Nationwide Financial Services, Inc.

Retirement Solutions Governmental and Institutional Business

Nationwide Financial Services, Inc.'s System Relevant to Security and Availability of its Nationwide Retirement Solution's Governmental & Institutional Business System

Throughout the period January 1, 2023 to December 31, 2023

SOC 2® Report on Controls Placed in Operation and Tests of Operating Effectiveness

kpmg.com

Nationwide Financial Services, Inc.
Retirement Solutions Governmental and Institutional Business

Report on Nationwide Financial Services, Inc.'s Description of its Nationwide Retirement Solution's Governmental & Institutional Business System and on the Suitability of the Design and Operating Effectiveness of its Controls Relevant to Security and Availability

SOC 2 Type II Report
For the Period January 1, 2023 through December 31, 2023

Table of Contents

Section I.

Independent Service Auditors' Report Provided by KPMG LLP

KPMG LLP
Suite 500
191 West Nationwide Blvd.
Columbus, OH 43215-2568

Independent Service Auditors' Report

Board of Directors of Nationwide Mutual Insurance Company and its Nationwide Financial Services, Inc.:

Scope

We have examined management of Nationwide Financial Services, Inc. (Nationwide)'s accompanying description of its system titled "Management of Nationwide Financial Services, Inc.'s Description of Its Nationwide Retirement Solution's Governmental & Institutional Business System" throughout the period January 1, 2023 to December 31, 2023 (the Description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria* (the Description Criteria), and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period January 1, 2023 to December 31, 2023 to provide reasonable assurance that Nationwide's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Nationwide uses the subservice organizations identified in Section III to perform some of the services provided to user entities. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nationwide, to achieve Nationwide's service commitments and system requirements based on the applicable trust services criteria. The Description presents Nationwide's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Nationwide's controls. The Description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization(s), and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

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

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of the design and operating effectiveness of the controls stated in the Description based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the Description is presented in accordance with the Description Criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were

achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

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

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

Inherent Limitations

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

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

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

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects,

- the Description presents Nationwide's Retirement Solution's Governmental & Institutional Business System that was designed and implemented throughout the period January 1, 2023 to December 31, 2023 in accordance with the Description Criteria

- the controls stated in the Description were suitably designed throughout the period January 1, 2023 to December 31, 2023 to provide reasonable assurance that Nationwide's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period, and subservice organizations applied the complementary controls assumed in the design of Nationwide's controls throughout the period January 1, 2023 to December 31, 2023

- the controls stated in the Description operated effectively throughout the period January 1, 2023 to December 31, 2023 to provide reasonable assurance that Nationwide's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls, assumed in the design of Nationwide's controls, operated effectively throughout the period January 1, 2023 to December 31, 2023.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Nationwide, user entities of Nationwide's Retirement Solution's Governmental & Institutional Business System during some or all of the period January 1, 2023 to December 31, 2023, business partners of Nationwide that were subject to risks arising from interactions with Nationwide's Retirement Solution's Governmental & Institutional Business system, and practitioners providing services to such user entities and business partners, who have sufficient knowledge and understanding of the following:

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

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

KPMG LLP

Columbus, Ohio
April 26, 2024

Section II.

Management of Nationwide Financial Services, Inc.'s Assertion

Management of Nationwide Financial Services, Inc.'s Assertion

We have prepared the accompanying description of Nationwide Financial Services, Inc. (Nationwide)'s system titled "Management of Nationwide Financial Services Inc.'s Description of Its Nationwide Retirement Solution's Governmental & Institutional Business System" throughout the period January 1, 2023 to December 31, 2023 (the Description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria*) (the Description Criteria). The Description is intended to provide report users with information about the Nationwide Retirement Solutions Governmental & Institutional Business System that may be useful when assessing the risks arising from interactions with Nationwide's system, particularly information about system controls that Nationwide has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Nationwide uses subservice organizations to perform some of the services provided to user entities. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nationwide, to achieve Nationwide's service commitments and system requirements based on the applicable trust services criteria. The Description presents Nationwide's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Nationwide's controls. The Description does not disclose the actual controls at the subservice organizations.

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

a. The Description presents Nationwide's Retirement Solutions Governmental & Institutional Business System that was designed and implemented throughout the period January 1, 2023 to December 31, 2023, in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed throughout the period January 1, 2023 to December 31, 2023 to provide reasonable assurance that Nationwide's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and subservice organizations applied the complementary controls assumed in the design of Nationwide's controls throughout the period January 1, 2023 to December 31, 2023.

c. The controls stated in the Description operated effectively throughout the period January 1, 2023 to December 31, 2023 to provide reasonable assurance that Nationwide's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Nationwide's controls, operated effectively throughout the period January 1, 2023 to December 31, 2023.

Roger Green

Roger Green
AVP, Retirement Solutions – Finance
April 26, 2024

Michael Carrel

Michael Carrel
SVP, Chief Technology Officer, Nationwide Financial Technology
April 26, 2024

Section III.

Management of Nationwide Financial Services, Inc.'s Description of Its Nationwide Retirement Solution's Governmental & Institutional Business System

Overview of Company and Services

Business Overview and Services

Nationwide Financial Services, Inc. (Nationwide) or (NFS) provides a breadth of services and includes several companies focusing on domestic property and casualty insurance, life insurance and retirement savings, asset management, and strategic investments.

Certain retirement plan operations of NFS are provided by Nationwide Retirement Solutions, Inc. (NRS), Retirement Solutions Government, and Institutional Business (RSGIB), in coordination with its custodial affiliates Nationwide Life Insurance Company (NLIC) and Nationwide Trust Company, FSB (NTC). NRS, NLIC, and NTC are indirect wholly owned subsidiaries of NFS.

RSGIB offers a range of investment products and services to meet the retirement and savings needs of government entities and their employees and ERISA plans. The majority of plan participants contribute to employer-sponsored plans (including Internal Revenue Code Section 401, 403, and 457 plans), which allow the accumulation of retirement assets through pretax employee contributions. Contracts with plans are separated into two different levels of service based upon whether RSGIB handles the participant accounting. These levels of service are Full Service (plan and participant level records are maintained) and Unallocated Service (only plan level records are maintained). Professional money management is available to Full-Service contract plan participants through Nationwide ProAccount, a managed account service offered by Nationwide Investment Advisors, LLC, (NIA), a subsidiary of NFS. NIA utilizes the services of RIA Services, Inc., a subsidiary of NFS, to interface with the operations of RSGIB. This report has been prepared to provide information on RSGIB's RIA Services and ProAccount's controls, which may be relevant to internal control of both types of User Entities as well as both levels of service entered into by the plans.

Service Commitments and Requirements

Nationwide designs its processes and controls, related to RSGIB, to meet its products and services security and availability objectives. Those objectives are based on the service commitments that Nationwide makes to users for the related products and services.

Service commitments to users have been established and are principally documented and communicated in contracts and customer agreements as well as in descriptions of the service offerings. Underlying these service commitments are various system requirements that must be in place for the system to function in a way to meet the stated commitments.

Nationwide has evaluated the service commitments made in the delivery of their services, and in doing so has identified the following commitments that are key to the delivery of the services provided.

Security Commitments

- Nationwide has established security policies and procedures that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Nationwide has established an information security awareness and training program for all associates and contractors.
- Nationwide has established risk assessments over its information systems in order to identify potential threats to the systems and the environment in which it operates: determine the likelihood of the threats, identify and evaluate vulnerabilities, and determine the loss impact if one or more vulnerabilities are exploited by a potential threat.

- Nationwide performs periodic assessments to evaluate whether the controls implemented to mitigate security and availability risks are adequate and effective.
- Nationwide employs the use of encryption technologies to protect customer data both at rest and in transit.
- Nationwide has established a formal security event response policy and related procedures to identify, monitor, and report security incidents.
- Access and activity logging and monitoring is in place to support incident management.
- Nationwide has secure development and change management processes to implement authorized and tested changes to system components.
- Hardware and software used to support provided services are required to be at a currently supported version and have valid support service contracts with the vendor.
- Nationwide restricts physical access to facilities, and protected information assets are restricted to authorized personnel.
- Data Loss Prevention (DLP) solutions are used to scan for and limit sensitive information in outgoing transmissions, including email and instant messaging.
- Firewall configurations are used to allow/limit access to appropriate personnel, organizations, and services.
- Antivirus and antimalware detection tools are used to scan data, transmissions, and email in order to mitigate processing and service interruptions caused by viruses or malware.
- Distributed Denial of Service (DDoS) attack preventative software is in place, and a service-based solution is used to handle DDoS attacks.
- Nationwide has data retention and disposal policies and procedures for proper processing and secure maintenance, disposal, and destruction for Nationwide system hardware and sensitive data.

Availability Commitments

- Incident response support is provided 24 hours a day, 7 days a week (24x7), with committed response times based on severity of the problem.
- Nationwide designs and implements business continuity and disaster recovery plans and procedures (including pandemic) to meet the availability commitments of Nationwide's systems.
- Nationwide actively tests or reviews and updates its contingency plans and procedures on at least an annual basis.
- Nationwide's system uptime commitments are supported through application processing environment redundancy and geographic separation of data centers.

Components of the System

The components of the RSGIB system that support the services within the scope of this report are as follows and described in detail below:

- **Infrastructure** – The physical structures, IT, and other hardware (e.g., facilities, computers, equipment, mobile devices, and telecommunications networks)
- **Software** – IT system software that supports infrastructure support services programs (operating systems, middleware, and utilities)
- **People** – The associates involved in the governance, operation, and usage of a system (developers, operators, entity users, vendor personnel, and managers)
- **Procedures** – The automated and manual procedures used in operation of the system
- **Data** – Transaction streams, files, databases, tables, and output used or processed by the system

Infrastructure

Nationwide's data centers in Ohio provide the infrastructure supporting the systems included within this report. The in-scope servers and supporting processes reside within the corporate network domain, which is segmented from other Nationwide locations and data centers. The server environment includes Windows and Red Hat Linux. Red Hat Linux hosts the in-scope databases and applications. Windows consists of web servers running Windows operating system that are used to centrally manage the network domain, data loss prevention (DLP) tools, and antivirus software. The perimeter systems are protected from external threats (including other Nationwide locations outside the corporate network domain) by firewalls, intrusion prevention and detection systems, and threat intelligence software. This infrastructure is monitored by the Cyber Security Operations Center (CSOC). When Nationwide acquires new business units or service offerings, the acquired infrastructure is not connected to the corporate infrastructure until assessed by Information Risk Management (IRM) and determined to be compliant with secure configuration standards.

Software

The below applications support the various services Nationwide provides to its customers and are in scope for this report:

Internally Hosted	
Application	**Purpose**
Agent Information Management System (AIMS)	NF Centralized licensing and appointment information system for Agents, Brokers, Advisors and Firms.

Internally Hosted	
Application	**Purpose**
AWD 10 NF	Automated Workflow Distribution, an imaging and workflow application for the independent channel used by Retirement Solutions. AWD 10-NF (AWD) – is a vendor application owned by SS&C, licensed to Nationwide Financial, and being configured for use by Retirement Solutions for managing the workflow related to processing financial and non-financial transactions. AWD interfaces with DCdirect (RPLink), NF's record-keeping application for Retirement Solutions, and FileNet, via APIs. It produces and consumes Kafka events for messaging and alerting. Participant-facing applications, such as RSC (Task Center and Status Tracker), access AWD workflow information through APIs, as well.
DCDirect (RP Link)	A Java-based application allowing both online real-time and batch processing. DCdirect (RPLink) uses a batch flow to apply the majority of financial transactions. Nonfinancial and financial transactions, for which the price of the investment options is known, are processed real-time. Investment options include fixed and variable options provided by various financial institutions. Daily interfaces provide pricing information for the variable products while fixed pricing is calculated daily based on certain predetermined rate factors. DCdirect (RPLink) uses a combination of different online inquiry transactions to aid in customer's inquiries. Online update transactions are also available for plan level activity. DCdirect (RPLink) houses many accounts and processes large volumes of transactions while still meeting daily service level agreements. DCdirect (RPLink) interfaces with different systems to facilitate User Entity record keeping and provides daily reports, which support transaction activity.
Payment Management Transaction System (PMTS)	The Payments system is used for the processing of disbursements. These can be checks, Digital, or Wires. PMTS is responsible for creating, tracking, and reporting on all payments issued by the Nationwide Financial administration areas listed: Financial Operations, Commissions, Individual Investment Products, Nationwide Advisory Solutions, Nationwide Life, Nationwide Financial Network, Claims, Payouts, Pensions, and Public Sector Retirement Plans.

Externally Hosted		
Application	**Hoster**	**Purpose**
RIA Managed Accounts TMS (Public)	1/1/2023-8/25/2023 Tierpoint 8/26/2023-12/31/2023 Amazon Web Services (AWS)	TMS (Public) is an Oracle Reports and PL/SQL based application that provides omnibus level modeling and trade capability of portfolios of mutual funds, a fee calculating engine, and reporting. The application allows both online real-time and batch processing. TMS (Public) is used by Nationwide Investment Advisor ProAccount for managing 457 plans participant investments.
UV Cloud (UVC)	Zinnia	A variable product asset management and unit value pricing functionality platform. UVC calculates unit values and provides prices to Nationwide administration systems each business day. Additionally, UVC is an intermediary between Nationwide and National Securities Clearing House and is used to execute trade orders interfaced from the respective Nationwide administration systems. Also, UVC is utilized to reconcile shareholder account activity between fund houses, the G/L, and administration systems. Last, UVC calculates fund performance to report downstream to the various lines of business and provides funds of fund administration capability.
Retail Service Center (RSC)	Amazon Web Services (AWS)	RSC provides participants and plan sponsors with a variety of plan and individual participant level information, including balances and current investment allocations. The RSC allows input of participant enrollments, participant demographic changes and participant exchange and investment allocation change transactions.

People

Nationwide comprises enterprise-wide groups, as well as specific teams, who are involved in the operation of the RSGIB system. Nationwide has a staff of approximately 24,400 associates organized into the following functional areas.

Nationwide Technology

The Nationwide Technology organization, led by the Chief Technology Officer, is responsible for the hardware, network, and operating systems support and maintenance, as well as server and database access user provisioning.

Board of Directors

Nationwide's Board of Directors comprises members who are independent of management of Nationwide who are appointed to act on behalf of members (i.e., customers). The composition and competency of the Board of Directors is reviewed at least annually.

Nationwide's Board of Directors serves multiple functions, such as providing oversight of the strategic direction and performance of Nationwide and working with management to establish measurable financial and nonfinancial goals and performance criteria that address short-term and long-term objectives.

Nationwide's Board of Directors is also part of a layered and effective security governance structure. In support of the Board's commitment to security governance, Nationwide's Board of Directors has chartered several committees that serve in that capacity. Additionally, management has chartered several committees. Below are several of these key board and management committees (not comprehensive):

- Business Innovation and Transformation Committee (BIT-C) – Works with Nationwide Technology's risk management team to clarify and define strategy and budget goals and works throughout the year to review progress reports, ensuring alignment. They also are responsible for reviewing any updates/changes to those goals.
- Nationwide Audit Committee – Oversees the audit function of Nationwide Technology's risk management team, and specifically oversees audit items that rise to a "high" rating, ensuring remediation and tracking is in place.
- Chief Technology Officer Council – Supports Nationwide's Chief Technology Officer to help ensure IT risk commitments are implemented.
- Enterprise Operational Risk Management Committee (EORC) – Acts as a coordinating body for operational risk, overseeing management of operational risks, and promoting the alignment of operational risk management practices, language, and definitions across the enterprise. The following are subcommittees supporting the EORC:
    - Legal and Regulatory Risk Subcommittee – Manages legal and compliance risk at the enterprise level.
    - Data, Quality, Sufficiency, and Protection (DQSP) - Acts as the governing body for data-related risks, reducing the potential for adverse consequences from decisions based on the use, misuse, or inconsistent use of data
    - Third-Party Risk Committee (TPRC) – Acts as a coordinating body for the identification and management of risk posed by third parties. The TPRC promotes the alignment of third-party risk management practices, language, and definitions across the enterprise.
    - Technology Risk Committee – Helps ensure Nationwide's technology risk profile (including oversight for cybersecurity risk) is effectively managed holistically through proper governance, policies, established risk appetite, set tolerances, monitor key risk indicators, and aligned priorities for mitigating Nationwide's risk associated with Technology.

Information Risk Management

The IRM organization, led by the Chief Information Security Officer (CISO), seeks to integrate distributed security and associated risk management-related activities into the following functions:

- Business Continuity and Disaster Recovery (BC/DR)
- Identity and Access Management
- Third-Party Risk Management (TPIRM)
- Information Governance
- Information Security
- Risk and Compliance

Organization charts for the Nationwide Technology Risk Management organization are reviewed and updated at least annually to help ensure Nationwide's commitments and requirements as they relate to security and availability. In addition, roles and responsibilities for designing, developing, implementing,

operating, monitoring, and maintaining the system are defined within job descriptions, policies, and procedures.

Business Continuity and Disaster Recovery

Nationwide firmly believes in the value of pre-planning for business interruptions. In our effort serve both our internal and external customers, by providing continuous service operations, Nationwide has developed a comprehensive Continuity Management (Business Resiliency) program. Our program includes three disciplines: business recovery, system recovery, and crisis management. The Continuity Management Program resides in the Information Risk Management organization, under Nationwide Technology. They are responsible for ensuring compliance activities are completed, as well as governance, continuity improvement, and crisis management. Nationwide has a Crisis Management team in place to reduce enterprise-wide risk exposure by analyzing foreseeable risks and planning for potential events. Nationwide has an on-going relationship with federal, state, and local emergency management response organizations and regulatory agencies, many of which participate in our annual simulations.

