya recordkeeping systems.

**Fund Operations Trading**
Application module that processes recordkeeping system trades for all investment options offered in Retirement Services, Annuity and Life products, and transmits the trades to applicable investment companies.

**Fund Operations Share Recon**
Application module that reconciles Voya positions by shareholder account to fund company records, validating the accuracy of pricing data and trade processing.

**OmniPlus**
A defined contribution participant accounting system developed by SunGard. OmniStation, a front-end application, and OmniSecurity, a front-end security management system for OmniStation, control access to the OmniPlus functions. These systems provide daily transaction activity, online inquiry, and standard and customized reporting for VIPS.

**OmniDB**
A defined benefit record keeping system that was developed by SunGard and implemented on UNIX and LINUX platforms. OmniDB provides transaction activity, online inquiry and standard and customized reports for VIPS until Voya exited the Defined Benefits market, effective 06/30/2016.

**Pension Calculator**
A business rules management system that was used as a pension calculator for VIPS until Voya exited the Defined Benefits market, effective 06/30/2016. This system was integrated with OmniDB.

**PeopleSoft electronic Disbursements System (eDS)**
PeopleSoft eDS is a Voya custom built application that resides in the PeopleSoft Financials environment. PeopleSoft eDS processes disbursement request information from the administration systems for policyholder and commission payments for VRIAC. PeopleSoft eDS has on-demand functionality that allows checks, wires, and ACHs to be produced on an as needed basis.

**PLUS**
A lump sum and periodic payment application utilized by State Street Retiree Services (SSRS) and hosted by Voya.

**PSRConnect**
Client Service system that consists of call center workstations used to service participant calls made to the RRSC. This front-end system for VIPS is the conduit for call center representatives’s to the in-scope Omni platforms. This application does not store data.
PWeb
PWeb is a front-end to the platforms and provides self-service capabilities to participants through the use of the Internet. Based on plan provisions, participants are able to perform allowed transactions as well as certain inquiry and update functions.

ReconPlus
The ReconPlus application (Frontier) is a vendor product from Fiserv with a Windows interface designed to automate the reconciling of accounts for VIPS and VRIAC. It accomplishes this through the use of a data-matching engine driven by pre-defined matching criteria. It is used to reconcile the administration systems and the various bank accounts to the general ledger. Source code is not available for modification.

Logical Access
Voya’s environment includes both a distributed and mainframe environments. The logical access controls described in this report includes coverage for both environments.

Voya IT Risk Policies and Standards outline controls for logical access. These standards document the policies and procedures for application, database and network access control, such as those pertaining to password configuration parameters and log-on attempt limitations. Annually, the IT Risk Policies are reviewed by the Voya Financial Risk Committee or its delegate. Any amendment to these policies requires review and approval from either the Voya Financial Board or its delegate. The Control Standards Approval Board approves new IT Control Standards. (1.1)

For the network and mainframe environments, the password requirement standard is enforced via configuration settings documented in the domain policies and through IBM’s RACF configuration settings for the mainframe. Any change to the password policies that would make the password requirements no longer compliant with the company standards would require approval via the change management process. For the application environment, prior to or concurrent with application implementation in production, and on a periodic cycle based on risk thereafter, IT Asset Custodians approve completed Application Operational Security Guidelines (AOSGs) or Security Control Assessments (SCAs), confirming in-scope applications comply with password parameters. (1.2).

Requests for new access or changes to existing access rights for network, mainframe, server, database, and applications are submitted via the applicable forms in ServiceNow. Voya asset owners/managers or their delegate approve access (both non-privileged and privileged) to IT assets, based on the user’s job responsibilities and as documented in the access request form. (1.3) Oracle Identity Management (OIM) automatically disables the user account for terminated employees’ (including contract employees) access to network domains within 24 hours of receipt of the daily HR system termination feed. (1.4) Access to downstream applications is revoked either by the Oracle Identity Analytics (OIA) generated or manager submitted ServiceNow tickets.

Network Level Access, Mainframe Level Access, Operating System Server Access and Database Level Access
Administrator access to the Network Domain controllers and Active Directory, which are used to manage access to the network resources, is granted based on job responsibilities. Active Directory access is required prior to access being granted to the mainframe. Semi-annually, managers or their delegate review to certify or revoke access (both non-privileged and privileged) to IT assets, to ensure the level of access/role remains commensurate with job responsibilities. (1.5) Semi-annual reviews of privileged access to network domains
and the mainframe are performed utilizing the OIA tool. Subsequent to the entitlement review process, access is disabled by the assigned team based on the revoke requested by the manager or delegate. (1.6)

Network-level access is automatically disabled upon termination at the Network layer. Mainframe level access is manually disabled upon notification of terminations.

Administrator access to application servers and databases servers is restricted to IT operations and system administration personnel based on their job responsibilities.

For database and operating system level access, IT security administration personnel are notified of terminations. Access is removed at the application server and database server levels.

**Application Level Access**

Voya asset owners/managers or their delegate approve access (both non-privileged and privileged) to IT assets, based on the user's job responsibilities and as documented in the access request form. (1.3)

Application access for individuals, including privileged access, is reviewed semi-annually by management to ensure access remains commensurate with job responsibilities. (1.5) The semi-annual reviews includes a review of users with privileged and non-privileged access to network domains, the mainframe, servers, databases, applications, job schedulers, as well as the privileged tools. User access listings are generated from OIA and are provided to managers for review. Subsequent to the entitlement review process, access is disabled by the assigned team based on the revoke requested by the manager or delegate. (1.6)

Managers review and confirm usage of privileged accounts by developers in production is appropriate. (1.7)

Access to privileged functions at the application, database, server, network and mainframe layers is controlled through the use of privileged tools. Usage activity by developers in production is logged. Once activity is logged, the log is forwarded to the user's manager where it is reviewed and authorized by the manager (some may review daily, others may be scheduled to be bi-weekly).