Our recovery strategy and plans address individual business process, applications, and systems architectures throughout the organization. Nationwide plans for loss of a facility, loss of a datacenter, loss of staff, loss of a critical vendor and impact from cyber-attacks. Business functions and system applications have pre-assigned recovery windows to help ensure that resources are appropriately allocated. Recovery plans have been developed, are updated routinely, certified annually, and are required to perform either a walkthrough or validation test annually in accordance with our Contingency Planning Standard. To identify and prioritize processes and information systems that support Nationwide's critical business processes. Nationwide conducts a Business Impact Analysis every four years or when a core business process changes in a way that impacts the criticality of the process.

The Technology Risk Committee and the Enterprise Operational Risk Committee provide oversight over Nationwide Technology Resiliency and System Availability to minimize related business disruption and improve Nationwide Technology's resilience posture.

Third-Party Risk Management

Nationwide's TPIRM team is responsible for evaluating suppliers and conducting assessments/reassessments. TPIRM has an established guideline for the minimum-security control requirements for third-party organizations who store, process, handle, or exchange private, sensitive personal and restricted data as defined in the Nationwide Information Classification Standard. The third-party organizations shall implement these security controls (based on NIST SP 800-53) or have proper compensating controls in place. Nationwide TPIRM assesses third-party suppliers based on the TPIRM IT Security Guidelines. Each supplier is assigned a program priority based on a qualitative risk scoring methodology and is reassessed as outlined below:

Program Priority Rating	Assessment Frequency
High	Every year
Medium	Every Two Years
Low (CEV*or Regulatory/SOC 2**)	Every Three Years
Low	At contract renewal (if assessment is 3 or more years old)
Note: Any third-party can be re-assessed outside of the standard schedule if a security concern is identified as a result of scope changes or any other reason (e.g. access to sensitive NW data, new regulatory standard).	

Program Priority Rating	Assessment Frequency
*CEV: Critical External Vendor **Regulatory/SOC: Includes third parties that provide applications that are in scope for SEC, HIPPA, GLBA, and/or SOC 2	

Nationwide's TPIRM utilizes three Security Review Questionnaires (SRQ), which are all based on National Institute of Standards and Technology (NIST). Nationwide's SRQs are the Security Foundation Assessment, Security Infrastructure for Data Protection Assessment, and Security in the Cloud Assessment. Nationwide also requests evidence and conducts virtual reviews of documentation to support the assessment. The data protection SRQ includes, but is not limited to, the following topics:

- Access Control
- Awareness and Training
- Audit and Accountability
- Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identity and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environment Protection
- Planning
- Management Controls
- Risk Assessment
- System and Service Acquisition
- System and Communications Protection
- System and Information Integrity

Corporate

The Corporate functional area includes Nationwide executives, senior operations staff members, and Nationwide administrative support staff members, including risk management associates, non-IT project managers, and business planning associates. Finance, real estate, and client banking associates are included in the corporate organization, as well as associates in the areas of compliance, privacy, facilities, legal, training, client and vendor contracts, human resources, internal communications, and internal audit.

The Compliance and Regulatory team reports to the Office of the Chief Legal Officer and provides direction across Nationwide regarding privacy and confidentiality policies, procedures, and practices as they relate to the protection of client and Nationwide restricted information. The Office of Associate Relations is responsible for providing the ethical and behavioral policies and framework governing Nationwide associate activities. Nationwide is dedicated to creating, providing, and delivering instructional design and training for the organization. In support of that objective with respect to cybersecurity, Nationwide has developed the

"Protect Nationwide – Cybersecurity" awareness and training program. This program uses multiple mediums to influence and change habits:

Awareness and Training Activities

- Manage and promote a robust Intranet/SharePoint site with news and resources.
- Post timely cyber security news, such as changes to policies, current events, or general awareness on company Intranet site.
- Distribute timely cyber security communications to affected subgroups.
- Hold a virtual event across the enterprise during October Cyber Security Awareness month. Festivities include guidance, challenges, and keynote speakers.
- Require annual associate acknowledgement of Nationwide's Information Security Policy.
- Provide Computer-Based Training (CBT) courses on multiple topics directed to multiple audiences.
- Create and manage cybersecurity digital learning programs in the learning management system to assign, track, and report relevant data to achieve goals and compliance requirements.
- Partner with business units across the enterprise to consult on cybersecurity education impacting members and associates.

Phishing Education Program

- Administer 12 simulated phishing tests per year, which includes targeted tests to high-risk groups.
- Provide a Report Phishing button in Outlook so associates can report suspicious emails and give direct associate feedback on the type of emails they have reported (legitimate, spam, malicious, phishing tests).
- Provide immediate education when an associate fails a phishing test and assign training course when associates fail three or more tests at half year intervals, and if an associate falls victim to a real phishing email.
- Provides individual coaching to associates failing four or more tests at half year intervals.
- Send recognition award to associates when the pass all tests or pass and report all tests at half year intervals.
- Post a phishing email "Catch of the Week" on Yammer and publicly recognize the associate who reported it.

Computer-Based Training Offerings

Frequency	Audience	Course Name	Topics
Annual and Upon Hire	All Associates	Annual Cyber Security Training Course	Social engineering, data protection, physical and mobile security, passwords, access, secure data storage
Provided Upon Hire	All Contractors	Cyber Security for Contractors	Data protection, access control, social engineering, secure remote connection

Frequency	Audience	Course Name	Topics
Bi-annual	Associates who fail three phishing tests in a quarter; associates who fall victim to real phishing attack	All About Phishing	Definition, most common types, potential damage, methods of recognition and reporting
Provided Upon Entry to Role	All People Leaders	IdentityIQ for People Leaders	Importance of access management, how to use IdentityIQ tool to manage associate access
Provided Upon Entry to Role	All Application Developers	iSecure curriculum	Secure coding
Provided Upon Entry to Role	Associates with Privileged Access	Privileged Access: Practice Secure Behaviors	Risks, types of IDs, methods of secure access and use
Provided Upon Entry to Role	Associates with Cloud Accounts	Cloud Data Security at Nationwide	Privacy, access review, IT asset and cloud solution governance
Provided Upon Entry to Role	All Application Developers and Their Managers	Open-Source Software at Nationwide	Secure methods to use and contribute to open-source software
Provided Upon Entry to Role	Business Continuity Plan Owners and Planners	Contingency Planning at Nationwide	Explains the why and the how of contingency planning, including key roles and terms
Provided Upon Entry to Role	Business Continuity Plan Owners and Planners	AssuranceCM Quick Start Guide	Provides training on using the AssuranceCM tool for Contingency Planning
Provided Upon Entry to Role	Business Continuity Plan Owners and Planners	Walkthrough Exercise	Learn to plan, conduct, and report a walkthrough exercise of a contingency plan
Provided Upon Entry to Role	Enterprise Crisis Team Members	Enterprise Crisis Management	Provides training on Nationwide's enterprise crisis management program and the steps to take to respond to a crisis

Frequency	Audience	Course Name	Topics
Provided Upon Entry to Role	Enterprise Crisis Team Members	Facility Crisis Management	Details the people, process and resources used during a facility crisis event

Nationwide monitors compliance with training requirements via course completion tracking in the learning management system. This is actively monitored, and notifications are provided in the event of noncompliance to parties responsible for remediation.

Regulatory and legal claims management compliance is an essential component of the Nationwide solution. Nationwide's team of cross-functional, multilevel business unit subject matter experts includes experienced professionals in claims management compliance, antifraud, quality performance, and line of business practices all working together to actively monitor, assess, and apply the applicable claims administration requirements.

Information Technology:

Nationwide Technology is supported by the CISO and infrastructure organizations, encompassing Compliance, the CSOC, NT Infrastructure associates, and NT Help Desk associates. Nationwide's CISO reports to the Chief Technology Officer. Nationwide Technology also includes software developers, technical team leads, architects, supervisors, development managers, release coordinators, project managers, system analysts, and quality assurance testers.

The IRM team provides company-wide system and electronic device security policies and procedures covering significant aspects of Nationwide technology operations, including, but not limited to:

- Access Control
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Contingency Planning
- Data Protection
- Identification and Authentication
- Incident Response
- Planning
- Program Management
- Recovery and Resiliency
- Risk Assessment
- Secure Application Development
- Security Assessment and Authorization
- System and Communications Protection
- Third-party Risk Management.

In addition to the above standards maintained by IRM, Nationwide Corporate Real Estate maintains a standard governing physical and environmental security.

The Information Security Policy and NT standards are reviewed by management/subject matter experts at least annually. After the Information Security Policy is reviewed, it is approved by the Enterprise Operational Risk Committee (EORC). Once the standards are reviewed, they receive sign off from the IRM Standards Review Board (SRB). The Information Security Policy and technology security standards are published on Nationwide's intranet and are communicated to employees on a periodic basis. Nationwide requires that all associates and contractors read and attest to the Information Security Policy at onboarding and annually thereafter.

NT Governance associates provide direction, policies, procedures, and standards for software development change management. The NT Service Desk provides support for associates and clients, including password resets and defect reporting for supporting applications used in claims processing.

The Nationwide Application Development Support Team is a team of developers who provide support services for proprietary applications. The services include basic application functionality and support for applications not working properly (i.e., design defects). Application-level problems are recorded and tracked on a problem management system, escalated appropriately, and monitored through resolution.

Procedures

Nationwide maintains multiple types of application documentation. These can include design documents, context diagrams, and various in-code notations. Documentation is held within the application teams' SharePoint site, within GitHub repository, as well as made available in the Lucy Knowledge Management sharing tool. Documentation is reviewed and updated as part of the normal project development lifecycle process whenever necessary.

In addition, RSGIB maintains service and administration documentation such as procedures, job aids, and checklists that reference how Nationwide Retirement Solutions applications are utilized as part of day-to-day service and operations. These documents are housed within department share drives and reviewed and updated as changes are made or needed to procedures and applications.

RSGIB primarily uses Microsoft Outlook email, Microsoft Teams, and SharePoint to collaborate electronically. Multiple SharePoint pages have been created to record project work, including solution recommendations, project plans, research, statuses, and delivery. The SharePoint pages are linked to Microsoft Teams for reference by employees within collaboration sessions and to access immediate information on projects impacting the design and operation of Nationwide systems.

RSGIB has a legal and regulatory duty under federal and state information security laws, contracts, and industry standards to protect its customers' nonpublic personal information (NPI), including any NPI in the custody of a third-party service provider.

RSGIB partners with IRM, the Office of the Chief Legal Officer, and Procurement when establishing any agreements with business partners and third parties to help ensure consistency with Nationwide standards and expectations related to security. RSGIB collaborates with these same internal partners to implement within the business comprehensive written information security procedures that include administrative, technical, and physical safeguards for the protection of information and system security.

RSGIB does have a continuity management plan and processes in place to help ensure that systems and associates are available to continue to meet the servicing expectations of our customers and all legal and regulatory duties.

Data

Data, as defined for the scope of this report, includes Customer and Personably Identifiable Information (PII) included in data files used during Nationwide's RSGIB on-boarding, maintenance, support and servicing of plans and participants.

Access to data as defined above is limited to authorized Nationwide personnel and is only granted in accordance with the Access Control IT Security Standard and adheres to the concept of least privilege. Access is reviewed on a regular basis, and access for users who no longer require it is removed systematically (with an expedited process in place for terminations).

Data retention is based on Nationwide's data retention schedule and retention periods are based on legal, audit, and/or management requirements. Nationwide's process for records retention is supported by the Office of Records Management, which is responsible for providing legal and regulatory guidance with respect to record-keeping as well as ensuring that records are kept for as long as required (both legally and operationally).

Storing and transferring data is an integral part of Nationwide's day-to-day company process and all system data is managed, processed, and stored in accordance with the relevant Nationwide data security policies and procedures, with specific or customized requirements formally established in client contracts.

Nationwide Retirement Solutions department systems interfaces include multiple in-house written applications. The applications support a range of business functions, from on-boarding plans and participants, maintenance, support, and servicing. Primary users of these applications are internal Nationwide associates with some outputs going externally to the various areas within Nationwide and external partners. Feeds to external partners are using secure file transfer protocols, such as (SFTP).

Technologies vary by application and include both web-based and local client user interfaces, back-end databases, and various batch processing flows to support business processes. Coding technologies include JAVA, Angular and python. Database technologies include Amazon Redshift, Oracle and SQL. Application hosting is a mix of on-premises and off-premises.

All applications are written using secure coding practices and routinely audited by standard Nationwide vulnerability management scanning tools to help ensure any possible vulnerability is identified and mitigated, based on defined severity possibility.

DCDirect (RP Link)

DCDirect (RP Link) data is stored in Oracle 19C. Data is introduced into the system through various front-end applications like RPLink, RSC, mobile apps etc., and from partners using Batch flow. Files are received and sent through SFTP protocol. The front-end applications use an application programming interface (API) or back-end code to insert data into DCDirect (RP Link). Non-financial transactions are usually processed when received. Financial transactions are held in staging tables and have dependency on prices file that is received after stock market is closed and processed in the batch flow. Database connections are established to access data from upstream systems (e.g. AIMS).

RIA Services (Public)

RIA Services is a niche product used to manage participant retirement account by investment advisors. The data is stored in Oracle 19C. Data is introduced into the system through transaction management system (TMS), and from partners using Batch processes. Files are received and sent through SFTP protocol. The front-end applications use back-end code to insert data into RIA services. Transactions are held in staging tables and processed in the batch flow.

Applicable Trust Services Criteria and Related Control Activities

Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to the achievement of the entity's security and availability commitments and requirements. Control activities, whether automated or manual, relate to the achievement of the applicable Trust Service Criteria and are applied at various organizational and functional levels.

Specific control activities are provided in the section of this report titled "Nationwide Financial Services, Inc.'s Trust Services Criteria and Related Controls, KPMG LLP's Tests of Operating Effectiveness, and Results of Testing".

Nationwide has developed the following policies and standard operating procedures to operate, maintain, and secure the systems, and to achieve security and availability commitments as aligned to the AICPA Trust Principles and Criteria.

Availability

Nationwide has multiple controls and processes in place to help ensure availability commitments are met. This includes a robust BC/DR program, an emphasis on data center security/environmental controls, 24x7 monitoring of capacity/service delivery, and data backup and recovery standards.

Nationwide has controls in place to address environmental risks, which could compromise availability. Nationwide's data center personnel monitor the status of environmental protections 24x7. Alarm mechanisms are in place to communicate discrepancies in environmental thresholds. Nationwide schedules environmental systems for periodic maintenance checks throughout the year (cooling systems, uninterruptible power supply, backup generators, fire extinguishers, etc.).

Nationwide further maintains availability by backing up or replicating application processing environments and related production data to a secondary facility. This is in accordance with the management backup and recovery strategy. Nationwide has also implemented 24x7 processing capacity monitoring to allow for real-time adherence to service level agreements (SLAs). Traffic management capabilities, such as redundancy, are in place to meet business requirements. Specifically for the UVC SaaS application, system backups are regularly performed by the vendor, Zinnia (formerly Convergent Financial Technologies and SE2). They maintain and provide all detailed backup information.

In addition to data center physical/environmental security, BC/DR planning, and capacity monitoring, Nationwide has data backup and recovery standards in place that are defined by the relevant business organizations and are based on criticality. Nationwide has established RTO/RPO guidelines and tests and monitors those capabilities regularly.

Availability Monitoring

The Nationwide Enterprise Command Center (ECC) aligns to the Technology Operations department and works to maintain the health and availability of enterprise IT systems. The ECC comprises the Internet and Distributed Operations Center (IDOC), and Major Incident Management personnel. Network Technology and Operations Center (NTOC), which aligns to the Network Engineering department, works with the ECC to enable 24x7 monitoring and improve operations for speed, efficiency, and expense.

Team	Role
Internet and Distributed Operations Center (IDOC)	24x7 Level 1 and 2 Support for many different operations throughout Linux, Windows, and cloud-based services. Initiates Major Incident technical calls outside of business hours and engages the Major Incident Manager when technology service impacts are confirmed by Nationwide Technology assignment group.
Network Technology Operations Center (NTOC)	24x7 Network support and monitoring
Enterprise Command Center (ECC)	Responds to Event Management alerts and manages the Major Incident response process and provides 24x7 Major Incident coverage, facilitation, and works with Nationwide Technology support groups to restore technology services.

Incident Response Support

Nationwide defines an incident as an event that is not the standard production operation of a service and affects the quality of service, such as:

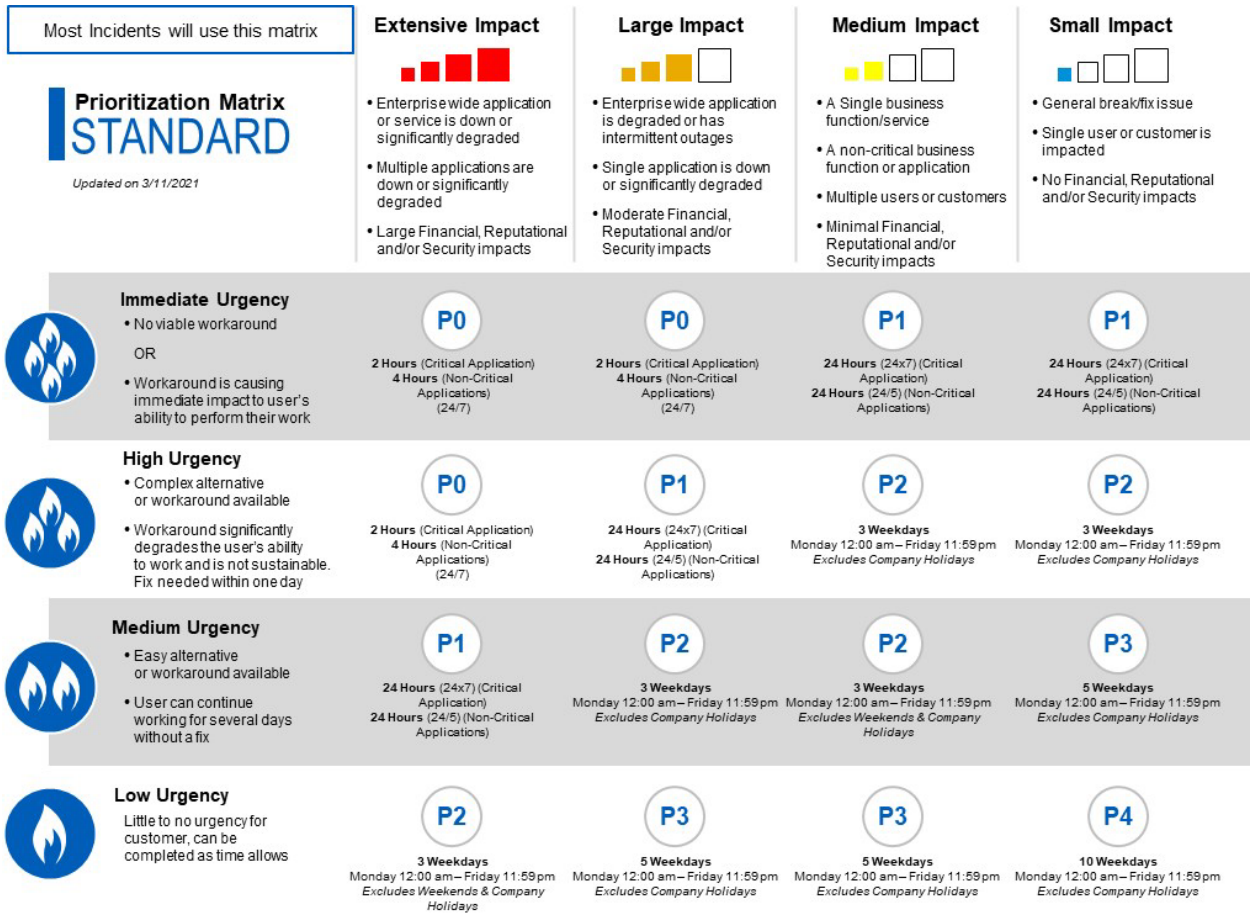
- An unplanned interruption or reduction in the quality of a Nationwide Technology service
- An event that could affect a Nationwide Technology service in the future

Nationwide also has an established Enterprise Command Center (ECC), which monitors the availability and health of Nationwide Technology's systems with extraordinary care 24x7, 365 days a year. The goal of ECC is to identify and prevent or restore unplanned outages/reductions in availability of expected Nationwide Technology services as quickly as possible. This is achieved:

- By quickly identifying and fixing service outages or degradation
- By promptly communicating incidents and resolutions to business and Nationwide Technology support staff as they occur
- By making restoration of business activities and priorities our top priority

Major Incidents (P0s) are logged in ServiceNow either manually or auto-generated by Big Panda and Netcool Operations Insight. Manually logged incidents are logged by Nationwide Technology resources that discover an incident or by the helpdesk after an incident has been reported by users of the systems.

Priority levels are assigned to incidents based upon potential impact and urgency and are defined below:



Once a priority has been determined, incident tickets are assigned to the appropriate Assignment Group for resolution within the established SLA. Assignment Groups are responsible for monitoring their queues for incidents and tasks and are responsible for monitoring the status and progress toward resolution.

Assignment Groups and group members receive email notifications when an incident is assigned to their group.

Assignment Groups are responsible for the notification and updating of tickets. Once service is restored, tickets are closed. Procedures for real-time monitoring have been established with the Technical Service Desk to help monitor tickets and prevent missed Service Levels within specific groups and specific priorities.

Priority 1 Incidents should be reviewed daily to watch for trends that might indicate an emerging major incident (Priority 0), which is defined as the following:

Any application in the production environment, within the Hours of Operation, that is completely down and/or partially down based upon the following:

1. Critical core function of an application impacting a group of users by location, state, region, or technology specific
2. Degradation of performance rendering an application unusable as indicated by high volume of calls or alerting as identified by the Configuration Item (CI) Owner
3. Intermittent failures and alerts determined by CI Owner in conjunction with Event Management Policies

4. Data which is unavailable to the business and is incorrect or corrupted as defined by CI Owner
5. Any infrastructure technology impacting groups of users by location, state, region, or technology specific where a loss of critical core function occurs (as defined above)
6. Batch jobs which have breached an SLA or a critical trigger alert within the batch processing window.

Incidents impacting, or may impact, an application with a Critical Designation may be designated Major (P0) even outside of Hours of Operation, if necessary.

Priority 0 Incidents (Major Incidents) are monitored and managed by the ECC. Once the Major Incident impact is confirmed with Nationwide Technology assignment group(s), the incident ticket is moved to an ECC Service Now queue until service is restored. Once service is restored for a Major Incident, the ECC closes the incident ticket in the assignment groups Service Now queue.

Data Center Power and Environmental Controls

Nationwide protects power equipment and power cabling in data centers and critical network facilities from damage and destruction. Protections include, but are not limited to:

- Redundant power cabling with paths that are physically separated at entry by at least 20 m from each other and maintain 1.2 m separation
- Automatic voltage controls for limiting transient voltage to equipment

Nationwide has controls in place to address emergencies related to electrical power, including emergency shutoff switches/devices where required and protection from unauthorized activation of emergency power shutoff capability.

Nationwide also employs continuous fire detection and suppression systems. Fire suppression systems are on an independent power source, are automatically activated, immediately notify corporate security/corporate real estate, and are inspected and tested by certified personnel at least annually.

Nationwide also protects information systems from damage resulting from water leakage with controls. This includes accessible master shutoffs, restriction of water systems over/around information systems (only fire suppression and cooling systems are permitted in these facilities), and inspection and maintenance activities that are documented and conducted at least annually.

System hardening

Nationwide has developed, documented, and implemented required baseline hardening standards for deploying servers (including webservers) and network devices. Nationwide considered the Center for Internet Security (CIS) framework and configuration settings as the primary reference for secure configuration policies. Hardening standards are reviewed annually. Revisions are conducted as needed to stay current with security requirements as CIS produces updated benchmarks for technologies. Monitoring processes have been established to help ensure that systems remain current with the hardening standards. Nationwide requires all hardware and software used to support provided services to be at a current version and have valid support service contracts with the vendor.

Nationwide has an experienced configuration management program/team that has an established intake process, conducts review meetings (for the CIS Benchmark), and provides for a draft/review stage where subject matter experts work with the BISO team to review any controls that conflict with business requirements or Nationwide implementation needs. Once the secure configuration document has been submitted by the subject matter expert, it is reviewed and approved by an Assistant Vice President (AVP) or above sponsor. When the configuration has received AVP approval and been validated, it is added to the bi-weekly scanning cadence where results are provided to the subject matter experts for validation with specific thresholds in place for acceptance. Additionally, metrics are tracked to help ensure the configuration remains in compliance.

End-user desktop security

Nationwide has developed, documented, and implemented required computer hardening standards for deploying end-user workstations. End users are made aware of these controls and must abide by these standards. The standards include:

- Removal of end-user administration rights
- Whole disk encryption: Nationwide applies encryption methodology that conforms to the NIST-approved algorithms, key lengths, and related standards as outlined by NIST
- Implementation of antivirus, antimalware, and Endpoint Detection and Response (EDR) software
- USB mass storage ports are disabled
- CD/DVD writing is prevented
- Secure configuration setting applied to operating systems and based on CIS industry standards
- Remote desktop support session acceptance

Additionally, Nationwide monitors all workstations, portable media devices, solid-state hard drives, and removable media containing sensitive data are monitored using device control tools to block data exfiltration. Digital and Non-Digital Media containing sensitive data incorporates the use of physical and logical access controls to protect the confidentiality, integrity, and availability of the data in question. To further support end-user desktop security, Nationwide only allows authorized software for installation on company assets and has a managed list of approved software.

User provisioning and deprovisioning

After a new employee or contractor is onboarded into the HR Workday system, the automated provisioning tool Identity IQ (IIQ) triggers an onboarding event, which includes creation of a basic logon ID.

Once the user account is provisioned, the first-time password is delivered to the user's manager. Managers receive the password from IIQ and share it with the new employee. Upon first logon, users are required to change their password.

Requests for additional access (i.e., email, Linux, and application IDs) are submitted through Identity IQ. A workflow will route the request to obtain approvals. Once approvals are granted, IIQ will create the new access and notify the requestor. Access is granted for these IDs based upon the requested for and approved access in the request. If an individual is transferred between departments or changes roles, then the access is reviewed by the new manager to either retain or remove the current access.

The off-boarding process is tied into the HR systems. Once a user is marked as terminated in the HR system, IIQ triggers an event that disables the user's NWIE credentials, thereby removing access to all managed accounts, and auto-generates an IIQ ticket to the Nationwide Identity Lifecycle Management Team (ILMG) or appropriate application team (for applications not managed by ILMG) to handle any non-managed endpoint accounts. Once the ticket is received, the disable is immediate for the network user account. ILMG will process ID disables on non-managed endpoint accounts to which they had access. All other account disables will be handled by the appropriate application team. These ancillary ID disables are completed within 45 days.

User access reviews

Nationwide conducts a multistep, quarterly access review that is designed to help ensure employees have only the access that is necessary for their specific role and responsibilities. This begins with a prestaging check where the Identity and Access Management team scopes applications for review. Once applications have been scoped, they are staged using a parameter template. During the staging process, any application that has seen a change of 20% or more in number of entitlements is investigated and the reason for the increase is documented. Procedures are performed by either the application owner, IRM team, or financial

reporting controls team to help ensure the data feed files to Identity IQ (IIQ) are complete and accurate. Once staged, the certification activity is reviewed and approved by the Director of Identity Lifecycle Management and Governance (ILMG). Upon approval, the certification is made active, and managers have ten business-days to complete their reviews in IIQ. During the certification, people leaders will review the access for each of their direct reports and indicate which access is appropriate and which access should be removed. When a people leader requests the removal of a user's access, the process for revoking access depends on whether the application is fully automated within IIQ or if manual intervention is required. If the revocation process is fully automated, the system will automatically revoke the person's access based on the predefined rules and configurations set up in IIQ. If the revocation process requires manual intervention, a work item will be generated. This work item will be sent to either the Application Team or the ID Administration ILMG. It is the responsibility of the designated team to remove the person's access accordingly.

Once the 10 business-day review period ends, the people leaders are no longer able to access the certification. The IIQ Team will utilize the Manager Decision Report to determine which people leaders have not yet completed the certification. For those who have not completed the certification on time, the following actions will be taken:

- The People Leader will lose their access to the Nationwide Network (including access to business applications).
- Their Direct Leader will receive a manual certification for that People Leader's team's access, which the Direct Leader will need to complete.
- The manual review must be completed and returned within three business-days.
- Once the completed access review has been returned from their leader and processed, access is reinstated.

To monitor review accuracy, Nationwide includes test applications/entitlements in the certification process. If a manager fails to revoke the test entitlements as part of the certification, they will receive additional training and be required to complete a secondary certification.

Once the manager certifications are complete, the Identity and Access Management Team conducts a post-certification performance check to confirm that each application scoped for the certification was included and all remedial training and certifications have been addressed. A post validation report is then created and published.

Identification and authentication

Nationwide's identification and authentication controls include enforced user ID and password composition requirements, prohibiting the sharing of passwords, authorization engines for in-scope systems are designed to default to either no access or redundant infrastructure if they fail, multifactor authentication (MFA) for remote/virtual private network (VPN) access to system components, and usage of SFTP for transmission of confidential/sensitive information over public networks.

The following user account and password parameters have been established:

- User accounts are automatically disabled after 120 days of inactivity and will not be re-enabled without a specific documented request
- Must be a minimum of 8 characters
- Where technically feasible, passwords should be a minimum of 12 characters
- Must have at least 3 of the following:
    - Combination of alphabetic and numeric characters
    - Special character(s) (e.g., !@#$%&)

    - Uppercase letter(s)
    - Lowercase letter(s)
- Cannot be default password
- Cannot be same as User ID or Account Name
- Cannot contain months or seasons
- Cannot be numbers or characters in sequence where there are three or more instances of the same character in a row, or characters that increase or decrease in sequence
- Passwords must automatically expire at a maximum of 90 days
- ID Accounts cannot reuse one of their past 20 passwords
- Passwords must not be stored or transmitted in clear text
- The logon process must not be validated until all logon data is input
- In the event of a failed logon, only a generic “failed” message can be displayed—no indication of what part of the logon (e.g., ID or password) failed can be included in the message
- Passwords must be changed whenever there is suspicion or likelihood that the password or system has been compromised
- Passwords for Primary and Secondary Exclusive ID Accounts for the same person must be substantially different

Privileged accounts

Privileged accounts (root and administrator) are administered by the Identity Lifecycle Management and Governance (ILMG) team. Passwords for privileged accounts are to expire on a 90-day basis or when someone with knowledge of the password transfers or resigns. Ninety-day password changes are handled via automated reminders. Users with administrative access to systems are assigned a separate individual user ID for that use. Nonprivileged user IDs are used for day-to-day work. Administrators are restricted from multiple physical location logins.

Access to the default privileged accounts is granted through the “run as authority” in Windows and SUDO commands in Linux. Privileged users log in using their unique accounts but are able to assume this higher-level authority. For SUDO-level access, users log in using their unique user ID and password. Knowledge of the root password is limited to console log-in only. Consoles are in secured data centers. This level of access is limited to Linux System Administrators and members of the Security Administration group based upon job function.

For administrator-type access, privileged users are added to the administrator group. Membership in this group provides the administrator-type access but requires the individual to authenticate with a unique ID and to supply a unique password. This level of access is limited to those individuals identified as Windows and Linux system administrators and the individuals in the Information Security group responsible for access controls.

Access is controlled by the “least privilege” approach, which means access is denied by default. On Linux systems, access is restricted by implementing a default SUID setting, while it is an O/S default on Windows. Although access controls are managed by the ILMG team, access changes are submitted through IIQ, which is the Identity Lifecycle Management tool. A predetermined workflow will route the requests for appropriate approvals.

Network security and tools

In conjunction with the Information Security Policy, Nationwide has developed and maintains a comprehensive System and Communications Protection and Data Protection IT Security standard that provide the requirements necessary to secure the Nationwide network. These control baselines include the following:

- Firewall configurations allow/deny access to appropriate personnel/organizations/services (reviewed semiannually).
- From January 1st, 2023, Nationwide began a transition to Akamai Application & API Protector via AT&T Business. In 2023 Nationwide ingress firewalls are monitored via automated processes to help ensure inbound connections are being properly filtered by an approved web application firewall policy or have been onboarded to Akamai and are protected by Akamai Application & API Protector via AT&T Business, which automatically updates signatures.
- Encryption standards and other security techniques/technologies are required to help ensure secure transmission of private or confidential information sent over public networks. Information written or stored on backup media is also encrypted.
- DLP solutions are used to scan for and limit sensitive information in outgoing transmissions, including email and instant messaging.
- Antivirus and antimalware detection tools are used to scan data, transmissions, and email to mitigate processing/service interruptions caused by viruses or malware.
- DDoS attack preventative software is in place, and a service-based solution is used to handle DDoS attacks.
- Access management to network devices (routers, firewalls, etc.) follows the standard Nationwide access management procedures outlined in the “User Access Reviews” section above.
- Web proxy is used to restrict access to unauthorized websites, including external email providers (e.g., Google, Yahoo).
- Mobile devices used for company communications are password protected and configured for full device encryption.

Network firewalls are configured to only allow access for ports, protocols, and services that are necessary for required functionality. Firewalls on the Nationwide network are configured based upon baseline rule-set standards. Management performs a quarterly review of firewall rulesets. Management performs a quarterly review of privileged access to firewalls to reconfirm access is appropriate based upon job responsibility.

Secure asset disposal

Nationwide computing equipment or data storage devices (workstations, laptops, network devices, etc.) that have reached their useful end of life are disposed of using the services of a Nationwide Information Risk Management department-approved disposal vendor. All disposal vendors enter into a Nationwide Legal department-approval agreement. Resale or donation of Nationwide computing equipment to Nationwide employees or anyone else other than an approved disposal vendor is forbidden.

Physical security

Nationwide has a physical security program in place that protects the corporate campuses, transmission medium, and data center locations. This program is guided by documented procedures, which are reviewed annually and updated as needed to provide a secure environment for associates and data.

Corporate Campuses

Physical access to nonpublic portions of key Nationwide facilities is limited to those individuals that have been granted access based on their role, position, and requirement to be physically on-site. Appropriate

credentials such as a badge or visibly distinguishable temporary badge are issued and are required to be displayed at all times. All key Nationwide facilities have a process to develop, approve, and maintain an access list, which is reviewed at least twice a year to verify that each individual continues to require access. Individuals no longer requiring access are removed from the list and their credentials revoked.

To help ensure that access is only granted to authorized individuals, all Nationwide facilities enforce physical access authorizations (such as badge/card readers) at all entrances and exits, have 24x7 monitoring (CCTV) at all entrances and exits, and staff security officers 24x7. Physical access is monitored in a way that allows Nationwide to detect and respond to physical security incidents, including having systems in place that facilitate the identification of and response to suspicious activities such as off-hour access and access to areas not applicable to one's work. To further support least privilege with respect to physical security on campus, Nationwide has special provisions for sensitive areas such as the CSOC and executive floors.