The managers receive an email alert requesting that they review the log, along with a due date for the completed review listed in the subject line. Managers are responsible for completing their review within the time provided to them. If they do not, additional follow ups are sent to them until they review the logs. The manager is then responsible for reviewing each usage for reasonability and validity, and updates the log report with correct usage reason and authorization. Once managers have updated and authorized all uses on their report, they validate the entire report and send it back to the technical team for completion. Any unauthorized or questionable usages are followed up on by the manager as necessary. The technical team then verifies that all usage reasons and authorizations have been completed and compiles a completed report of all manager reviews for internal documentation. Non-response from managers is put into an escalation process where they are reminded by email and in person if necessary.

**Network Level Security**

Firewalls are used to limit ports available to external users and to limit access to internal computing resources. (1.8) Only network management personnel, based on their job responsibilities, have administrator access to firewalls. (1.9) An IPS/IDS tool is used to monitor, identify, and block potential unauthorized access on the network. It is configured to generate alarms based on unusual network activity. Network support and information security personnel monitor and act upon alarms. (1.10)
Virus protection software is installed on all email servers and configured to automatically update the virus definitions.

**Change Management**

Voya IT Risk Policies and Standards outline controls for change management. These standards document the policies and procedures for application, database, network and mainframe change control, such as those pertaining to testing, approval, and migration of changes to production.

Annually, the IT Risk Policies are reviewed by the Voya Financial Risk Committee or its delegate. Any amendment to these policies requires review and approval from either the Voya Financial Board or its delegate. The Control Standards Approval Board approves new IT Control Standards. (2.1)

Systems development and change controls ensure system software development and programming changes are authorized, prioritized, tested, approved, implemented, and documented. Policies provide for segregation of duties among business, application, and production acceptance personnel between development, testing, and production environments. Code asset management tools are used throughout the program change control process.

Application and system changes are logged into the ServiceNow change management system. Once a change is logged into the change management system, the appropriate approver is identified and automatically added. As the change process progresses, the entry in the change management system is updated appropriately.

Development, testing, and acceptance environments are separate from the production environment. (2.2)

On a regular basis, each respective IT application area works with the business to discuss change requests to ensure that appropriate resources are available and assigned.

After appropriate business approvals, an application programmer is assigned to the system change request and identifies the affected modules. Developers check the source modules out of the production libraries and move a copy into the development environment or to their workstation where the authorized changes are performed. Once changes have been made within the development environment or on the developer’s workstation, copies of the changed code are then migrated to a user testing environment by authorized individuals. Specific configuration parameters provide for segregation of access between development, testing, and production environments as defined for each application.

Changes are reviewed and approved weekly during the Production Promotion meeting by the Change Management group after conferring with business and IT management. This group reviews all changes determined to be ‘major risk’ changes and certain ‘medium risk’ changes to help ensure that they are adequately prioritized, tested, approved and implemented in a way that is not disruptive to the production environments. Concerns over application and systems software changes are discussed, the impact is assessed and potential conflicts are resolved. Emergency code change requests are generally made directly into production and validated in production before turning the application back over for use.

Planned changes are accompanied by an approved test plan that documents testing results to support the required approval to move to production. (2.4) Change Agents review all activity for accuracy, completeness, and risk/impact prior to production installation. If the change does not operate as intended,
the source module is moved back to the development environment or workstation where corrections are made, and then the revised code is retested by the end users or IT business Analysts.

Prior software versions are archived.

It is the responsibility of the appropriate change management committee to review and schedule all major system development and modification projects that have been approved by the Project Prioritization Process. Concerns over application and systems software changes are discussed, the impact is assessed, and potential conflicts are resolved.

Once testing is completed, ServiceNow is used to obtain approval from IT management to proceed with the change process. A production change request form is submitted to Production Control, the Desktop Release Manager (DRM) area, or the application team librarian before any mainframe or distributed program is moved into the production environment. For infrastructure and application changes, the appropriate Owner or Custodian approves all changes to production (excluding Emergency changes). (2.3)

Prior to migration to production, changes are reviewed and approved weekly by the Change Approval Board (CAB). (2.5) CAB reviews major, medium, and standard risk changes to determine the impacts and/or conflicts of the changes. Once the change impacts are reviewed and approved, the change ticket is updated within ServiceNow with the approval information.

Each morning, a Daily Change report is produced from ServiceNow and posted on Voya’s intranet for IT Change Management personnel for requests that were approved within the past twenty-four hours.

Approved software changes are released into the production environment by Migration Control, DRM personnel, or the application team librarian on a pre-defined and pre-approved release management schedule. Distributed system changes are released from a testing environment to the production environment by the application librarian.

Library management utilities are used to manage mainframe and distributed production application libraries, and to document and track changes to source code.

Subsequent to development and testing, the designated migration team, who is independent of the developer, deploys code into production through the approved managed ID process. (2.6) The managed ID process includes utilizing the privileged tools to control how changes are being migrated to production. Provisioning, de-provisioning and review of these privileged tools follow the process described within the logical access section of this narrative. Changes are either manually or automatically migrated into production. For manual changes, once approvals are granted for a change the Release Engineering and Migration control personnel configure the changes in a staging environment to be pulled into production via a synchronization job process. Other change management tools automatically migrate a change to production once the flag in the tool has been set to indicate approval is received. Segregation of duties is enforced through the use of tools and directory permissions.

All releases to the production environment are monitored after implementation. A meeting is held by IT management/Release management upon completion of the release to discuss post-implementation issues.

Requests for emergency changes to applications, databases, servers, network and the mainframe are documented and approved by the responsible Voya change owner. Approvals are documented in the
incident ticket and added to a change ticket, which must be created and closed within one business day of
the emergency change. (2.7)

Physical Access

IT Risk Policies and Standards outline controls for physical security. These standards document the policies
and procedures for physical data center access. Annually, the IT Risk Policies are reviewed by the Voya
Financial Risk Committee or its delegate. Any amendment to these policies requires review and approval
from either the Voya Financial Board or its delegate. The Control Standards Approval Board approves new
IT Control Standards. (3.1)

Voya’s Minneapolis, Minnesota and Jacksonville, Florida Data Centers

Access through all entry and exit points to the Voya data centers is restricted through the use of a card
access control system. (3.2) Access to card access applications is restricted to Facility Access Coordinators
based on their job responsibilities. Only Facility Access Coordinators may make changes to user access
levels. (3.3)

The IT Infrastructure Director or the Data Center Service Team approves access to the data centers
commensurate with job responsibilities. (3.4) Semi-annually, managers review and validate system
generated access lists for the data centers to ensure the level of access/role remains commensurate with job
responsibilities. (3.5)

All entry and exit doors at the data centers are connected to an alarm system in the Central Security Control
Center or Local Security Station to monitor for unauthorized entry. If the doors are held open for an
extended period of time, an alarm is triggered.