Visitor access to Nationwide campuses is also strictly controlled and monitored. Nationwide security verifies the identity of the visitor and validates their purpose for being on premises, and visitor access records are maintained for one year and include (but are not limited to):

- Name and organization of the visitor
- Name and organization of the visited
- Forms of identification provided
- Date and time of access
- Purpose of the visit

Nationwide's physical and environmental protection program also has provisions to protect the transmission/distribution lines to prevent damage (accidental or intentional), disruption, tampering, and interception/misdirection.

Data Centers

As with all nonpublic areas of Nationwide, physical access to data centers is limited to individuals with a legitimate purpose. Nationwide utilizes a key card system, has a security officer on site 24x7, and maintains 24x7 monitoring (CCTV) of all entrances and exits.

Access to the data center requires a formal request and an approval from the on-site manager or team lead. Access levels are programmed into the card key system according to the job functions performed. Nationwide uses 18 access levels that can provide access to a room/space based on least privilege. A monthly review of all individuals with data center access is conducted to help ensure that access is still required. Access for terminated individuals is immediately disabled.

Visitors to the data center facilities must be verified by photo ID and the RITM even if they are known to Corporate Security. If the visitor does not have a government ID or a Nationwide associate/contractor badge, another form of identification must be provided. Verification of visitors is performed by checking the visitor's photo, name, and any applicable notes either two forms of identification or one form of government/Nationwide prior to issuing a credential to permit access. prior to issuing a credential to permit access. Access to sensitive areas, such as the raised floor of the data centers, is highly restricted to those individuals whose job function requires it. Associates and visitors who require temporary access to data center sensitive areas are always escorted by an authorized individual. Visitors are required to sign in and out at the security desk and must have a valid Request Item (RITM), Incident (INC), or Request for Change (RFC) (with an RITM attached). All Nationwide Technology personnel/vendors sign into iVisitor for all work beyond the office area. All vendors performing work on the raised floor also sign into iVisitor. Cleaning crews are contractors and must have a valid RITM to enter each day to perform their work. Access is added by Security when they arrive and removed when they leave.

Security monitoring

Nationwide's CSOC is a team of security professionals who continuously monitor the external network perimeter 24x7, 365 days a year. This team receives intel from various sources: the central logging system, suspicious activity reports, the latest threats, vulnerabilities from industry groups, and reports from employees. Nationwide's team of security professionals leverages advanced web application firewalls, intrusion detection and prevention tools, data protection tools, and security incident and event management tools as well to identify and respond to suspicious activity. To support the handling of incidents, Nationwide has incident response policies and procedures in place that include an escalation plan based on the nature and severity of the incident. The IR Cyber Investigations Team (CI) monitors for security incident alerts records and follows a process of analyzing the security incident. The process begins with detailing what specific attack occurred, which system(s) were affected, and what happened during the attack. If root cause cannot be determined, then it is routed to the IR Threat Response Team for further analysis. Automated mechanisms and alerts have been established using various tools, including Splunk and Phantom.

Nationwide has a comprehensive threat monitoring program in place to support the incident response teams. Nationwide receives notification of possible security events via either manual reports or automated mechanisms from various tools. All of these methods have a starting point of creating an event within Phantom, which is subsequently worked by the Cyber Investigations team according to their documented processes. Automated mechanisms can flow into Phantom via various methods such as an email ingestion, an ingestion direct from the tool recording the alert, or an ingestion from data received and/or correlated by Splunk indicating a possible security event. The action taken will be based on analysis of the activity along with appropriate log and other sources involved. The action could be closure as a benign act, taking defensive action to stop/kill the activity permanently and close the case, or escalation for further action. Escalation follows a path of escalation to the Threat Response (TR) Team within IR. At this point in the flow, the Phantom case is considered closed regardless of the action taken by CI. For any cases escalated to TR, they leverage a secured MS Teams space to track all of their actions regarding cases they investigate. They will triage the information provided and leveraging their processes, experience, and indications within the data available, work the investigation. If there are indications of any possible data compromise, then TR will engage Privacy Legal for consultation and assistance as needed. Routine operational reports are monitored in regard to several aspects of Phantom work ranging from tracking mean time to contain (MTTC) to monitoring cases through their lifecycle to closure. This helps ensure all are handled in an effective and timely manner. All case data (in Phantom and case data captured in collaboration tools like Microsoft Teams) is retained for five years.

Event Management

Nationwide's Incident Management program is also designed to identify, isolate, respond to, and remediate suspected or actual cybersecurity events. A holistic approach is taken to incident management to help ensure triggers are monitored and incidents are uncovered. This involves log aggregation, security information, and event management, an incident response case management system, and end-user education. An Incident Response process is in place to systematically respond to any identified Nationwide Technology security incident that could threaten the confidentiality, integrity, or availability of an information resource.

If a cybersecurity event is identified, Nationwide's CSOC works cross-functionally with the Event Management Program or ERT and Response Team to investigate the security event fully and take appropriate action to remediate if necessary.

The CSOC's primary functions are incident response, vulnerability management, and defensive optimization. Nationwide also has a mature Event Management Program, which investigates security incidents, substantiates facts, and conducts legal analysis according to state and/or federal statutes, and contractual obligations.

The CSOC IR plan:

- Provides a roadmap for implementing the incident response capability

- Describes the structure and organization of the incident response process
- Provides a high-level approach for how the CSOC Incident Response Process works in conjunction with the Nationwide Event Management Program
- Defines reportable incidents

The plan is owned and governed by the CSOC IR Team; and reviewed/updated at least annually according to IRM documentation requirements. The incident response plan is continually updated based on lessons learned through incident handling and testing.

The CSOC Incident Response Process is tested at least annually to determine its effectiveness. Testing methods may include, but not be limited to, one or more of the following methods:

- Walk-Through or Tabletop Exercise
- Simulation (parallel or full interrupt)
- Checklist Approach

Selected individuals from the CSOC IR Team are required to participate in testing events.

The Incident Response IT Security Standard owner oversees the testing effort with participation by groups relevant to the testing scenario. Test results are documented and maintained for a period of 24 months. The results of testing are utilized to enhance the CSOC Incident Response Process.

Problem Management

Nationwide Technology Problem Management is the process responsible for managing the lifecycle of all "Problems." A Problem is the cause of one or more incidents, which is usually unknown until further investigation through Problem Management is done and defines a problem as the unknown root cause of one or more existing or potential incidents. A Problem record is automatically created for Major P0 incidents or manually created through the identification of an incident trend or ad hoc Problem. The appropriate team and Problem Manager are assigned the Problem record to investigate. Upon the Problem Manager's assessment of the Problem, they will assign a Problem Analyst or cancel the record should it be deemed an invalid or a duplicate Problem. Notification from ServiceNow occurs when the problem ticket is assigned. Incidents are closed once service is restored and related incidents are linked to the problem ticket within ServiceNow.

A root cause analysis (RCA) is performed by both the Problem Analyst and the Problem Support Team. The Problem Analyst engages appropriate resources as necessary and assigns investigative tasks to the Problem Support Team(s). Several iterations of RCA may be performed until determined complete by the Problem Analyst.

Upon completion of RCA work, the problem will be identified as Root Cause Known, Root Cause Unknown, or Risk Reduced. If a Workaround is identified, it is documented in the record. If a Workaround requires a change be made to any Nationwide Technology asset or Nationwide configuration item (CI), then the Change Management process is followed before it can be applied. In some cases, simple instruction constitutes the Workaround and a Knowledge Article is created. When a problem ticket is identified as Root Cause Known, it becomes a Known Error record. Known errors identified by vendors and testing have a related problem record.

Once mitigation via a Workaround or a permanent solution has been applied, the Problem enters the resolution and closure phase. Necessary details gathered throughout the lifecycle of the Problem are logged in the Problem ticket and then resolved and auto closed within 7 days. A notification is sent to the Problem Creator. Any necessary continuous improvement efforts are determined. In cases when a root cause nor a Workaround can be identified for a Problem, the ticket is required to include detailed information on why an RCA was not found and acknowledged by the related owner/assignment group prior to closure.

Change Management

The Nationwide IT Change Management process is responsible for controlling activities involving the recording, documenting, approving, and monitoring of changes made to Nationwide Technology applications and supporting infrastructure, including data center environmental systems. Nationwide maintains a central repository to track and maintain all relevant information on IT Configuration Items (CI). Changes to standard IT configuration items on Nationwide systems require the IT Change Management process to be followed.

Formal IT Change Management Process and Policy Guides have been created and approved that outlines structured change management processes and procedures to help ensure that Nationwide associates maintain and protect the security and availability of the infrastructure and systems that support Nationwide and its customers. The process and supporting documentation is reviewed annually by management and updated as appropriate. Changes are managed to minimize risk exposure, identify severity of impact and disruption, and help ensure quality delivery of changes to meet business needs.

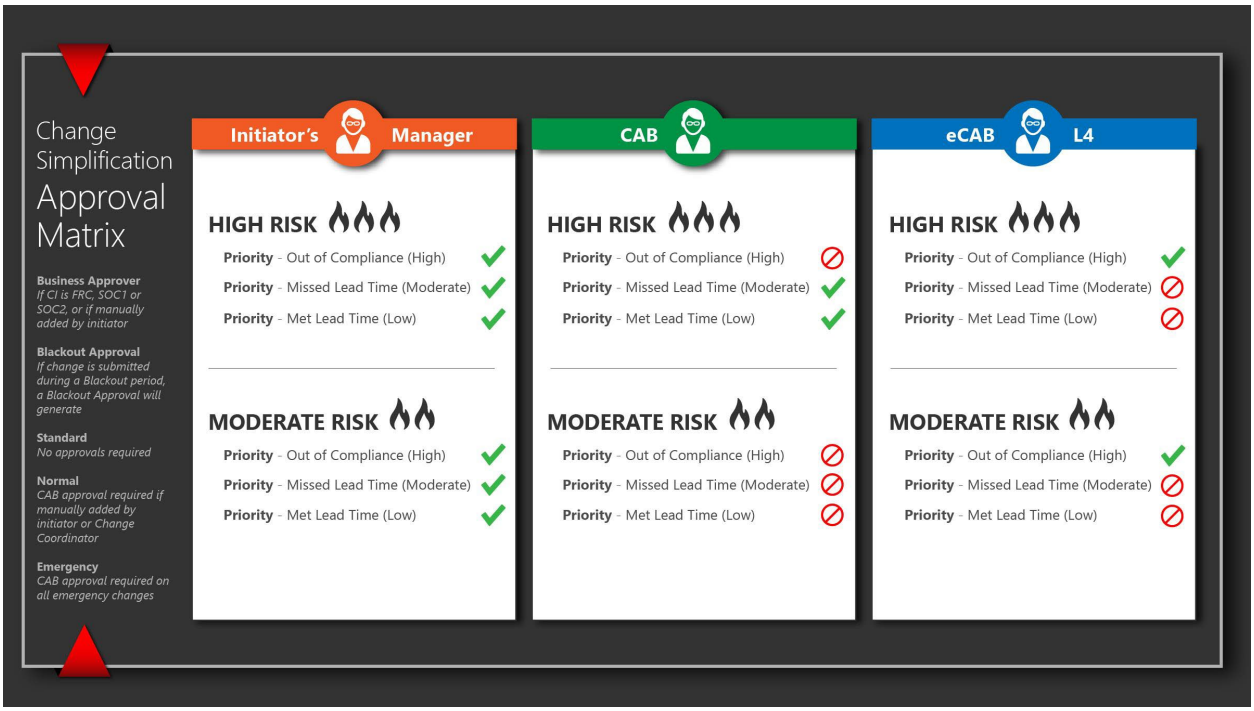
A Change Advisory Board (CAB) group exists to provide change management recommendations, process input, high-risk change review/approval and standard change template review/approval. They may represent the entire Nationwide Enterprise IT operations areas, specific IT units or specific business areas.

Enterprise Change Management Process

Nationwide Technology Change Management Process

The primary objective of the Nationwide Technology Change Management process is to permit changes to be made via consistent and standardized processes and procedures while minimizing disruption of, or impact to, Nationwide Technology Services. Other objectives include ensuring appropriate review and analysis of changes for optimum scheduling, conflict detection/analysis, and enabling Audit functions to protect Nationwide Technology Services that serve Nationwide and its Critical Business Partners.

Change records must be submitted and approved prior any change activity and must contain relevant information such a description, justifications, test plan, backout plans, deployment tools, configuration items, activity time/dates, etc. Once submitted, the change follows structured workflows that may include additional review and/or required information. Based on the change risk, priority and/or change type, the change requires from 1 to 4 different approvals (ex: Manager, CAB, eCAB, Blackout or Business).



Change controls and supporting documentation

Nationwide has a secure application development program in place that is designed to set development standards and embed security into the development life cycle. To help accomplish this, Nationwide has implemented secure coding tools that scan code logic for known flaws and vulnerabilities at deployment in order to resolve the vulnerabilities prior to introducing the code into the production environment.

Emergency changes

An Emergency Change may only be used to restore service during a P0 incident, as authorized during the Problem Management Critical Situation meeting, or by authorized Security and Information Risk or Enterprise Release Delivery Management (ERDM) personnel to address imminent, or current and ongoing security threats to Nationwide. A P0 is an unplanned interruption or degradation of service that has an impact to revenue-generating services and/or multiple systems affecting multiple groups throughout the enterprise. Since an emergency denotes an outage to a production system and/or multiple systems affecting multiple groups throughout the enterprise, an Emergency Change Request addresses the outage in a timely manner with the goal of restoring regular operations with minimal risk. Emergency changes follow the normal change management process in an expedited manner.

Patch management

Nationwide has a comprehensive vulnerability management program that incorporates asset management, vulnerability detection, established guidelines for ranking vulnerabilities (by severity), established patching SLAs, and remediation tracking and reporting. Nationwide's patch management program helps ensure vulnerabilities are ranked by severity (using factors such as severity of the vulnerability itself, known exploits of the vulnerability, and location of the asset) and are assigned an SLA based on that determination. All critical vulnerabilities are required to be patched within seven days. For patch distribution, Nationwide leverages Windows OS (SCCM) and Linux (in-house developed patching automation tool). Servers and workstations are scheduled for monthly patching.

Relevant Aspects of the Control Environment, Risk Assessment, Information and Communication, Monitoring, and Control Activities

Nationwide's control environment reflects the overall attitude, awareness, and actions of the Board of Directors, management, and colleagues concerning the importance and relevant components of internal controls and their emphasis within the organization through its policies, procedures, methods, and organizational structure. Internal control consists of interrelated components that are integrated with the management process guided by the COSO 2013 framework:

A. Control Environment

B. Risk Assessment

C. Information and Communication

D. Monitoring

E. Control Activities

Control Environment

The control environment sets the tone of an organization. It is the foundation for other components of internal control, providing discipline and structure. An effective control environment is created by developing policies and practices that promote adherence to the requirements of the control environment.

Nationwide Organizational Structure

RSGIB's activities are overseen by Nationwide's Board of Directors and Audit Committee of the Board of Directors of Nationwide. The Board of Directors is comprised 16 members, including 15 external members. The Audit Committee monitors internal and external examinations of RSGIB's retirement and savings plan activities and helps ensure that suitable internal control is maintained.

Retirement and savings plan activities within the RSGIB group are conducted in accordance with the established policies and procedures, which are periodically updated. The responsibilities of RSGIB case administration are allocated among personnel so as to segregate the following functions: input of transactions, processing of transactions, recording of transactions, cash disbursement requests, and reconcilement activities.

Infrastructure and Operations

Nationwide Infrastructure and Operations delivers technical support and infrastructure management in support of Nationwide and RSGIB.

HR Resources Policies and Practices

Nationwide has in place a clearly defined organizational structure, supported with regular oversight by supervisory and management personnel. The organization has formal HR policies and behavioral standards that clearly communicate organizational values, expectations, and ethical standards. An annual review is also performed for each employee to communicate performance feedback and create objectives. Managers and supervisors provide formal and on-the-job training as required to maintain required levels of competency.

Nationwide Talent Acquisition is responsible for screening candidates for the appropriate skill set. Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements

are evaluated as part of the hiring or transfer process. New hires are required to sign a confidentiality agreement that requires them to maintain strict confidentiality of both internal and customer information. In addition, policies governing the conduct of employees, as well as other matters related to employment, are communicated and provided to employees at onboarding. Nationwide maintains a code of conduct, which covers company polices and core values. All associates are required to read and acknowledge the code of conduct annually. Failure to comply with the code could lead to disciplinary action, up to and including termination of employment. Employee candidate background screening procedures are included in the recruitment process.

Security Policies and Practices

Nationwide has established an Information Security Policy and IT Security Standards, which are reviewed at least annually via the SRB and receives approval from Nationwide's EORC. The Information Security Policy is required to be reviewed by employees at onboarding and at least annually thereafter. Additionally, the Information Security Policy and IT Security Standards are published and available on the Nationwide intranet and communicated to all employees on a periodic basis.

Responsibility for Internal Controls and Risk Management

Nationwide management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Board of Directors. The objectives incorporate the service commitments and system requirements of the RSGIB along with financial and operational objectives. The risks are assessed annually through a survey sent to subcommittee leadership personnel to identify changes in underlying threats or in the environment that would require an update to assessed risks.

Additionally, Nationwide has defined a formal Enterprise Risk Management (ERM) process that identifies risks relating to achievement of security and availability objectives, among other risks, through subcommittees where the top risks are documented and reported out to the Board of Directors on an annual basis by means of an Own Risk and Solvency Assessment (ORSA) report.

Information Security

Data Protection

Nationwide has an established framework for the classification of enterprise data that is designed to comply with regulatory requirements and is based on potential adverse impact to the enterprise of unauthorized access to or disclosure of that data. The requirements established in this framework apply to all enterprise data, including third-party data, whether stored on premises or in the cloud.

Nationwide's information classification standard classifies data into one of five ways:

- Public
- Internal
- Private
- Sensitive Personal
- Restricted

Nationwide's information classification standard is in place to help ensure that data is classified, properly secured, and restricted to authorized personnel. Nationwide's current information classification process requires the Software Engineering Product Manager (SEPM) to assign the data classification (public, internal, private, sensitive personal, restricted) in the Application Configuration entry in ServiceNow. Then, the Data Custodians for the Auditable Business Units verify that the data classification is correct.

The Application Software Engineering Product Manager is responsible for linking databases to their applications within the Servicenow Configuration Management Database (CMDB). For structured data in databases, classification scans document private and sensitive personal data only, per direction of the Office of Privacy.

BigID is a licensed tool used to discover and classify data using scanners hosted on Nationwide's AWS tenant. Nationwide implemented BigID for structured data classification in Q2 2023 and scanning began in June of 2023. Nationwide utilizes the CMDB in ServiceNow to obtain the list of databases in scope for classification scanning with BigID. BigID will scan in scope databases and tag private and sensitive personal data according to the Information Classification Standard. BigID is the source of record for sensitive data classification. Prior to June of 2023, the Nationwide Governance Catalog was used to scan database metadata.

Third-Party Risk Management

Nationwide has policies and procedures in place to review and manage third-party suppliers and service providers, which include three different Supplier Risk Questionnaires (SRQs), all based on NIST. Nationwide's SRQs are the Security Foundation Assessment, Information Security Infrastructure for Data Protection Assessment, and Information in the Cloud Assessment.

Risk Assessment

Nationwide management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Board of Directors. The objectives incorporate the service commitments and system requirements as they relate to security and availability of RSGIB, along with financial and operational objectives.

The assessed risks are circulated annually through a survey sent to subcommittee leadership personnel to identify changes in underlying threats or in the environment that would require an update to assessed risks. Further, as part of the annual risk assessment process, Continuity Management performs analyses on scenarios to address availability and resiliency risks.

Vulnerability Management

Nationwide identifies, analyzes, and communicates threats and vulnerabilities from external bulletins. This includes communicating this information to the Vulnerability Response Team and advisory representatives of potential impacted areas for assessments and modeling.

Nationwide also engages an outside vendor to perform continuous penetration testing and monitoring on their environment. Identified issues are raised to Nationwide and tracked through resolution in a governance, risk, and compliance (GRC) tool.

Further, Nationwide uses a commercial software tool to conduct vulnerability scanning on a defined basis. To remediate vulnerabilities, Nationwide's patch management program helps ensure vulnerabilities are ranked by severity (using factors such as severity of the vulnerability itself, known exploits of the vulnerability, and location of the asset) and are assigned an SLA based on that determination.

Internal Audit

Internal Audit reports functionally to the Audit Committee of the Board of Directors and administratively to the Chief Legal Officer. Nationwide's Internal Audit organization performs its duties in accordance with a charter that has been approved by the Audit Committee, and is an independent, objective assurance activity designed to add value and improve the organization's control environment, including a focus on security and confidentiality.

On a quarterly basis, Nationwide's Internal Audit organization develops an audit plan based on the key risks identified during the risk assessment process and communicates the plan to the Audit Committee. These

audit programs include a mix of manual and automated controls, as well as preventive and detective controls, to mitigate risks identified during the risk assessment and engagement scoping processes. Further, the audit programs are designed to include various levels of management.

Internal audit performs audit/advisory procedures using a formal methodology, documents their procedures and results in the GRC tool, and prepares audit/advisory reports summarizing the engagement scope, findings, and an overall opinion on the control environment. Management is responsible for responding to all issues identified by Internal Audit. Management may decide to either mitigate or assume each issue, based on issue ratings and management level. Management tracks the issues they own and communicates status of remediation activities to relevant stakeholders on a periodic basis. All assumed issues require annual reassessment to decide whether to mitigate or reassume. All issues are monitored by Internal Audit and escalated as necessary and considered for aggregation risk.

Within the Internal Audit organization, annual performance reviews are performed, and trainings are required for Internal Audit personnel. Several factors are considered when staffing audit engagements (e.g., subject matter expertise, individuals' strengths and opportunities, timing/availability, complexity of the engagement). Additionally, during each engagement there is an Auditor Evaluation criterion for auditors to provide coaching and feedback to each other.

Merger and Acquisition Reviews

Nationwide's corporate growth strategy includes plans for organic growth and growth through acquisition. As such, a need exists to assess and report information risks during the due diligence steps in the Nationwide Merger and Acquisition process and to monitor risks following a merger and acquisition. Information risks assessed prior to an acquisition assist decision maker's with understanding the total cost of ownership (money/time/resources) for an acquisition company.

Information risks monitored after an acquisition help to protect the Nationwide brand for majority-owned acquisition companies. Documented information risks assist in developing post-acquisition roadmaps:

- Policy Compliance Road Map – Defines milestones for all majority-owned affiliates to comply with the Nationwide Information Security Policy
- Connectivity Road Map – Defines milestones for entities (Nationwide and non-Nationwide) requesting network connectivity termination into a network segment beyond that allowed by their current Nationwide assessment.

Investment in an existing company generating liability for Nationwide beyond the investment amount will invoke IRM's Mergers and Acquisitions Process. Investment in a new Nationwide start-up company would be considered an affiliate of Nationwide and not be required to follow this process; likewise, divestures would not follow this process.

Information and Communication

Nationwide employs various methods of communicating relevant information regarding security across the entity and throughout the business units.

Employee Information and Communication

Nationwide Technology Risk Management is responsible for the enforcement of corporate IT product security standards and guidelines. Nationwide Technology is responsible for overseeing the Network Systems Administration, User Support Database Administration, and Product Support Groups. Nationwide Technology is also responsible for maintaining objective system descriptions for critical applications, network diagrams, procedure manuals, and/or system runbooks, and availability of corporate data.

Nationwide Technology Risk Management is responsible for the security of systems and consumer data. This group maintains information security and privacy policies and standards made available to all

Nationwide employees via the corporate intranet. Sensitive data is only stored on Nationwide-owned devices that are governed by the information security policy.

The information security controls described in the corporate information security policy (e.g., access controls, authorization, monitoring, network controls, wireless connectivity, logging) apply to all Nationwide environments (production, QA, testing, and development) unless otherwise noted. Additionally, privacy policy notices are available at all points where personal information is collected, transmitted, processed, or stored. Data Owners are designated, in writing, for all customer information under Nationwide control, and are reviewed on a periodic basis.

Nationwide has documented internal communication policies and procedures to help ensure that employees understand their individual roles and responsibilities and that significant events are communicated in a timely manner. These policies include formal and informal training programs, use of email messages to communicate time-sensitive information, and communications via intranet sites.

Nationwide maintains an ongoing security awareness program through new employee orientation, periodic email communications, intranet sites, email communications, and required training. Additionally, the Compliance department communicates compliance-related information to Nationwide associates. Through these mediums, information security and availability obligations are communicated to new and existing employees as part of the onboarding and periodic security awareness communications processes.

Customer Information and Communication

Nationwide security and availability commitments, requirements, and related changes are communicated to customers through a Master Services Agreement, Statement of Work, and/or customer-specific SLAs to identify and communicate:

- Security and availability commitments regarding the system and services provided
- Client responsibilities related to system security and availability
- Notification of approved and in-process changes that may affect system security and/or availability.

Nationwide has a policy that defines the support and communications procedures and guidelines in the event of information security and availability failures, incidents, concerns, and other complaints. Associates, contractors, and customers are made aware of their ability to report incidents via a service desk hotline located on the corporate website through the Nationwide Information Security Policy, training, and/or master service agreements with customers. Nationwide has a Service Desk that provides monitoring and support for various Nationwide products and services 24x7. In addition, RSGIB provides its customers with direct contact information to the RSGIB service desk which is available during business hours. RSGIB also maintains various procedures that align to the Nationwide policy to help ensure appropriate support and communications for addressing information security and availability events.

The processes that Nationwide employs to help ensure quality systems implementation and support are constantly evolving to reflect business conditions. There is distinct development, testing, quality assurance, and change management functions that interact to complete established system release processes.

Monitoring

A formal management information and reporting system exists to provide monitoring of key controls and performance measurement by management. Adherence to controls is monitored through periodic management reporting of exceptions and production and transaction volume. Results of RSGIB operations are communicated to various levels of management and culminate in a monthly report. Management maintains the relationship with AT&T Business by conducting periodic discussions and reviews of output reporting with AT&T Business personnel in the evaluation of AT&T Business' performance against established service level objectives and agreements.

For other subservice organizations, management conducts an annual review of the carved-out subservice organizations' SOC 1 or SOC 2 reports, where they review the applicable third-party service organization's reports for:

1. The subservice organization's general IT controls to help ensure they are addressed within the report and to review them for any potential deficiencies.

2. For any nested subservice organizations to determine if additional SOC reports are needed for review.

3. The subservice organization's recommended user controls to help ensure Nationwide has the necessary processes and controls in place.

Control Activities

The control activities that Nationwide has implemented are included in section 4 of this report. Although the controls supporting Nationwide's system of internal control are included in section 4, they are an integral part of Nationwide's description of the system.

Complementary Subservice Organization Controls

Nationwide's system was designed with the assumption that certain controls supporting system requirements and service commitments related to security and availability can be achieved only if complementary subservice organization controls assumed in the design of Nationwide's controls are suitably designed and operating effectively, along with the related controls of Nationwide.

The table below reflects the subservice organization providers upon which Nationwide relies for certain functions and controls that are relevant to Nationwide's security and availability commitments and system requirements. For subservice providers, the table summarizes the expected controls to be implemented by the subservice organizations and the related trust service criteria.

Specifically, subservice organizational entities should have controls in place to address the following:

Subservice Organization	Complementary Subservice Organization Controls	Services Provided	Related Criteria
Amazon Web Services (AWS)	AWS should have controls to help ensure that: • physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals as it relates to the RSC system. • physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals as it relates to RIA Managed Accounts TMS (Public) system for the period 8/26/2024-12/31/2023. • manage the risks associated with environmental threats to critical information technology infrastructure. • backup and recovery of infrastructure to meet critical business objectives. • notifying Nationwide personnel of any potential security breaches. Notifying Nationwide personnel, in a timely manner, when changes are made to technical or administrative controls impacting AWS' systems.	Application and infrastructure hosting, environmental safeguards, backup and recovery	CC6.4, CC6.5, A1.2, A1.3
AT&T Business	AT&T Business should have controls to help ensure that Intrusion detection/prevention systems (IPS/IDS) are utilized to monitor, detect, and prevent unauthorized access to external connection attempts to the Nationwide's network	Intrusion detection and prevention	CC6.6

Subservice Organization	Complementary Subservice Organization Controls	Services Provided	Related Criteria
Zinnia (formerly Convergent Financial Technologies and SE2)	Zinnia should have controls to help ensure that changes to the UVC system are authorized, tested, approved, properly implemented, and documented.	Change management	CC8.1
	Zinnia should have controls to help ensure that physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals as it relates to the UVC system.	Application and infrastructure hosting	CC6.4, CC6.5
	Zinnia should have controls to help ensure that administrative and operational procedures are established within the systems operations group to provide for backup and retention of systems and data as it relates to the UVC system.	Backup and recovery	A1.2, A1.3
Tierpoint	Tierpoint should have controls to help ensure that: • physical security to information systems is protected from unauthorized access, damage, and interference. • environmental security to critical information technology infrastructure is protected from environmental threats. • backup and recovery of infrastructure to meet critical business objectives. • notifying Nationwide personnel of any potential security breaches. Notifying Nationwide personnel, in a timely manner, when changes are made to technical or administrative controls impacting Tierpoint's (RIA) systems.	Application and infrastructure hosting, environmental safeguards, backup and recovery	CC6.4, CC6.5, A1.2, A1.3

Subservice Organization	Complementary Subservice Organization Controls	Services Provided	Related Criteria
Stack	Stack should have controls to help ensure that: • physical security to information systems is protected from unauthorized access, damage, and interference. • environmental security to critical information technology infrastructure is protected from environmental threats. • backup and recovery of infrastructure to meet critical business objectives.	Application and infrastructure hosting, environmental safeguards, backup and recovery	CC6.4, CC6.5, A1.2, A1.3
Cohesity	Cohesity should have controls to help ensure that: • physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals as it relates to the Cohesity system. • environmental security to critical information technology infrastructure is protected from environmental threats. • program logic changes to the Cohesity system are authorized, tested and approved prior to implementation into the production environment. • backup and recovery of infrastructure to meet critical business objectives. • notifying Nationwide personnel, in a timely manner, when changes are made to technical or administrative controls impacting Cohesity's systems.	Application and infrastructure hosting, environmental safeguards, backup and recovery	CC6.4, CC6.5, CC8.1, A1.2, A1.3

Subservice Organization	Complementary Subservice Organization Controls	Services Provided	Related Criteria
Stonebranch	Stonebranch should have controls to help ensure that: • physical access to computer equipment, storage media, and program documentation is limited to properly authorized individuals as it relates to the Stonebranch (UAC) system. • environmental security to critical information technology infrastructure is protected from environmental threats. • program logic changes to the Stonebranch (UAC) system are authorized, tested and approved prior to implementation into the production environment. • backup and recovery of infrastructure to meet critical business objectives. • notifying Nationwide personnel of any potential security breaches. • notifying Nationwide personnel, in a timely manner, when changes are made to technical or administrative controls impacting Stonebrach's systems.	Application and infrastructure hosting, environmental safeguards, backup and recovery	CC6.4, CC6.5, CC8.1, A1.2, A1.3

Trust Services Criteria and Related Controls

Nationwide's trust services criteria and related controls are included in Section IV of this report, "Nationwide Financial Services, Inc.'s Trust Services Criteria and Related Controls, KPMG LLP's Tests of Operating Effectiveness, and Results of Testing," to eliminate the redundancy that would result from listing them in this section and repeating them in Section IV. Although the trust services criteria and related controls are presented in Section IV, they are, nevertheless, an integral part of Nationwide's description of the system in achieving the system requirements and service commitments related to security and availability.

Section IV.

Nationwide Financial Services, Inc.'s Trust Services Criteria and Related Controls, KPMG LLP's Tests of Operating Effectiveness, and Results of Testing

Control Considerations

KPMG's examination of the operating effectiveness of certain controls of the company was restricted to the system requirements and service commitments related to security and availability and the related controls specified by Nationwide in the "Testing Matrix" within this section and was not extended to procedures in effect at client locations or other controls that may be included in management's description of its system but not listed in the aforementioned matrix.

KPMG's tests of the effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls and the extent of compliance with them were sufficient to provide reasonable, but not absolute, assurance that the specified system requirements and service commitments were achieved during the specified period. KPMG's tests of the operating effectiveness of specific controls were designed to conclude on the operating effectiveness of controls throughout the specified period, for each of the controls listed in the matrices in Section IV. In selecting particular tests of the operating effectiveness of controls, the following were considered: (a) the nature of the items being tested; (b) the types and competence of available evidential matter; (c) the nature of the control objectives to be achieved; and (d) the expected efficiency and effectiveness of the test.

Considerations of information produced by the entity: In addition, when using information produced by RSGIB, we evaluated whether the information was sufficiently reliable for our purposes, including, as necessary, obtaining evidence about the completeness and accuracy of the information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Test procedures performed in connection with determining the operating effectiveness of controls detailed in the matrices in Section IV are described below:

Test Procedure	Description
Inspection	Inspected documents, reports, or electronic files that contain evidence of the performance of the control. This includes, among other things, inspection of client-directed documents and reading of reconciliations and management reports that age and quantify reconciling items, to assess whether balances and reconciling items are properly monitored, controlled, and resolved on a timely basis.
Observation	Viewed the application of specific controls by the Nationwide personnel
Inquiries	Interviewed the appropriate Nationwide personnel about the relevant controls

The Management Response statements, provided by the management of Nationwide, included within Section IV, are the responsibility of the management of Nationwide.

The following table (Table 1) represents the AICPA Trust Services Criteria related to Security and Availability, and the related control activities of RSGIB supporting the Retirement Solution's Governmental & Institutional Business system. Control activity references included within Table 1 map to the control activities included within Table 2.