Video cameras and monitoring equipment are installed near the entry and exit points to the data centers and
at perimeter areas to allow security personnel to monitor activities around the critical entry points and the
outside perimeter of the data centers. The video displays are monitored 24 hours/day and 7 days/week by
on-site security personnel.

IBM’s Boulder, Colorado Data Center

All points of access to the data center are secured at all times. The doors are closed, locked, and designed
to prevent or delay low-level forced entry attempts. If the doors remain open for an extended period of time,
an alarm will sound to prevent possible unauthorized entrance. Those doors designated as “Exit Only” have
no removable exterior hardware. For controlled areas that have emergency exits, exits have audible alarms
and are monitored by security personnel. Periodic verification that the alarms are functioning are performed,
documented and retained. (3.8)

Access to the data center is controlled by dual authentication including a card-key access system and
biometrics technology. In addition, the entry point to the data center is a vestibule man-trap and uses an
anti-pass back feature where individuals also must utilize the card-key access system to exit the data center.
Access activity is recorded for the data center by the card-key access system.

Local external Security personnel receive notification of access security breaches via local alarm. Closed
circuit television (CCTV) cameras record the data center doors and Emergency Power Off (EPO) switches
twenty-four hours a day and seven days a week. Additionally, CCTV’s, physical patrols, and monitoring
equipment enable external Security personnel to monitor the activities around critical facilities, the loading
dock, critical entry points, and the outside perimeter of the campus where the Boulder data center reside. A combination of both twenty-four hours a day and seven days a week recording and event driven recording is utilized to monitor activities in areas outside of the data center.

IBM’s access to controlled areas is restricted to authorized personnel only and requires documented approval from management.

All individuals without authorized access to the controlled areas must sign in and be escorted by an individual with approved controlled area access. (3.6) IBM’s levels of access rights to controlled areas are fully revalidated on an annual basis. An annual revalidation is performed to determine that a business need for access still exists. (3.7)

Job Processing

Voya IT Risk Policies and Standards outline controls for Job Processing. These standards document the policies and procedures for job scheduling processes and tools. Annually, the IT Risk Policies are reviewed by the Voya Financial Risk Committee or its delegate. Any amendment to these policies requires review and approval from either the Voya Financial Board or its delegate. The Control Standards Approval Board approves new IT Control Standards. (4.1)

New or modified job streams, resulting from program changes, follow a structured migration process into the production environment. Defined steps and processes are followed from development, through QA, and implementation to production. Additionally, prior to migrating modifications into production, appropriate documentation, review, and sign-offs are required as part of the systems test. This determines, among other things, that the job stream is scheduled in the appropriate sequence.

Access to job schedulers and their specific functions is limited to authorized users. The IT Infrastructure Director or Production Control Managers approve requests for access to job scheduling tools, based on the user's job responsibilities and as documented in the ServiceNow ticket. (4.2) Semi-annually, managers or their delegate review, certify or revoke access (both non-privileged and privileged) to IT assets, to ensure the level of access/role remains commensurate with job responsibilities. (4.3) Subsequent to the entitlement review process, access is disabled by the assigned team based on the revoke requested by the manager or delegate. (4.4) Periodic reviews conducted by Voya of greater than read access to the scheduling tools are performed utilizing OIA.

The Technology Services Distributed Scheduling Team creates or changes job schedules as requested in the approved change request. (4.5). Only IT operations, production control and systems administration personnel, based on their job responsibilities, have the ability to perform changes to a job schedule in the production environment.

In the event that a job terminates abnormally, the Voya or IBM application or infrastructure support team resolves the job failure and documents the resolution action in the ServiceNow ticket. (4.6)

A daily meeting is held by IT Operations to discuss the highest priority incidents that occurred in the prior production run cycle and any outstanding priority incidents from prior production cycles that have yet to be resolved. The purpose of this meeting is to discuss circumstances surrounding the incidents, possible causes, resolutions applied and facilitate closure of any outstanding incidents.
Data Backups

Voya IT Risk Policies and Standards outline controls for File Backups. These standards document the policies and procedures for data backup and restoration. Annually, the IT Risk Policies are reviewed by the Voya Financial Risk Committee or its delegate. Any amendment to these policies requires review and approval from either the Voya Financial Board or its delegate. The Control Standards Approval Board approves new IT Control Standards. (5.1)

Data backup and recovery tapes are generated through the job scheduling process as described within the Job Processing section of this report.

ACES
For the ACES mainframe environment, Voya application owners are responsible for ensuring that critical data is backed up by IBM specifying the frequency of backups via a backup schedule. These specifications are implemented using Job Control Language. (5.2)

Voya-hosted Applications
Backups are executed according to business requirements and stored securely. (5.3) For applications that reside in the Minneapolis, MN and Jacksonville, FL data centers, data is replicated between the two data centers through a synchronization job. In the event a data synchronization job terminates abnormally during replication between systems, error notifications are automatically generated. IT operations personnel follow-up on error notifications and resolve the issues. (5.4) Disaster recovery servers are located in a separate location from production servers.

Modifications to backup jobs follow the change management process described above under Change Management.
SUBSERVICE ORGANIZATION

The Company uses IBM as a subservice organization to provide certain computer operations and infrastructure support services pertaining to Logical Access, Physical Access, Change Management, and Job Processing related to the ACES application.

- Logical & Physical Access – IBM contractors are provisioned access via the noted Voya processes. IBM is responsible for approving access for their employees at the time of provisioning as well as semi-annually (1.3, 1.5, 3.6, 3.7, 3.8).

- Change Management – All changes to configuration items are subject to Voya's SDLC controls. Pieces of these controls are carried out by IBM contractors (2.3, 2.7).