Table 1: AICPA Trust Services Criteria and Related Control Activity Mapping

Area	Criteria	Control Activity Reference
Control Environment	1.1: The entity demonstrates a commitment to integrity and ethical values.	CC01-01.1 Code of Conduct CC01-02.1 Agreements with Service Providers CC01-03.1 Pre-Employment Screenings
	1.2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	CC01-04.1 Board of Directors Roles and Responsibilities CC01-05.1 Audit Committee CC01-06.1 Board of Directors Oversight and Independence CC01-07.1 Board of Directors and Subcommittee Boards CC01-08.1 Business Innovation Transformation Committee
	1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CC01-09.2 Organizational Structure CC01-10.1 Job Position Requirements CC01-11.1 Job Description Acknowledgement
	1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	CC01-12.1 Employee Performance Reviews CC01-13.1 Candidate Experience and Training Evaluation CC01-14.1 Background Checks and Drug Screenings
	1.5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CC01-15.1 Department Achievement of Responsibilities CC01-16.1 Management Goals and Performance Criteria

Area	Criteria	Control Activity Reference
Communication and Information	2.1: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CC02-01.3 Security Training Compliance Monitoring CC02-02.1 RSGIB Application Documentation CC02-03.1 CrowdStrike Security Alerting CC02-04.1 Security Event and Incident Review
	2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CC02-01.3 Security Training Compliance Monitoring CC02-05.1 Annual Cybersecurity Training CC02-06.1 Specified and Additional Training CC02-07.1 Subcommittee and Board of Directors Reviews CC02-08.2 Information Security Policy and Standards CC02-09.1 Information Security Policy Employee Review CC02-10.1 Reporting of Incidents CC02-11.1 Employee Information Sharing CC02-12.1 Continued Security Training CC02-13.1 Security Knowledge and Awareness Improvements
	2.3: The entity communicates with external parties regarding matters affecting the functioning of internal control.	CC02-14.1 Security and Availability Commitments CC02-15.1 External Party Incident Communication CC02-16.1 Contracting Templates with Service Providers
Risk Assessment	3.1: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CC03-02.2 ERM Risk Subcommittees CC03-03.2 Legal and Regulatory Subcommittee CC03-04.1 Operating Budgets CC03-05.2 Annual Risk Assessment CC03-06.1 Technology Risk Committee CC03-07.2 Continuity Management in Annual Risk Assessment

Area	Criteria	Control Activity Reference
	3.2: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	CC03-01.2 Enterprise Command Center CC03-05.2 Annual Risk Assessment CC03-07.2 Continuity Management in Annual Risk Assessment CC03-08.2 External Security Bulletins Review CC03-09.3 Analysis of Threats from External Bulletins CC03-10.2 Threat and Vulnerability Communication CC03-11.1 Enterprise Risk Committee Meetings CC03-12.2 Enterprise Risk Management Process
	3.3: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CC03-13.1 Fraud Risk Assessment CC03-14.1 Compensation and Performance Evaluation Program
	3.4: The entity identifies and assesses changes that could significantly impact the system of internal controls.	CC03-03.2 Legal and Regulatory Subcommittee CC03-12.2 Enterprise Risk Management Process CC03-15.1 Acquired Entity Security Assessments CC03-16.2 Third-Party Supplier Management

Area	Criteria	Control Activity Reference
Monitoring Activities	4.1: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	CC02-01.3 Security Training Compliance Monitoring CC04-01.1 Periodic Internal Audit Security Assessments CC04-02.1 Internal Audit Plan CC04-03.2 External Penetration Testing CC04-04.2 Internal Penetration Testing CC04-05.1 Independent Internal Audit Function CC04-06.1 Internal Audit Program CC04-07.1 Mix of Levels for Internal Audit Program CC04-08.1 Internal Audit Methodology CC04-10.1 Internal Audit Training and Evaluations
	4.2: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and board of directors, as appropriate.	CC04-03.2 External Penetration Testing CC04-04.2 Internal Penetration Testing CC04-09.1 Management Remediation of Findings
Control Activities	5.1: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	CC01-09.2 Organizational Structure CC03-02.2 ERM Risk Subcommittees CC05-01.1 Threat Modeling Assessment
	5.2: The entity also selects and develops general control activities over technology to support the achievement of objectives.	CC05-02.1 Procurement Methods CC05-03.2 Information Security Policy for Technology CC05-04.2 Access Control Standard CC05-05.2 Secondary ID Access CC05-06.3 Systems Development Life Cycle Methodology

Area	Criteria	Control Activity Reference
	5.3: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	CC02-08.2 Information Security Policy and Standards CC05-03.2 Information Security Policy for Technology CC05-07.1 SRB Security Policy Review CC05-08.1 Internal Audit Testing CC05-09.1 Risk Mitigation Strategy Alignment with Policies
Logical and Physical Access Controls	6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CC05-04.2 Access Control Standard CC06-01.1 Data Classification Strategy CC06-02.1 Password Configurations CC06-03.1 Password Reset CC06-04.1 Database Encryption CC06-05.1 User Access Management and Certification CC06-06.1 Single Sign on Authentication CC06-07.2 Remote and VPN Access CC06-08.1 Data In Transit and At Rest Encryption CC06-09.1 Workstation and Laptop Encryption
	6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	CC06-10.1 Quarterly Access Review CC06-11.1a Access Approvals and Manual Provisioning CC06-11.1b Access Approvals and Automated Provisioning CC06-12.2a Terminated Employees and Contractors CC06-12.2b Access De-provisioning Timeliness CC06-44.1 Workstation Administrator Access Provisioning and Deprovisioning

Area	Criteria	Control Activity Reference
	6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties to meet the entity's objectives.	CC06-14.1 Segregation of Duties – Provisioning CC06-15.1 Role-Based Security CC06-16.1 Administrative Access CC06-17.1 Management Periodic Access Reviews CC06-18.1 Job Scheduler Access CC06-20.1 Transferred User Review
	6.4: The entity restricts physical access to facilities and protected information assets (e.g., data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	CC06-19.1 Physical Security CC06-22.1 Sensitive Area Physical Access CC06-23.1 Physical Access Removal CC06-24.1 Data Center Access Review
	6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	CC06-25.1 Data Retention Procedures CC06-26.1 Digital Media Sanitization
	6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CC06-07.2 Remote and VPN Access CC06-27.1 Firewall Configurations CC06-28.1a Firewall Quarterly Review CC06-28.1b Firewall Activity Monitoring CC06-29.1 Review of Privileged Access to Firewalls CC06-30.1 Internet Access CC06-31.1 IPS and IDS

Area	Criteria	Control Activity Reference
	6.7: The entity restricts transmission, movement, and removal of information to authorized internal and external uses and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	CC06-32.1 DLP CC06-33.1 Standard Encryption Technology CC06-34.1 Transmission of Information CC06-35.1 Mobile Device Passwords and Encryption CC06-36.1 Removable Media CC06-37.1 Mobile Device Authentication and Connection
	6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	CC06-38.1 Software Installation CC06-39.1 Administrator Access on Workstations CC06-40.1 Administrator Access Review CC06-41.1 AntiMalware Technology CC06-42.1 AntiVirus Software CC06-43.1 Phishing and Spoofing Attempts
System Operations	7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities and (2) susceptibilities to newly discovered vulnerabilities.	CC03-09.3 Analysis of Threats from External Bulletins CC07-01.1 Continuous Detection for Unauthorized Components CC07-02.2 Review of Information Security Metrics Report CC07-03.1 Internal Vulnerability Scanning CC07-04.1 Computer Hardening Standards
	7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors, affecting the entity's ability to meet its objectives, anomalies are analyzed to determine whether they represent security events.	CC07-05.1 Real-Time Monitoring of Information CC07-06.2 Incident Response Policies and Escalation Plans

Area	Criteria	Control Activity Reference
	7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	CC07-07.2 Security Incident Alerting and Analysis
	7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	CC07-02.2 Review of Information Security Metrics Report CC07-06.2 Incident Response Policies and Escalation Plans CC07-07.2 Security Incident Alerting and Analysis CC07-08.2 Security Incident Response
	7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.	CC03-08.2 External Security Bulletins Review CC03-09.3 Analysis of Threats from External Bulletins CC03-10.2 Threat and Vulnerability Communication CC05-06.3 Systems Development Life Cycle Methodology CC07-08.2 Security Incident Response CC07-09.1 Workstation Updates and Testing

Area	Criteria	Control Activity Reference
Change Management	8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CC05-05.2 Secondary ID Access CC05-06.3 Systems Development Life Cycle Methodology CC08-01.1 Change Management Process and Tools CC08-02.1 Change Development and Testing CC08-03.1 Baseline Configurations CC08-04.1 Secure Development Program CC08-05.1 Change Management Procedures CC08-06.1 Secure Coding Tools CC08-07.1a Segregation of Duties – Change Management CC08-07.1b Segregation of Duties – UrbanCode Deploy Configuration CC08-07.1c Segregation of Duties – Harness Configuration CC08-07.1d Segregation of Duties – GitHub Configuration CC08-07.1e Segregation of Duties – GitHub Configuration Log Review
Risk Mitigation	9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC09-01.2 System Recovery Plans CC09-02.1 Contingency Planning CC09-04.1 Business Continuity Plans CC09-05.1 Business Impact Analysis CC09-06.1 Cyber Related Insurance

Area	Criteria	Control Activity Reference
	9.2: The entity assesses and manages risks associated with vendors and business partners.	CC03-16.2 Third-Party Supplier Management CC06-12.2a Terminated Employees and Contractors CC06-12.2b Access De-provisioning Timeliness CC09-08.1 Third-Party Risk Management Program CC09-09.1 Third-Party Vendor Information Security Policies CC09-10.1 Third-Party Monitoring CC09-11.1 Third-Party Periodic Risk Assessments
Availability	A1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	A01-01.1 Processing Capacity A01-02.2 Systems Validation and Recovery Exercise A01-03.1 Computer Operations and Job Processing A01-04.1 Traffic Management and Redundancy
	A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environments protections, software, data backup processes, and recovery infrastructure to meet its objectives.	A01-05.1 Environmental Protections Monitoring A01-06.1 Environmental Systems Maintenance A01-07.1 Environmental Protections A01-08.1 Backup and Recovery Standards A01-09.1 Production Data Backup and Replication CC03-01.2 Enterprise Command Center
	A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A01-02.2 Systems Validation and Recovery Exercise CC09-01.2 System Recovery Plans