- Job Processing – All job scheduling controls are subject to Voya's policies and procedures. IBM contractors may execute the controls but the process is managed and owned by Voya and documented in ServiceNow (4.2, 4.5, 4.6, 5.1).
SECTION IV

DESCRIPTION OF CONTROL
OBJECTIVES, CONTROLS, TESTS AND
RESULTS OF TESTS (DESCRIPTION OF
TESTS AND CONTROLS)
SECTION IV – DESCRIPTION OF CONTROL OBJECTIVES, CONTROLS, TESTS AND RESULTS OF TESTS (DESCRIPTION OF TESTS AND RESULTS)

PURPOSE AND SCOPE OF REPORT

On the pages that follow, the description of control objectives and the controls to achieve the objectives have been specified by, and are the responsibility of the Company. The testing performed by EY and the results of tests are the responsibility of the service auditor.

The control environment represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by the Company. In planning the nature, timing, and extent of EY’s testing of the controls specified by the Company, they considered the following aspects of the Company’s control environment: organizational structure, policies and procedures, risk assessment processes and management monitoring procedures.

CONTROL ENVIRONMENT COMPONENTS

The control environment represents the collective effect of various components in establishing, enhancing or mitigating the effectiveness of specific controls. In addition to tests of the operating effectiveness of controls in the matrices of this report, EY’s procedures also included tests of, or consideration of, the relevant components of the Company’s control environment, including:

- The Company’s organizational structure and the segregation of duties
- Management oversight
- External regulations and supervision
- Human Resources’ policies and practices
- FCR
- Internal Audit

EY’s tests of the control environment, risk assessment, monitoring, and information and communication included the following procedures to the extent they considered necessary:

- Inquiries concerning the Company’s organizational structure, including segregation of duties, policy statements, accounting and processing manuals, personnel policies, and the Internal Audit and Compliance Departments’ policies, procedures and reports
- Inspections, observations and re-performances with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to, and applying internal controls
- Inspections of control testing exceptions identified by management to determine their impact to the Company’s control environment
- Observations of personnel in the performance of their assigned duties
- Inquiries of the Company’s actions taken in response to recommendations to improve internal controls made by Internal Audit or FCR
The results of EY’s tests of the control environment, risk assessment, monitoring, and information and communication controls did not identify any relevant deviations, and they considered them in determining the nature, timing and extent of EY’s testing.

TESTING PERFORMED AND RESULTS OF TESTS WHEN USING THE WORK OF MANAGEMENT

In performing their examination of the Description, EY has used the work of FCR to assist in determining whether the controls related to the control objectives stated in the Description were operating with sufficient effectiveness to provide reasonable assurance that those control objectives were achieved throughout the period October 1, 2015 to September 30, 2016. EY performed independent walkthroughs of all controls. EY used the work of FCR for testing of certain controls in each the following process areas:

- Logical Access
- Change Management
- Physical Security
- Job Processing
- Data Backups

The nature of the testing performed by FCR related to controls over routine process activities, and included inquiry of relevant parties who performed the control activities, observation of the performance of the control activities at different times during the examination period, inspection of samples of documents evidencing the functioning of controls, and re-performance of the operation of certain controls. Any deviations identified by FCR are included under the Results of Testing for each control objective.

In connection with using the work of FCR, EY obtained the work papers supporting the tests performed and reviewed the work papers to evaluate whether the work was: (1) performed by a person having the appropriate skill and expertise, (2) properly supervised, reviewed and documented, (3) supported by sufficient, appropriate evidence to draw reasonable conclusions that were appropriate in the circumstances and consistent with the work performed, and (4) any exceptions or unusual matters were appropriately resolved. In addition, EY: (1) re-performed all samples selected for testing, and (2) inspected the supporting documentation for all other tests to evaluate the consistency of the working papers to the supporting documentation. No deviations were noted as a result of these procedures.

TESTING OF INFORMATION PRODUCED BY THE ENTITY

For tests of controls requiring the use of information produced by the entity (e.g., controls requiring system-generated populations for sample-based testing), we perform a combination of the following procedures where possible based on the nature of the information produced by the entity to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspected the source of the information produced by the entity, (2) inspected the query, script, or parameters used to generate the information produced by the entity, (3) tied data between the information produced by the entity and the source, and/or (4) inspected the information produced by the entity for anomalous gaps in sequence or timing to determine the data is complete and accurate.
INFORMATION TECHNOLOGY GENERAL CONTROLS

Control Objective 1: Logical Access

Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to (1) support properly authorized processing of transactions and data relevant to user entities’ financial reporting, (2) support the segregation of duties, and (3) protect applications and data from unauthorized modification, to support user entities’ internal control over financial reporting.

<table>
<thead>
<tr>
<th>Description of Controls Provided by the Company</th>
<th>Tests of Operating Effectiveness Performed by EY</th>
<th>Results of Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 IT Risk Policies and Standards outline controls for logical access. These standards document the policies and procedures for application, database and network access control, such as those pertaining to password configuration parameters and log-on attempt limitations.</td>
<td>Inspected the IT Risk Policies and Standards to determine whether they outlined controls for logical access and included policies and procedures for application, database, network and the mainframe access control, such as those pertaining to password configuration parameters and log-on attempt limitations.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>Description of Controls Provided by the Company</td>
<td>Tests of Operating Effectiveness Performed by EY</td>
<td>Results of Tests</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>1.2 Network and Mainframe:</strong></td>
<td>Network and Mainframe:</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>The password requirement standard is enforced via configuration settings documented in the policies. Any change to the password policies that would make the password requirements no longer compliant with the company standards would require approval via the change management process.</td>
<td>Inspected the network and the mainframe level password settings to determine whether it is enforced via the configuration settings as documented in the policies.</td>
<td></td>
</tr>
<tr>
<td>Application:</td>
<td>Inspected the password policies to determine whether approval via the change management process was obtained for instances where a change made to the password requirements rendered the password settings no longer compliant with the company standards.</td>
<td></td>
</tr>
<tr>
<td>Prior to or concurrent with application implementation in production, and on a periodic cycle based on risk thereafter, IT Asset Custodians approve completed Application Operational Security Guidelines (AOSGs) or Security Control Assessments (SCAs), confirming in-scope applications comply with password parameters.</td>
<td>Application:</td>
<td></td>
</tr>
<tr>
<td>For new applications, inspected the Application Operational Security Guidelines (AOSGs) or Security Control Assessments (SCAs), to determine whether they were approved by the IT Asset Custodians to confirm in-scope applications comply with password parameters prior to or concurrent with application implementation in production.</td>
<td>For existing applications, inspected a sample of Application Operational Security Guidelines (AOSGs) or Security Control Assessments (SCAs), to determine whether they were approved by the IT Asset Custodians to confirm in-scope applications comply with password parameters on a periodic cycle based on risk.</td>
<td></td>
</tr>
<tr>
<td>Inspected password configuration settings for each application to determine whether application password configuration settings are appropriate.</td>
<td>Inspected password configuration settings for each application to determine whether application password configuration settings are appropriate.</td>
<td></td>
</tr>
<tr>
<td>Description of Controls Provided by the Company</td>
<td>Tests of Operating Effectiveness Performed by EY</td>
<td>Results of Tests</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>1.3</td>
<td>Inspected the access request forms for a sample of new users (both non-privileged and privileged) to determine whether access was granted to IT assets upon receipt of approval by Voya asset owners/managers or their delegate.</td>
<td>Deviation noted</td>
</tr>
<tr>
<td></td>
<td>Inspected the access requests forms and access listings for a sample of new users to determine whether access requested was same as access provisioned.</td>
<td>With regards to the test of access granted to new users, inappropriate access was granted to the ACES application for one new user out of the sample of 49 users who were provisioned access during the period.</td>
</tr>
<tr>
<td></td>
<td>Inspected the access granted for a sample of new users to determine whether access granted was commensurate with users job responsibilities.</td>
<td>Management Response:</td>
</tr>
<tr>
<td></td>
<td>Inspected the listing of individuals with ability to approve access to IT assets to determine whether the ability to approve access is restricted to authorized individuals based on job responsibilities.</td>
<td>Although the control was performed as expected IT operations requested the inappropriate group when attempting to reinstate access to the user whose permissions had been revoked by mistake. The access has subsequently been revoked. Other information technology mitigating controls (such as the semi-annual reviews, and de-provisioning controls) are in place to ensure that the access could not be used inappropriately.</td>
</tr>
<tr>
<td></td>
<td>Deviation noted</td>
<td>No further deviations noted.</td>
</tr>
<tr>
<td>1.4</td>
<td>Inspected the configuration settings for the HR system to determine whether upon termination, the HR system automatically sent a feed to the OIM tool to automatically disable terminated user access to the network domains within 24 hours.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td></td>
<td>Inspected configuration settings for the OIM tool to determine whether the tool has been configured to automatically disable terminated users access to the network domains within 24 hours of receipt of the daily HR system termination feed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inspected the access lists for users with access to the administrative function within the OIM tool to determine whether access to change the OIM configurations was limited to appropriate personnel, based on their job responsibilities.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inspected a sample of terminated employees and reviewed network domain listings to determine whether access was appropriately revoked to the network domains within 24 hours.</td>
<td></td>
</tr>
</tbody>
</table>
### Description of Controls Provided by the Company

| 1.5 | Semi-annually, managers or their delegate review to certify or revoke access (both non-privileged and privileged) to IT assets, to ensure the level of access/role remains commensurate with job responsibilities. |

### Tests of Operating Effectiveness Performed by EY

- Inspected the semi-annual access reviews (both non-privileged and privileged) to determine whether a semi-annual access review was performed by managers/delegates to ensure the level of access remains commensurate with job responsibilities.
- Re-performed the review for a sample of account confirmations to determine whether user was a current employee, and whether access was appropriate based on the users job responsibilities.
- Inspected access listings for all users with privileged access to network domains and the mainframe to determine whether access was commensurate with job responsibilities.

### Results of Tests

**Deviations noted**

While performing completeness and accuracy testing of the report used by management to perform semi-annual periodic access reviews, we noted two instances where certain privileged and non-privileged accesses were not included in the review. The two instances included privileged access to a tool that supports access and domain users. The entitlements initially excluded were less than 3% of the total population of all entitlements subject to review. All the users that were initially excluded from the review were subsequently reviewed without deviation.

1) During the period we noted that 33 out of the total population of 116 entitlements within one of the privileged tools that monitors access to the AdminStation, PSRConnect, PWeb, and PLUS applications were not included in the first semi-annual review performed in 2016.

**Management Response:**

Management’s efforts to create a source file to feed the access review system resulted in errors of missing user IDs and incorrect mapping of IDs to policies and subrules. As a result, reliance was placed on the Active Directory access review which resulted in some access not being reviewed. Upon identification, missing IDs were reviewed by management without exception.
Description of Controls Provided by the Company | Tests of Operating Effectiveness Performed by EY | Results of Tests
--- | --- | ---

2) During the period we noted that 302 out of the total population of 8644 entitlements with privileged and non-privileged access to in-scope applications were not included in the semi-annual review. The Admin Station, PSRConnect, and Share Recon applications were impacted. Additionally, 16 out of the total population of 3350 entitlements with privileged access to one of the network domains were not included in the semi-annual review.

**Management Response:**

Management is aware that several factors resulted in missing entitlements in the semi-annual review. Due to limitations with reporting, some cross domain access was excluded from the review process due to limitations with reporting. Additionally, the timing of the source file creation in conjunction with migration efforts resulted in several users being excluded from the access review process. Finally, management determined that an abnormal termination of the script used to create the Common Domain source file resulted in the missing entitlements. In this case, the change in file record count fell within acceptable limits as defined by management, and as such, the abnormal termination of the ACL script was not flagged for further research at the time. The parameters were set taking into account changes occurring within the environment. Users were subsequently reviewed and exceptions were not noted.