Table 2: Nationwide's Control Activities

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC01-01.1	Code of Conduct A documented "Code of Conduct" exists and is reviewed annually by management and is acknowledged by all Nationwide associates upon their hire and reaffirmed annually thereafter.	Inspected the Office of Ethics monitoring procedures to determine that Nationwide periodically monitored the completion of required training by employees who have not completed the required Ethics Trainings. Inspected meeting minutes from the November Audit Committee meeting to determine that the Annual Ethics Report was reviewed for completion statistics and that the Code of Conduct was reviewed for appropriateness by the Governance Committee. For a selection of new and current associates, inspected supporting documentation of completed trainings to determine that the Code of Ethics Acknowledgment Disclosure was performed and acknowledged by each associate at least annually.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC01-02.1	Agreements with Service Providers Agreements are established with service providers and business partners that include clearly defined terms, conditions, and responsibilities for service providers and business partners related to system security and availability.	Inspected policy and procedures to determine that standardized and structured contracting processes were in place for contracting with third-party service providers and business partners. Inspected contracting templates to determine that clearly defined terms, conditions, and responsibilities related to security and availability were included as sections for communication as requirements from third-party service providers. Inspected the centralized storage repository for contracting templates to determine that templates for contracting and purchasing were stored centrally.	No exceptions noted
CC01-03.1	Pre-employment Screenings Pre-employment screenings are performed on contractors prior to the candidate being offered temporary employment.	Inspected the Employment Eligibility Policy to determine that criteria was established for evaluation by Nationwide prior to offering a candidate employment. For a selection of third-party contracts reviewed, obtained, and inspected the Employment Eligibility Policy to determine that acceptable and unacceptable results were documented as part of background checks conducted for contractors. For a selection of third-party personnel engaged by Nationwide, inspected the contracts to determine that contract requirements were in place to complete background checks prior to being engaged by Nationwide.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC01-04.1	Board of Directors Roles and Responsibilities The members of the Board of Directors are elected to act on behalf of the policyholders. Roles and responsibilities of the Board of Directors as outlined in the Board of Directors' Charter are segregated from the roles and responsibilities of management.	Inspected the Board of Directors Charter to determine that roles and responsibilities of the Board of Directors were documented. Inspected the membership roster for the Board of Directors to determine that the board was segregated from that of management.	No exceptions noted
CC01-05.1	Audit Committee The Board of Directors has established an Audit Committee, which meets at least five times a year, to help oversee performance of internal controls and risk management.	Inspected the Audit Committee Charter to determine that the responsibilities of the committee were established to help oversee performance of internal controls and risk management. Inspected the meeting calendar/planner for the Audit Committee to determine that the committee met up to five times annually to discuss performance of internal controls and risk management.	No exceptions noted
CC01-06.1	Board of Directors Oversight and Independence The Nationwide Board of Directors provides oversight of the strategic direction and performance of the company. The Board includes members who are independent of management of the company, and the board composition and competency is reviewed at least annually	Inspected documentation for the Governance Committee to determine that a review of independence, composition, and competency was performed annually. Inspected the membership roster for the Board of Directors to determine that the board included individuals separate from that of management. Inspected meeting minutes from the Governance Committee to determine that the Board of Directors' competency, composition, and independence were reviewed.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC01-07.1	Board of Directors and Subcommittee Boards The Board of Directors and subcommittee boards understand and acknowledge their respective charters to accept their oversight responsibilities in relation to established requirements and expectations.	For a selection of subcommittees and the Board of Directors, inspected the meeting planners to determine that the schedule included a topic around the annual review of the charter and responsibilities for the Board and subcommittees. Inspected the Board of Directors Governance Guidelines and meeting minutes to determine that annual elections and a review of membership provided acknowledgement that members accepted their responsibilities.	No exceptions noted
CC01-08.1	Business Innovation Transformation Committee Nationwide has a Business Innovation and Transformation Committee (BIT-C) governed by their respective charter that provides support to the Board of Directors on IT security items	Inspected the Business Innovation and Transformation Committee Charter to determine that the responsibilities of the committee were to provide support to the Board of Directors on IT security issues and security commitments. Inspected the meeting calendar/planner to determine that the BIT-C committee met up to five times annually to discuss key responsible areas as outlined within the charter in order to fulfill their roles. For a selection of meeting minutes, inspected the committee meeting minutes to determine the topics covered and updates discussed within the committee and with the Board of Directors were related to technology and security commitments.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC01-09.2	Organizational Structure Nationwide has an entity-wide organization chart that defines organizational structure, reporting lines and responsibilities, and authorities across lines of the business to help meet its commitments and requirements related to security and availability.	Inspected Nationwide organization charts to determine that organizational structures were defined and documented for key departments to support security and availability commitments along with providing functional separation of incompatible duties within the organization.	No exceptions noted
CC01-10.1	Job Position Requirements Upon extension of an offer, the candidate will accept their position, acknowledging their understanding of their job profile, including the requirements to fulfil the position.	For a selection of personnel hired or transferred to a new role during the period, inspected system evidence their employee file showing their job description to determine that the employees had acknowledged their understanding of their responsibilities.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC01-11.1	Job Description Acknowledgement Roles and responsibilities for external party interaction and activity monitoring are defined in written job descriptions and communicated to the suppliers through a Vendor Management System (ex: Fieldglass). The supplier acknowledges the job description as to the understanding of their responsibilities by submitting resources to the requisition in the Vendor Management System.	Inspected Nationwide's Supplier Code of Conduct to determine that the standards for external party interaction and activity monitoring were defined within the documentation. Inspected Nationwide's Contingent Worker Handbook and Guidelines to determine that the roles and responsibilities for external party interaction and activity monitoring are defined. Inspected Nationwide's Employment Eligibility document to determine that the document communicates supplier eligibility requirements. For a selection of suppliers, inspected signed Master Contingent Workforce Agreement and job requisition documentation to determine that personnel were required to sign a copy of their job description to acknowledge their understanding of their responsibilities.	No exceptions noted
CC01-12.1	Internal Audit Performance Reviews Annual performance reviews are performed for all Nationwide employees.	Inspected Nationwide's Policy Guide for performance management to determine the performance evaluation process is defined and takes place on an annual basis. For a selection of employees, inspected the annual performance evaluation to determine it was completed successfully.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC01-13.1	Candidate Experience and Training Evaluation Candidate qualifications for employment or transfer are evaluated during the hiring process to support the achievement of objectives.	For a selection of new hires and transfers, inspected evidence to determine the HR employee or hiring manager completed an interview of the candidate. For a selection of new hires and transfers, inspected evidence to determine candidate assessments were completed in the HR system.	No exceptions noted
CC01-14.1	Background Checks and Drug Screenings Prior to employment (or when required assuming a new position within the company), a background check and drug screening test are completed by Nationwide for all personnel. An eligibility matrix and compliance guide is utilized to review and evaluate requirements and results, including compliance with state and local ordinances.	Inspected the Employment Eligibility Matrix to determine that criteria was established for evaluation by Nationwide prior to offering a candidate employment. For a selection of new hires, including those with responsibility important for internal control, inspected the background checks to determine that selected personnel successfully completed background checks prior to being hired by Nationwide.	No exceptions noted
CC01-15.1	Department Achievement of Responsibilities Information Risk Management (IRM) organization holds weekly meetings to review progress of each respective department's (Business Continuity and Disaster Recovery, Identity and Access Management, Third-Party Risk Management, Information Governance, Information Security, Risk and Compliance) progress of their annual goals and objectives.	Inspected IRM's goals for FY2023 to determine that the goals existed. Observed a selection of weekly IRM Cabinet Planning JIRA cards to determine that weekly IRM meetings occurred, and tasks were associated with FY2023 goals.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC01-16.1	Management Goals and Performance Criteria Management and the Board of Directors establish measurable financial and nonfinancial goals and performance criteria that consider short-term and long-term objectives. Midyear and year-end scorecards are used to assess management against their goals and reward executives based on established criteria.	Inspected the Nationwide strategic planning documentation to determine that the Board and management establish goals and evaluate semiannually against scorecards to assess achievements against established criteria.	No exceptions noted
CC02-01.3	Security Training Compliance Monitoring Management monitors compliance with security training requirements through the Learning Management System (LMS) and sends escalation notifications to an employee's people leader for delinquent trainings.	Inspected the required security training documentation for employees and contractors to determine that the frequency of completion for required trainings has been established. For a selection of required security campaigns, inspected LMS configurations to determine that the campaigns were set-up to alert employees and their people leaders of overdue required trainings. Inspected the Operations Review documentation to determine that management reviewed and monitored compliance with security training requirements.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC02-02.1	RSGIB Application Documentation Documentation is maintained for applications supporting the description, design, and data flow of the application and is made available on Nationwide's internal collaboration tools. The application documentation is reviewed when significant changes occur to confirm the continued relevancy and accuracy.	Inspected the collaboration tools where RSGIB system documentation is located to determine that central repositories existed for retaining and describing the description, design, and data flow for in-scope applications. For a selection of in-scope RSGIB systems, inspected supporting documentation retained for the latest architecture and change release updates to determine that system documentation was retained and updated upon significant changes.	No exceptions noted
CC02-03.1	CrowdStrike Security Alerting CrowdStrike software is utilized to detect, block and alert Security Operations Center (SOC) personnel of malicious activity on endpoints. Responses to alerts from the SOC team are based on defined service level agreements.	Inspected policies and procedures for the SOC to determine that criteria outlining Service Level Agreements (SLAs) for responding to security incidents/events were established. Inspected the dashboard and system configurations within CrowdStrike to determine that the alerting mechanism was configured for notifying individuals in the event of a security event. For a selection of CrowdStrike alerts, inspected the email notifications to determine that responsible personnel were notified in the instance of a security incident.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC02-04.1	Security Event and Incident Review A monthly (internal) and quarterly (external) aggregation of security events and incidents from CrowdStrike is reported and reviewed by Operations and the vendor to determine remedial action plans.	For a selection of monthly internally identified CrowdStrike security events and incidents, inspected supporting documentation to determine the data was reported and reviewed by Operations for remediation. For a selection of quarterly externally identified CrowdStrike security events and incidents, inspected supporting documentation to determine the data was reported and reviewed by Operations and the vendor for remediation.	No exceptions noted
CC02-05.1	Annual Cybersecurity Training Employees are reminded of their roles and responsibilities through the required completion of the annual cybersecurity CBT Training.	Inspected the Nationwide Information Security Policy to determine that security and availability training was required for employees to be completed annually. Inspected Nationwide's annual Protect the Protectors CBT Training curriculum to determine that associates were required to sign and review the policy annually which states that Nationwide provides role-based training. Inspected the Learning Management System (LMS) configurations to determine that the annual Protect the Protectors training was set-up to alert employees and their people leaders of overdue required trainings. Inspected Operation Review documentation to determine that management reviewed and monitored compliance with security and availability training requirements.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC02-06.1	Specified and Additional Training Additional trainings and resources are available for specified audiences to remind them of additional roles and responsibilities they have at Nationwide.	Inspected the Nationwide Information Security Policy to determine that security and availability training was required for employees to be completed annually. Inspected the Security and Availability training curriculum to determine that the training includes an overview of their roles and responsibilities related to security and availability commitments and requirements as well as provides updates on policy changes in accordance with client requirements. Inspected Operations Review documentation to determine that management reviewed and monitored compliance with the additional security and availability training requirements. Inspected a selection of security bulletins to determine that resources such as security awareness campaigns were conducted to educate employees.	No exceptions noted
CC02-07.1	Subcommittee and Board of Directors Reviews Nationwide management subcommittees and the Board of Directors meet at least five times annually to communicate information needed to fulfill their roles with respect to the achievement of Nationwide's service commitments and system requirements.	Inspected the Board of Directors meeting calendar to determine that the Board of Directors met on a defined schedule at a minimum of five times a year. For a selection of management subcommittees, inspected the meeting minutes to determine that each committee met up to five times annually to discuss key responsible areas as outlined within the charter in order to fulfill their roles.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC02-08.2	Information Security Policy and Standards Information security policy and standards are published and available on the Nationwide intranet and communicated to all employees on a periodic basis.	Inspected the Nationwide information security policies to determine that they were established and approved by management. Inspected the required annual training curriculum completed by employees to determine that the curriculum included communication of information security policies and standards. Observed the Nationwide intranet to determine that information security policies, procedures, and controls were available to employees.	No exceptions noted
CC02-09.1	Information Security Policy Employee Review Employees are required to review the Information Security Policy upon onboarding and annually thereafter.	Inspected the Nationwide information security policies to determine that they were established and approved by management. For a selection of Nationwide associates, inspected policy acknowledgement evidence to determine that the review and attestation of the information security policy was completed.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC02-10.1	Reporting of Incidents Associates and contractors are made aware of their responsibilities to report incidents via the Information Security Policy, trainings, master service agreements, and/or the Nationwide Intranet. Customers can report potential security issues via the Nationwide On Your Side phone number or email located on the corporate website.	Inspected the Nationwide information Security Policy to determine that the policy described responsibilities for reporting security incidents. Observed the Nationwide external website to determine the incident reporting email and phone number was available. Inspected Nationwide functionality to determine that employees can submit security incidents through an internal SharePoint site. Inspected Nationwide master services agreement template to determine responsibilities for reporting security incidents was communicated to customers within the agreements.	No exceptions noted
CC02-11.1	Employee Information Sharing A SharePoint repository and other collaboration tools are available to employees and maintained to share information regarding the design and operation of Nationwide's systems.	Observed the SharePoint repository and collaboration tools to determine that repositories were used to maintain and share information regarding the design and operation of Nationwide systems.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC02-12.1	Continued Security Training Management provides continued training about its security commitments and requirements for personnel to support the achievement of objectives.	Inspected the listing of trainings employees and contractors are required to complete to determine that the trainings are made available by management to achieve security commitments. Inspected the Security and Availability training curriculum to determine that the trainings include an overview of their roles and responsibilities related to security and availability commitments and requirements as well as provides updates on policy changes in accordance with client requirements. Inspected the IRM training dashboard to determine that completion of security trainings by employees and contractors was monitored and reviewed by Operations.	No exceptions noted
CC02-13.1	Security Knowledge and Awareness Improvements Nationwide provides user guides, security alerts, and known issues on the Nationwide website and customer portal with information to improve security knowledge and awareness.	Inspected a selection of Nationwide's user guides, security alerts, and known issues on the customer portal and Nationwide website to determine that user guides and a history of security alerts and known issues with information to improve security knowledge and awareness were available.	No exceptions noted
CC02-14.1	System Objectives Nationwide provides relevant communications related to system objectives to business partners.	Inspected agreement templates to determine that system objectives were included as terms for communication with external parties. For a selection of RSGIB agreements created and modified, inspected the terms to determine that system objectives were included as terms for communicating with external parties.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC02-15.1	External Party Incident Communication Nationwide communicates security and availability incidents to external parties based upon state statutes in the event that logical security, physical security, or system availability incident impacts client data or delivery of services.	Inspected the Nationwide Event Management Program Policy to determine that procedures were defined for assisting with the identification, reporting, and resolution of security and availability incidents. Inquired with management and was informed that there have not been any security or availability incidents during the audit period that resulted in incident disclosure based on established policies and guidelines. Inspected security event documentation to determine that there were no events that rose to the level of incident disclosure, as required by state law, to external parties.	Unable to conclude. We were informed that, and confirmed through inspection of event documentation, that there were no incidents that required communication to external parties during the testing period, therefore no testing was performed.
CC02-16.1	Contracting Template with Service Providers Master service agreement (MSA), Statement of Work (SOW), and Purchase Order agreement (PO) templates are established for consistency and are communicated through Nationwide's intranet for business leaders when contracting with service providers and business partners.	Inspected the storage repository for contracting templates to determine that MSA, SOW and PO templates for contracting and purchasing were stored centrally and were available for use by Nationwide business units. Inspected training course materials taken by Nationwide employees within business units to determine that the contract template locations were communicated to Nationwide employees for use.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC03-01.2	Enterprise Command Center The Enterprise Command Center (ECC) operates continuously (24/7) to monitor the health and availability of technology systems and services. Incidents potentially affecting the availability of systems are initiated by the ECC, who then collaborates with various Nationwide Technology groups for resolution.	Inspected incident policies and process documentation to determine that formal processes were established to define roles and responsibilities and monitor availability incident response based upon defined SLA timelines. For a selection of availability incidents, inspected the resolution documentation to determine that the incident was acknowledged and resolved within the defined SLA timeline.	No exceptions noted
CC03-02.2	ERM Risk Subcommittees Nationwide has defined a formal Enterprise Risk Management process that identifies Nationwide Technology operational and financial risks, which includes security and availability commitments, relevant to achieving corporate objectives through various ERM risk subcommittees that convene on a periodic basis.	Inspected ERM policies to determine that formal processes and policies were in place to identify risks associated with security and availability objectives. Inspected the ERM organizational structure to determine that the reporting of subcommittee lines within the ERM process were established and defined. For a selection of subcommittees within the ERM landscape, inspected the meeting minutes to determine that financial and operational risks were discussed within the committee monthly meetings.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC03-03.2	Legal and Regulatory Subcommittee Nationwide reviews regulatory and compliance requirements as identified by the Legal and Regulatory subcommittee and monitored by Information Risk Management to help ensure the internal control environment is in compliance with the prescribed requirements.	Inspected Risk Committee Structure and Policy Alignment documentation to determine that compliance committees and groups were formed. For a selection of Legal and Regulatory subcommittee meetings, inspected the meeting minutes to determine that legal and regulatory compliance requirements were assessed and reviewed. Inspected email-alerting configurations for the NAIC (National Association of Insurance Commissioners) Working Group to determine that Nationwide subscribed to alerts or mailouts from regulatory bodies. For a selection of NAIC Work Group meetings, inspected the meeting materials to determine that compliance requirements with the NAIC were assessed and reviewed.	No exceptions noted
CC03-04.1	Operating Budgets Management conducts an annual meeting to allocate operating budgets related to security and availability and reviews current spend to budget monthly.	Inspected a selection of monthly Information Risk Management Financial Results meetings to determine that IRM meets monthly with financial controllers to discuss current spend to budget.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC03-05.2	Annual Risk Assessment Nationwide management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the Board of Directors. The objectives incorporate the service commitments and system requirements of the business unit along with financial and operational objectives. The risks are assessed annually through a survey sent to subcommittee leadership personnel to identify changes in underlying threats or in the environment that would require an update to assessed risks.	Inspected the annual Emerging Risks and Risks Survey sent out to subcommittee members to determine that the risk landscape is assessed, and risk inventory updated for relevant risks each year. For a selection of quarterly EORC meetings, inspected the meeting minutes to determine that the top risks resulting from the risk landscape surveys were reviewed. Inspected the annual risk assessment presented at the Board of Directors meeting to determine that the risk assessment includes the risks surrounding key service commitments and security requirements for security and availability.	No exceptions noted
CC03-06.1	Technology Risk Committee The Technology Risk Committee and the Enterprise Operational Risk Committee provide oversight over Nationwide Technology Resiliency and System Availability in order to minimize related business disruption and improve Nationwide Technology's resilience posture.	Inspected the annual risk assessment documentation to determine that the risk assessment process included consideration of the service commitments and system requirements including for availability commitments. Inspected TRC and EORC documentation to determine that the committee existed, reported up to the EORC and regularly met to minimize business disruption and improve business resiliency.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC03-07.2	Continuity Management in Annual Risk Assessment As part of the annual risk assessment process, Governance, Risk, and Compliance (GRC) performs analyses on scenarios to address availability and resiliency risks.	Inspected the annual risk assessment documentation to determine that the risk assessment process included consideration of the service commitments and system requirements related to availability and resiliency risks. Inspected risk assessment documentation for a selection of TRC meetings to determine that the evaluation of resiliency and availability risks were identified and prioritized to drive maturity and improvements in the Business Resiliency Domain.	No exceptions noted
CC03-08.2	External Security Bulletins Review Vulnerability Management (Vulnerability Response) subscribes to external security bulletins from vendors of their IT products to stay aware of new vulnerabilities and the Threat Intelligence Team collects new threats as per the threat intelligence procedure.	Inspected email communications to the Vulnerability Response Team to determine that alerts and were set up from external bulletins.	No exceptions noted
CC03-09.3	Analysis of Threats from External Bulletins Security vulnerabilities and threats identified from external bulletins are analyzed and communicated to the Vulnerability Response Team and Advisory Representatives of potential impacted areas for assessments and modeling.	For a selection of alerts from external bulletins, inspected supporting documentation to determine that the risk of newly discovered threats was assessed and communicated to the Vulnerability Response Team and Advisory representatives.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC03-10.2	Threat and Vulnerability Communication Weekly digests of threats and vulnerabilities captured by internal and external monitoring are communicated to key personnel within the Information Technology department.	Inspected the Threat Intelligence work procedure to determine that the CSOC team analyzed and reported out results of threat monitoring to key personnel. For a selection of weekly threat and vulnerability digests, inspected email communications to determine that external monitoring results and recommendations were communicated to key personnel.	No exceptions noted
CC03-11.1	Enterprise Risk Committee Meetings Monthly, Nationwide's Technology Risk Committee meets to discuss strategic, financial, and operational technology risk considerations critical to the business based upon the annual Security Risk Assessment results.	Inspected the Enterprise Information Security Risk Assessment (SRA) 2023 Summary Results to determine that the results were incorporated into goals and objectives for subcommittees. Inspected a selection of monthly meeting minutes from Nationwide's Risk Committee charter for the Technology Risk Committee to determine that key technology risks, as identified in the SRA, were reviewed.	No exceptions noted
CC03-12.2	Enterprise Risk Management Process Nationwide has defined a formal Enterprise Risk Management process that identifies risks relating to achievement of corporate objectives, among other risks, through subcommittees where the top risks are documented and reported out to the Board of Directors on an annual basis by means of an ORSA report.	Inspected the Nationwide Enterprise Risk Management and Global Risk Management policies to determine that the policies defined a formal risk management process for aggregating and reporting on security and availability risks. Inspected a selected ORSA report to determine that a risk assessment of Nationwide's top risks was performed, and results were analyzed and reported out to the Board of Directors.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC03-13.1	Fraud Risk Assessment Management conducts a fraud risk assessment on product lines and business areas with at least one assessed high inherent risk at least once every 24 months, and other product lines and business areas at least once every 36 months.	Inspected the Enterprise Fraud Risk Assessment Standards to determine that the Standards existed and that they outlined the procedures for conducting fraud risk assessments. Inspected a selected copy of RSGIB's fraud risk assessment to determine that a fraud risk assessment occurred.	No exceptions noted
CC03-14.1	Compensation and Performance Evaluation Program The Board of Directors, Audit Committee, and management review the Nationwide's compensation and performance evaluation programs annually to identify potential incentives and pressures for employees to commit fraud.	Inspected the Enterprise Anti-Fraud Policy and Fraud Risk Assessment Standard to determine that policies and procedures were documented to combat fraud activities. Inspected HR Committee meeting minutes and Audit Committee meeting minutes to determine that a compensation and fraud were reviewed annually.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC03-15.1	Acquired Entity Security Assessments Global Information Security performs security assessments on newly acquired entities to identify and manage relevant security risks.	Inspected the IRM Mergers and Acquisitions process documentation to determine that activities were established for reviewing security practices of entities involved in a merger/acquisition. Inspected the security questionnaire template to determine the subject areas, IT considerations, and risk profiles measured for security and availability risks with the entity. Inquired with management regarding mergers and acquisitions during the period to determine that no mergers or acquisitions occurred for security and availability risks to be identified and tracked toward remediation. Inspected Finance Committee meeting minutes for the period to determine that no mergers or acquisitions occurred during the period.	Unable to conclude. We were informed that, and confirmed through inspection of Finance Committee meeting minutes, there were no mergers or acquisitions which occurred during the testing period, therefore no testing was performed.