No further deviations noted.
<table>
<thead>
<tr>
<th>Description of Controls Provided by the Company</th>
<th>Tests of Operating Effectiveness Performed by EY</th>
<th>Results of Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.6 Subsequent to the entitlement review process, access is disabled by the assigned team based on the revoke requested by the manager or delegate.</td>
<td>Inspected access rights for a sample of request for changes identified as part of the entitlement reviews and compared to active listings to determine whether requested modifications were made by the assigned team based on the request by the manager or delegate.</td>
<td>No deviations noted.</td>
</tr>
</tbody>
</table>
### Description of Controls Provided by the Company

1.7 Managers review and confirm usage of privileged accounts by developers in production is appropriate.

<table>
<thead>
<tr>
<th>Description of Controls Provided by the Company</th>
<th>Tests of Operating Effectiveness Performed by EY</th>
<th>Results of Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managers review and confirm usage of privileged accounts by developers in production is appropriate.</td>
<td>Inspected logs for a sample of usages to determine whether privileged account usages by developers in production were logged and reviewed by management. Inspected the log reviews for a sample of usages performed by management to determine whether unauthorized usages were identified, investigated and resolved. Inspected the names and titles of the individuals who accessed the production logs for a sample of dates to determine whether access was granted to authorized personnel based on job function. Inspected the names and titles of the managers who approved the access to determine whether usage was reviewed and approved by appropriate managers.</td>
<td>Deviation noted In a sample of 35 privileged usages to OmniPlus and PLUS applications for the period October 1, 2015 to June 30, 2016, we noted eight instances where usages were logged but not reviewed by the manager. Access and usage for those eight instances was later reviewed by management and determined to be appropriate. Subsequent to remediation referred to in management’s response that occurred in June 2016, we tested 100% of usages from July 1, 2016 through September 30, 2016 and noted all usages had been reviewed by the manager. Management Response: Managers completed a subsequent review that confirmed no inappropriate usage had occurred for the eight instances identified, and verified access was appropriate for the eight instances of usage. One of the usages was excluded from the review process due to the fact that the user was not correctly identified as a developer. Of the remaining seven items, four of the usages were initially routed incorrectly during the review process (an issue that was fixed in June), and the remaining three usages were appropriately routed and escalated, but management did not complete their review timely. Subsequent review by management of all usages from October through June indicated no inappropriate usages. No further deviations noted.</td>
</tr>
</tbody>
</table>
### Description of Controls Provided by the Company

#### 1.8
Firewalls are used to limit ports available to external users and to limit access to internal computing resources.

- **Tests of Operating Effectiveness Performed by EY**
  - Inspected network diagrams for the LAN/WAN and inquired of IT management to determine whether the network was configured to restrict unauthorized external access through the placement of firewalls at the network perimeter access points.
  - Inspected firewall configurations for a sample of firewalls placed at network perimeter access points to determine whether firewalls were configured to limit access to internal computing resources.

- **Results of Tests**
  - No deviations noted.

#### 1.9
Only network management personnel, based on their job responsibilities, have administrator access to firewalls.

- **Tests of Operating Effectiveness Performed by EY**
  - Inspected the access lists for all users with the ability to perform firewall system administration, to determine whether only network management personnel, based on their job responsibilities, had administrator access.

- **Results of Tests**
  - No deviations noted.

#### 1.10
An IPS/IDS tool is used to monitor, identify, and block potential unauthorized access on the network. It is configured to generate alarms based on unusual network activity. Network support and information security personnel monitor and act upon alarms.

- **Tests of Operating Effectiveness Performed by EY**
  - Inspected the IPS/IDS tool configuration settings to determine whether the tool has been configured to monitor, identify, and block potential unauthorized access on the network, and whether the tool is configured to generate alarms based on unusual network activity.
  - Inquired of IT management to determine whether network support and information security personnel monitored and acted upon alarms generated by the IPS/IDS tool.
  - Inspected a sample of ServiceNow tickets to determine whether network support and information security personnel monitored and acted upon alarms generated by the IPS/IDS tool.

- **Results of Tests**
  - No deviations noted.
### Control Objective 2: Change Management

Controls provide reasonable assurance that changes to application programs and related data management systems are authorized, tested, documented and approved prior to implementation into the production environment to (1) result in complete and accurate processing and data, (2) provide for the functioning of application controls and (3) support segregation of duties.

<table>
<thead>
<tr>
<th>Description of Controls Provided by the Company</th>
<th>Tests of Operating Effectiveness Performed by EY</th>
<th>Results of Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 IT Risk Policies and Standards outline controls for change management. These standards document the policies and procedures for application, database, network and mainframe change control, such as those pertaining to testing, approval, and migration of changes to production. Annually, the IT Risk Policies are reviewed by the Voya Financial Risk Committee or its delegate. Any amendment to these policies requires review and approval from either the Voya Financial Board or its delegate. The Control Standards Approval Board approves new IT Control Standards.</td>
<td>Inspected the IT Risk policies and standards to determine whether they include policies and procedures for application, database and network change control, such as those pertaining to testing, approval, and migration of changes to production. Inspected the IT Risk policies and standards to determine whether they were annually reviewed by the Voya Financial Risk Committee or its delegate. Inspected the IT Risk Policies to determine whether amendments to the policies were reviewed and approved by Voya Financial Board or its delegate. Inspected a sample of new IT Control Standards to determine whether the standards were approved by the Control Standards Approval Board.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>2.2 Development, testing, and acceptance environments are separate from the production environment.</td>
<td>Inquired of management to determine whether separate servers are utilized for development, test, and production for each application. Inspected screen prints of the development, test, and production servers to determine whether separate environments exist for development, test, and production.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>2.3 For infrastructure and application changes, the appropriate Owner or Custodian approves all changes to production (excluding Emergency changes).</td>
<td>Inspected change documentation for a sample of infrastructure and application changes to determine whether the appropriate Owner or Custodian approved the changes prior to migration to production.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>Description of Controls Provided by the Company</td>
<td>Tests of Operating Effectiveness Performed by EY</td>
<td>Results of Tests</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 2.4 Planned changes are accompanied by an approved test plan that documents testing results to support the required approval to move to production. | Inspected documentation for a sample of infrastructure and application changes to determine whether testing was performed, and signed off on prior to migration to production.  
Inspected documentation for a sample of infrastructure and application changes to determine whether test documentation exists, and includes items tested as well as results of testing. | No deviations noted. |
| 2.5 Prior to migration to production, changes are reviewed and approved weekly by the Change Approval Board (CAB). | Inspected change documentation for a sample of infrastructure and application changes to determine whether the CAB reviewed and approved the change prior to migration to production. | No deviations noted. |
| 2.6 Subsequent to development and testing, the designated migration team, who is independent of the developer, deploys code into production through the approved managed ID process. | Inspected the list of all users with access to production source code, to determine whether access was restricted to authorized personnel, based on job responsibilities and whether segregation of duties exists between the developer and migrators of changes to production.  
Inspected the change documentation for a sample of changes to determine whether the individual who developed the change did not migrate the code change into production. | Deviation noted |

As part of our inspection of all users with access to production source code, we noted that three users of the Fund Ops Accounting application out of the total population of 283 could modify code and approve code migration to production representing a segregation of duties violation across the Fund Ops Accounting application throughout the period.

Management Response:
Of the three users who were identified with the ability to both develop and migrate code to production, two were fulfilled in error and one was approved in error. All of the access has subsequently been removed and no inappropriate usage was identified. Management has reached out to the responsible parties to ensure they understand and follow the documented process. In addition, management continues to research options within the request tool to ensure access is not fulfilled in error when approvals are not obtained.
<table>
<thead>
<tr>
<th>Description of Controls Provided by the Company</th>
<th>Tests of Operating Effectiveness Performed by EY</th>
<th>Results of Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests for emergency changes to applications are documented and approved by the responsible Voya change owner. Approvals are documented in the incident ticket and added to a change ticket, which must be created and closed within one business day of the emergency change.</td>
<td>Inspected the change approvals for a sample of emergency changes to determine whether the approvals were documented in the incident ticket and added to the change ticket upon creation. Inspected documentation for a sample of emergency changes to determine whether a ticket was created and closed within one business day of the emergency change.</td>
<td>No deviations noted.</td>
</tr>
</tbody>
</table>
Control Objective 3: Physical Access

Controls provide reasonable assurance that physical access to data centers is restricted to authorized individuals.

<table>
<thead>
<tr>
<th>Description of Controls Provided by the Company</th>
<th>Tests of Operating Effectiveness Performed by EY</th>
<th>Results of Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Voya Minneapolis, MN and Jacksonville, FL Data Centers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1 IT Risk Policies and Standards outline controls for physical security. These standards document the policies and procedures for physical data center access. Annually, the IT Risk Policies are reviewed by the Voya Financial Risk Committee or its delegate. Any amendment to these policies requires review and approval from either the Voya Financial Board or its delegate. The Control Standards Approval Board approves new IT Control Standards.</td>
<td>Inspected the IT Risk Policies and Standards to determine whether they outline controls for physical data center access. Inspected the IT Risk policies to determine whether they were annually reviewed by the Voya Financial Risk Committee or its delegate. Inspected a sample of policies to determine whether amendments to the policies were reviewed and approved by Voya Financial Board or its delegate. Inspected a sample of new IT Controls Standards to determine whether they were approved by the Control Standards Approval Board.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>3.2 Access through all entry and exit points to the Voya data centers is restricted through the use of a card access control system.</td>
<td>Observed all entry and exit points to the Minneapolis and Jacksonville data centers to determine whether access was restricted through the use of a card access control system. Observed employees using card access control devices to determine whether access control devices were operating.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>3.3 Access to card access applications is restricted to Facility Access Coordinators based on their job responsibilities. Only Facility Access Coordinators, may make changes to the user access levels.</td>
<td>Inspected the system generated listing of all users with card access application access and inquired of IT management to determine whether access to the card access application was limited only to Facility Access Coordinators based on their job responsibilities.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>Description of Controls Provided by the Company</td>
<td>Tests of Operating Effectiveness Performed by EY</td>
<td>Results of Tests</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>3.4</strong> The IT Infrastructure Director or the Data Center Service Team approves access to the data centers commensurate with job responsibilities.</td>
<td>Inspected documentation for a sample of new access granted to the data center to determine whether the requests were approved by the IT Infrastructure Director or the Data Center Service Team. Inspected documentation for a sample of new access requests to the data center to determine whether access was appropriate based on the access request form and the user’s job function.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td><strong>3.5</strong> Semi-annually, managers review and validate system generated access lists for the data centers to ensure the level of access/role remains commensurate with job responsibilities.</td>
<td>Inspected a sample of data center access reviews to determine whether a semi-annual review was performed by managers to verify that only active personnel have appropriate access to data centers, and level of access/role remains commensurate with job responsibilities. Reperformed the review for a sample of account confirmations to determine whether access was appropriate based on the user’s job responsibilities. Inspected access rights for a sample of requests for changes identified as part of the data center access reviews and compared to active listings to determine whether requested modifications were made.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>Description of Controls Provided by the Company</td>
<td>Tests of Operating Effectiveness Performed by EY</td>
<td>Results of Tests</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>IBM Data Center (Boulder, CO)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.6 IBM’s access to controlled areas is restricted to authorized personnel only and requires documented approval from management. All individuals without authorized access to the controlled areas must sign in and be escorted by an individual with approved controlled area access.</td>
<td>Inspected documentation for a sample of new access granted to IBM’s controlled areas to determine whether access was approved by management. Inspected documentation for a sample of new access requests to IBM’s controlled areas to determine whether access was appropriate based on the access request form and the user’s job function. Observed individuals without authorized access to the controlled areas sign in to a log sheet, and be escorted by an individual with approved controlled area access.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>3.7 IBM’s levels of access rights to controlled areas are fully revalidated on an annual basis. An annual revalidation is performed to determine that a business need for access still exists.</td>
<td>Inspected the annual controlled areas access review to determine whether an annual review was performed to revalidate access. Reperformed the review for a sample of account confirmations to determine whether access was appropriate based on the user’s job function. Inspected access rights for a sample of request for changes identified as part of the data center access reviews and compared to active listings to determine whether requested modifications were made.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>3.8 For controlled areas that have emergency exits, exits have audible alarms and are monitored by security personnel. Periodic verification that the alarms are functioning are performed, documented and retained.</td>
<td>Observed an individual attempt to exit a controlled area using an emergency exit to determine whether an audible alarm was triggered and responded to by security personnel. Inquired of management to determine whether periodic verification that the alarms are functioning are performed, documented and retained.</td>
<td>No deviations noted.</td>
</tr>
</tbody>
</table>
Control Objective 4: Job Processing

Controls provide reasonable assurance that application and system processing are authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner.

<table>
<thead>
<tr>
<th>Description of Controls Provided by the Company</th>
<th>Tests of Operating Effectiveness Performed by EY</th>
<th>Results of Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 IT Risk Policies and Standards outline controls for Job Processing. These standards document the policies and procedures for job scheduling processes and tools. Anually, the IT Risk Policies are reviewed by the Voya Financial Risk Committee or its delegate. Any amendment to these policies requires review and approval from either the Voya Financial Board or its delegate. The Control Standards Approval Board approves new IT Control Standards.</td>
<td>Inspected the IT Risk Policies and Standards to determine whether they outlined controls for Job Scheduling processes and tools. Inspected the IT Risk policies to determine whether they were annually reviewed by the Voya Financial Risk Committee or its delegate. Inspected a sample of policies to determine whether amendments to the policies were reviewed and approved by Voya Financial Board or its delegate. Inspected a sample of new IT Controls Standards to determine whether they were approved by the Control Standards Approval Board.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>4.2 IT Infrastructure Director or Production Control Managers approve requests for access to scheduling tools, based on the user's job responsibilities and as documented in the ServiceNow ticket.</td>
<td>Inspected the access request forms for a sample of new users with access to scheduling tools to determine whether access was approved by the IT Infrastructure Director or Production Control Managers in a ServiceNow ticket. Inspected the access requests forms and job scheduling application access listings for a sample of new users to determine whether access requested was the same as access provisioned. Inspected the access granted for a sample of new users to determine whether access granted is commensurate with job functions.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>4.3 Semi-annually, managers or their delegate review to certify or revoke access (both non-privileged and privileged) to IT assets, to ensure the level of access/role remains commensurate with job responsibilities.</td>
<td>Refer to 1.5 above for test procedures.</td>
<td>Refer to 1.5 above for results of testing.</td>
</tr>
<tr>
<td>Description of Controls Provided by the Company</td>
<td>Tests of Operating Effectiveness Performed by EY</td>
<td>Results of Tests</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>4.4 Subsequent to the entitlement review process, access is disabled by the assigned team based on the revoke requested by the manager or delegate</td>
<td>Refer to 1.6 above for test procedures.</td>
<td>Refer to 1.6 above for results of tests.</td>
</tr>
<tr>
<td>4.5 The Technology Services Distributed Scheduling Team creates or changes job schedules as requested in the approved change request.</td>
<td>Inquired of management to determine whether the Technology Services Distributed Scheduling Team creates or changes job schedules as requested in the approved change request. &lt;br&gt;Inspected documentation for a sample of changes to jobs or job schedules to determine whether the Technology Services Distributed Scheduling Team creates or changes job schedules as requested in the approved change request.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>4.6 In the event that a job terminates abnormally, the Voya or IBM application or infrastructure support team resolves the job failure and documents the resolution action in the ServiceNow ticket.</td>
<td>Observed a Computer Operator create a job and force the job to abend intentionally, to determine whether a ServiceNow ticket was automatically generated. &lt;br&gt;Inspected the job monitoring console for each in-scope application to determine whether the monitoring console displayed the status for each job, and in the event that a job terminated abnormally, error notifications were displayed on the job monitoring console. &lt;br&gt;Inspected a sample of ServiceNow tickets to determine whether job failures were investigated, resolved and documented within the ticket.</td>
<td>No deviations noted.</td>
</tr>
</tbody>
</table>
Control Objective 5: Data Backups

Controls provide reasonable assurance that data and programs are backed up and available for restoration.

<table>
<thead>
<tr>
<th>Description of Controls Provided by the Company</th>
<th>Tests of Operating Effectiveness Performed by EY</th>
<th>Results of Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1  IT Risk Policies and Standards outline controls for File Backups. These standards document the policies and procedures for data backup and restoration. Annually, the IT Risk Policies are reviewed by the Voya Financial Risk Committee or its delegate. Any amendment to these policies requires review and approval from either the Voya Financial Board or its delegate. The Control Standards Approval Board approves new IT Control Standards.</td>
<td>Inspected the IT Risks policies and standards to determine whether they outlined controls for File Backups. Inspected the IT Risk Policies and Standards to determine whether they were reviewed annually by the Voya Financial Risk Committee or its delegate. Inspected a sample of policies to determine whether amendments to the policies were reviewed and approved by Voya Financial Board or its delegate. Inspected a sample of new IT Controls Standards to determine whether they were approved by the Control Standards Approval Board.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>5.2  Voya application owners ensure that critical ACES data is backed up by IBM specifying the frequency of backups via a backup schedule. These specifications are implemented using Job Control Language.</td>
<td>Observed lists of critical application data sets and the backup frequency requirements to determine whether specifications were documented by application owners, and implemented using Job Control Language. Inspected the backup schedule for a sample of critical application datasets within the mainframe environment to determine whether critical files and data specifications were included.</td>
<td>No deviations noted.</td>
</tr>
<tr>
<td>5.3  For Voya-hosted applications, backups are executed according to business requirements and stored securely.</td>
<td>Inspected all backup configuration settings for the applications to determine whether backups were executed according to the business requirements and stored securely.</td>
<td>No deviations noted.</td>
</tr>
</tbody>
</table>
For applications that reside in the Minneapolis, MN and Jacksonville, FL data centers, data is replicated between the two data centers through a synchronization job. In the event a data synchronization job terminates abnormally during replication between systems, error notifications are automatically generated. IT operations personnel follow-up on error notifications and resolve the issues.

<table>
<thead>
<tr>
<th>Description of Controls Provided by the Company</th>
<th>Tests of Operating Effectiveness Performed by EY</th>
<th>Results of Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4</td>
<td>Inspected configuration settings for all systems to determine whether data is being replicated in two separate Voya physical locations through a data synchronization job. Inspected configuration settings for all systems to determine whether data synchronization jobs were configured to generate error notifications and whether the error notifications were sent to notify operators of errors when a data synchronization job completed abnormally. Inspected a sample of ServiceNow tickets to determine whether job failures were investigated, resolved and documented within the ticket.</td>
<td>No deviations noted.</td>
</tr>
</tbody>
</table>