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC03-16.2	Third-Party Supplier Management Policies and procedures are in place to review and manage the Third-Party suppliers and service providers, which includes but is not limited to a general assessment and security assessments.	Inspected the Nationwide Enterprise Supplier Risk Management Policy to determine that policies and procedures were in place to review and manage third-party suppliers/service providers. Inspected the supplier risk questionnaire template to determine that factors and assessment criteria were established for risk ranking a third-party supplier and service provider. Inspected the Ariba assessment configuration for suppliers to determine that requirements were set to enforce a general assessment and a scheduled recertification. For a selection of suppliers, inspected the general assessment performed, to determine that the assessment was completed and recertification dates were set.	No exceptions noted
CC04-01.1	Periodic Internal Audit Security Assessments The internal audit department performs periodic audits to include information security assessments.	Inspected the Internal Audit Planning and Risk Assessment Policy, the Internal Audit methodology documentation regarding the annual audit universe risk assessment and supporting documentation from the Internal Audit update to the Audit Committee presentation to determine that the documentation included information security assessments.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC04-02.1	Internal Audit Plan On a quarterly basis, Internal Audit develops an internal Audit Plan based on the key risks identified during the risks assessment process and communicates the Plan to the Audit Committee.	Inspected the Nationwide Internal Audit Planning and Risk Assessment Policy and the Internal Audit Entities Report, completed audit plan, and report summary to determine that Internal Audit performs periodic audits of Nationwide's internal control environment. Inspected a selection of Audit Committee meeting minutes to determine that the progress of audits performed for the current year and the internal audit plan was communicated to the Audit Committee.	No exceptions noted
CC04-03.2	External Penetration Testing Nationwide engages an outside vendor to perform continuous penetration testing and monitoring on their environment. Identified issues are raised to Nationwide and tracked to resolution in the GRC tool.	Inspected system evidence on the third-party portal to determine that penetration testing issues were logged and reported to Nationwide. Inspected the third-party contract to determine that the scope of work, responsibilities, and commitments for 24/7 penetration monitoring were established. For a selection of externally reported penetration testing issues, inspected supporting documentation from the GRC tool to determine that the testing issues were worked and tracked toward resolution.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC04-04.2	Internal Penetration Testing Nationwide performs internal penetration testing and produces a report with results and recommendations that is communicated to ISRM and business unit leaders for remediation.	For a selection of internal penetration testing reports, inspected system evidence within the GRC tool repository to determine that penetration testing issues were logged for resolution by Nationwide. For a selection of internally identified penetration testing issues, inspected supporting documentation from the GRC tool to determine that the testing issues were logged, communicated to ISRM and the business unit, worked and tracked toward resolution.	No exceptions noted
CC04-05.1	Independent Internal Audit Function An internal audit department exists that is independent of management.	Inspected the organizational chart of Nationwide noting the organizational chart described functional areas and reporting structures within functional areas, including Internal Audit, to determine that reporting hierarchies were defined to maintain independence between management and Internal Audit. Inspected the internal audit department policies to determine that policies are established to govern the Internal Audit functional area's responsibilities.	No exceptions noted
CC04-06.1	Internal Audit Program Internal audit developed audit programs that include a mix of manual and automated controls, as well as preventive and detective controls, to mitigate risks identified during the risk assessment and engagement scoping processes.	For a selection of audit programs, inspected to determine that Internal Audit identified the risks and relevant controls to be assessed that included a mix of control assessments.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC04-07.1	Mix of Levels for Internal Audit Program Internal audit developed and executed audit programs that include oversight from various levels of management.	Inspected the Internal Audit Policy to determine that there were requirements for audit programs, including for various levels of management. For a selection of audit programs for relevant audits on the audit plan, inspected the audit activity involvement documentation to determine that test work was reviewed and approved in accordance with established policies.	No exceptions noted
CC04-08.1	Internal Audit Methodology Internal Audit performs audit/advisory procedures using a formal methodology, documents their procedures and results in the GRC tool, and prepares audit/advisory reports summarizing the engagement scope, findings, and an overall opinion on the control environment.	Inspected internal audit methodology, including the Risk Assessment Diagram including requirements for planning, execution, and reporting, and based on standards established in the Internal Audit Policy to determine that a formal methodology is established and documented. For a selection of internal audits performed, inspected documentation to determine that the documentation complied with the defined methodology and that results were documented and discussed with members of management and the Audit Committee.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC04-09.1	Management Remediation of Findings Management is responsible for responding to all issues identified by Internal Audit. Management may decide to either mitigate or assume each issue, based on issue ratings and management level. Management tracks the issues they own and communicates status of remediation activities to relevant stakeholders on a periodic basis. All assumed issues require annual reassessment to decide whether to mitigate or reassume. All issues are monitored by Internal Audit and escalated as necessary and considered for aggregation risk.	For a selection of Nationwide Internal Audit assessments, inspected the internal audit reports to determine that the reports included findings and recommendations and were shared with management. For a selection of Internal Audit reports, inspected the report summary and communication evidence to determine that the report described the open audit findings, and the report was shared with Nationwide management used to monitor remediation activities. Inspected the issue tracking log within the GRC tool for the findings from the selection of Internal Audit reports determine that the findings were tracked, remediation statuses monitored and communicated on a periodic basis to stakeholders. Observed management's GRC tool to determine findings and remediation activities from audits and internal assessments were tracked and escalated.	No exceptions noted
CC04-10.1	Internal Audit Training and Evaluation Trainings are required for internal audit personnel to continually review and confirm competency of personnel. Additionally, after each engagement, there is a Performance Audit Evaluation criterion for auditors to provide coaching and feedback to each other.	Inspected training logs for a selection of internal audit personnel to determine that trainings were completed as required. Inspected post audit evaluations for a selection of internal audit assessments performed to determine that post audit evaluations were prepared, reviewed, and discussed with members of the engagement for feedback and coaching.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC05-01.1	Threat Modeling Assessment On a bi-annual basis, management performs a threat modeling assessment to identify modes and methods of various threats. Observations from the assessment are analyzed on a heat map and remedial actions are determined and communicated out to leadership in Cybersecurity Operations Center (CSOC), Business Teams, Information Risk Management (IRM), and the Business Innovation and Transformation Committee (BITC) for implementation.	Inspected Threat Intelligence Procedure documentation to determine that Nationwide designed a policy requiring that threat modeling be performed and communicated to designated groups. For the 2023 mid-year assessment, inspected threat modeling assessment supporting documentation to determine that Nationwide performed a threat modeling assessment to identify modes, methods, and remedial actions for various threats. For a selection of weeks, inspected the threat and CSOC activity digests to determine that Nationwide communicated and distributed threat intelligence literature and leading practices to respective representatives.	No exceptions noted
CC05-02.1	Procurement Methods Nationwide employs organization-wide make or buy strategies and procurement methods for the purchase, development, and maintenance of information systems, system components, or information system services from technology suppliers.	Inspected the Source to Pay policy and Make or Buy strategy procedure to determine that acquisition, procurement from suppliers, and development strategies were established.	No exceptions noted
CC05-03.2	Information Security Policy for Technology Nationwide's information security policy and standards addresses controls over significant aspects of Nationwide Technology Operations.	Inspected the Information Security policy to determine that it included section headings that addressed controls over the significant aspects of system operations.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC05-04.2	Access Control Standard Nationwide's Access Control Standard addresses and requires formal user provisioning and deprovisioning procedures, limiting privileges/rights (least privileged), use of passwords, activity logging, and periodic user access reviews.	Inspected the User Access management policies to determine that the policies described requirements for formal user registration and de-registration, limiting privileges/rights, use of passwords, activity logging and periodic users' access reviews.	No exceptions noted
CC05-05.2	Admin Privileges via Privileged Identity Shared ID Administrative privileges are controlled through the Privileged Identity tool and are managed through a checkout process.	Inspected Privileged Identity password access configurations to determine that password checkout was enabled, and the maximum password checkout duration defaulted to 10 hours and a maximum duration of 20 hours. Inspected the Privileged Identity Account Permissions web page for a selection of users to determine that the users were only able to view and check out a password for IDs assigned to their Active Directory account. Observed a user attempt to extend the check out more than twice (greater than 20 hours) to determine that Privileged Identity denied the attempt.	No exceptions noted
CC05-06.3	Systems Development Life Cycle Methodology Nationwide has adopted a formal security and systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, maintenance, and disposal or decommissioning of computerized information systems and related technology requirements.	Inspected the Secure Application Development IT Standard to determine that formalized security and systems development methodology were established.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC05-07.1	SRB Security Policy Review Information security policy and standards are reviewed via SRB meetings at least annually.	For a selection of information security policies and procedures, inspected the review and revision history to determine the policies defined controls and were reviewed and approved by the Standards Review Board on an annual basis.	No exceptions noted
CC05-08.1	Internal Audit Testing Internal Audit performs testing over the design and operating effectiveness of controls in accordance with the internal audit plan.	Inspected the Nationwide Internal Audit schedule to determine that Internal Audit performs periodic audits of Nationwide's internal control environment. For a selection of Internal Audit assessments, inspected the Internal Audit Control Log and internal audit reports to determine that the reports included findings and recommendations related to the design and operating effectiveness of controls.	No exceptions noted
CC05-09.1	Risk Mitigation Strategy Alignment with Policies Nationwide's policy and procedure manuals are reviewed annually by the Owner and Lead Practitioner for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy.	Inspected the Information Security policy and the SRB charter to determine that policies and processes existed for reviewing and incorporating updates within policies based on the risk mitigation strategy. Inspected documentation of the annual review of the policy and procedures manuals by the Owner and Lead Practitioner to determine that manuals are reviewed at least annually, and updates are made as necessary.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-01.1	Data Classification Strategy Nationwide has an information classification strategy for the labeling and handling of data to help ensure that data is classified, secured, and restricted to authorized personnel. Data classification is in five levels: public, internal, private, sensitive personal, and restricted. 1/1/2023 – 5/31/2023 The above process was performed A central metadata repository to track and inventory information about data elements is maintained. 6/1/2023 – 12/31/2023 The above process was performed using BigID to identify and classify data.	Inspected the Nationwide Information Classification Standard to determine that restrictions are established for how data is used, secured, and restricted as Public, Internal, Non-public, Sensitive Personal, and Restricted. 1/1/2023 – 5/31/2023 Inspected the five-point Nationwide Governance Catalog to determine that procedures are in place to identify, capture, and track metadata data according to the Nationwide Information Classification Standard. 6/1/2023 – 12/31/2023 For a selection of in-scope databases, inspected BigID scanning configurations and sample scan results to determine database scanning is in place to identify, capture, and track metadata according to the Nationwide Information Classification Standard.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-02.1	Password Configurations Passwords for in-scope systems are configured according to password policies defined in the Access Control Standard, including for remote access authentication, including: • Password history • Account lockout • Length requirement • Password expiration • Password complexity	Inspected Nationwide's password policy to determine that password configurations were established as requirements for Nationwide Technology systems. Inspected Active Directory SSO configuration evidence to determine the in-scope applications that were configured to authenticate through Active Directory. Inspected the Active Directory Default Domain Policy password configuration to determine that for the in-scope applications with single sign-on (SSO) set, the passwords were configured to comply with company policy. Inspected the password configurations for the in-scope applications not configured to authenticate through Active Directory SSO to determine that passwords were configured to comply with company policy.	No exceptions noted
CC06-03.1	Password Reset New users are required to change their password upon first logon to their Nationwide computers.	Inspected the Nationwide Information Security Policy and the Identifications and Authentication IT Security Standard to determine that users are required to reset passwords upon first logon to their Nationwide computers. Inspected the password reset configuration to determine that the in-scope applications are configured to force a new user to reset their password upon first logging into their computer. Observed the setup of a new user account to determine that the account was configured to force a password reset upon first logon.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-04.1	Database Encryption Databases housing sensitive customer data are encrypted at rest.	Inspected the Nationwide Data Protection IT Security Standard to determine that encryption requirements were established for databases housing sensitive customer data at rest. Inspected system evidence of encryption configurations for a selection of databases to determine that encryption standards and protocols were in place for each type of storage drive, module, and backup domains.	No exceptions noted
CC06-05.1	User Access Management and Certification Nationwide has in place multiple tools and software to support user access management and certification including: a) SailPoint IIQ – identity and access management solution for user access management and certification b) Lieberman (PIDM) – password vault for privileged access, including shared IDs	Inspected access control policies and work procedures to determine that Nationwide established multiple tools and software to support user access management and certification including SailPoint IIQ and Lieberman (PIDM). Observed configurations within each user identity management tool to determine that the tools are configured to support user access management and certification.	No exceptions noted
CC06-06.1	Single Sign-On Authentication Active Directory Group Policy is utilized to enforce global security policies and authenticate users to Nationwide's systems via single sign-on (SSO).	Inspected Active Directory SSO configuration evidence to determine that certain in-scope applications were configured to authenticate through Active Directory. Inspected the Active Directory Default Domain Policy password configuration to determine that for the in-scope applications with single sign-on (SSO) set, the passwords were configured to comply with company policy.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-07.2	Remote and VPN Access Multifactor authentication (MFA) mechanism is utilized for remote and virtual private network (VPN) access to Nationwide system components.	Inspected Nationwide's Access Control IT Security Standard to determine that a requirement for multifactor authentication (MFA) mechanism was established for remote and virtual private network (VPN) access. Inspected configuration settings for MFA and VPN to determine that remote and virtual access to Nationwide system components was enabled and secured. Observed as a user logged into Nationwide production systems through a virtual private network (VPN) on their laptop device to determine that multifactor authentication (MFA) was enforced.	No exceptions noted
CC06-08.1	Data In Transit and At Rest Encryption Nationwide enforces encryption requirements for data in transit and at rest when such protections are deemed appropriate based on assessed risk. Encryption keys are maintained separately from the protected data.	Inspected the Nationwide Guidelines for the Use of Encryption and Security Guidelines for Certificate Management to determine management has defined procedures for key generation, storage, use and destruction. Inspected system evidence to determine that encryption keys are maintained in a separate location from the protected data. Inspected the encryption evidence for a selection of confidential email communications to determine that encryption standards were enforced.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-09.1	Workstation and Laptop Encryption Storage encryption software is installed on employee workstations and laptops.	Inspected the Nationwide Information Security Policy to determine that a process to encrypt employee workstations and laptops was defined. Inspected the Nationwide Information Classification Standard to determine that data was classified. Inspected configuration profile policies set within the system to determine that the policies were enabled to enforce encryption for a workstation connected to the Nationwide network, whether directly or through VPN. Observed an employee's laptop running on Windows and on Mac operating systems to determine that the laptops were protected by full disk encryption.	No exceptions noted
CC06-10.1	Quarterly Access Review Management performs a quarterly access review for the in-scope system components to help ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected Review Certification Procedural documentation to determine that process details were established for the performance, documentation, and resolution of the periodic user access certifications. For a selection of periodic reviews, inspected system evidence of the schedule and configuration for the SailPoint IIQ tool to determine that the reviews were configured to initiate based on a set of conditions and rules for the supervisor/manager, PIDM, and shared ID reviews.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-11.1a	Access Approvals and Manual Provisioning When a user submits a provisioning request in SailPoint IIQ, the system automatically routes it to the appropriate approvers and management provisions access as requested.	Inspected the provisioning approval workflow to determine that SailPoint IIQ user access requests are configured to route to the designated approvers. For a selected user access request, inspected system evidence to determine that the SailPoint IIQ access requests are automatically routed to the designated approvers. For a selection of new users, inspected access request to determine that management approved the users before access was granted, and that access was granted as authorized.	No exceptions noted
CC06-11.1b	Access Approvals and Automated Provisioning When a user submits a provisioning request in SailPoint IIQ, the system automatically routes it to the appropriate approvers and provisions access as requested.	Inspected the provisioning approval workflow to determine that SailPoint IIQ user access requests are configured to route to the designated approvers. For a selected user access request, inspected system evidence to determine that the SailPoint IIQ access request was automatically routed to the designated approvers, and access was automatically provisioned as requested.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-12.2a	Terminated Employees and Contractors Work items in SailPoint IIQ are automatically created based on users' termination date entered within Workday (for employees) or Boss (for contractors) to automatically de-provision Active Directory access and initiate the system de-provisioning process.	Inspected the terminated user workflow configuration to determine SailPoint IIQ creates de-provisioning work items and disables Active Directory access in accordance with the termination date from Workday/Boss. For a selected terminated employee and contractor, inspected system evidence to determine SailPoint IIQ automatically created a work item based on the users' termination date from Workday/Boss and disabled Active Directory access.	No exceptions noted
CC06-12.2b	Access De-provisioning Timeliness Access privileges are disabled or removed for terminated employees and contractors in a timely manner.	For a selection of terminated employees and contractors, inspected termination work items and system access listings to determine that access privileges are disabled or removed within a timely manner.	No exceptions noted
CC06-14.1	Segregation of Duties – Provisioning Nationwide has designed application-enforced segregation of duties to define what privileges are assigned to users within applications.	Inspected a system-generated listing of users with access to develop changes and compared the users to a system-generated listing of users with access to migrate changes to the production environment to determine that systematic segregation of duties was in place. Inspected the SailPoint IIQ provisioning configuration to determine that segregation of duties existed between requestor and approver within the provisioning of user access. For a selection of user access provisioned, inspected SailPoint IIQ workflow history evidence to determine that segregation of duties between requestor and approver existed to obtain approval.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-15.1	Role-Based Security Nationwide establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles.	Inspected the Information Security Policy and the Access Control IT Security Standard to determine that Nationwide establishes and administers privileged user accounts in accordance with a role-based access scheme. Inspected support documentation of the periodic manager, shared ID and privileged ID certifications to determine that role-based access was used.	No exceptions noted
CC06-16.1	Administrative Access Users with administrative access to systems are appropriate based on job responsibility.	Inspected system generated listings of individuals with administrative access for in-scope systems to determine that access was restricted based on the individuals' current job responsibilities. Additional Procedures: For the identified user with inappropriate DCDirect (RP Link) administrative level access, inspected system evidence to determine that 1) Access was removed 2) The user did not access DCDirect (RP Link) during the period the access was held	Exception noted. KPMG noted that 1 of 24 DCDirect (RP Link) administrative accounts had access that was not commensurate with their job responsibilities. No exceptions noted for other relevant systems. Additional Procedure Results: No exceptions noted.
Management's Response: Management identified that one business user had inappropriate administrative access to the DCDirect (RP Link) application. Management noted that access was inadvertently provisioned and remediated the access by removing administrative access from the user. Additional procedures included inspection of the DCDirect (RP Link) application log history and last login details for the identified user. As a result, management confirmed that no transactions were performed with the administrative access.			

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-17.1	Management Periodic Access Reviews Management performs quarterly access reviews for the in-scope system components (application, operating system, and database) to monitor the appropriateness of access. Access is removed from users marked for revoke in a timely manner. a) Manager certification b) Shared ID certification c) Privileged ID Management certification	For a selection of quarters, inspected the supporting documentation for the manager, shared ID, and privileged ID certifications to determine that system access was reviewed. For a selection of changes identified in the periodic access reviews, inspected system generated evidence to determine that changes to access permissions noted by management were implemented.	No exceptions noted
CC06-18.1	Job Scheduler Access Access to schedule and execute jobs through the job scheduling applications is restricted to appropriate personnel.	Inspected system evidence of the job scheduler tool to determine the security groups that were permitted for updating the job schedule/configuration/settings. Inspected system generated listings of users with access to update the job schedule to determine that access was restricted to authorized personnel based upon current job responsibilities from the company organizational chart.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-19.1	Physical Security Nationwide provides physical security in accordance with documented procedures. This includes a combination of some of the following measures: 24x7 security guards in the facilities, 24x7 monitoring video surveillance (CCTV), and badge (card) readers at all entrances.	Inspected the Nationwide physical security policies to determine that policies were in place describing requirements for security guards, monitoring video surveillance, badge readers, and biometric readers. Observed the Nationwide office to determine that security guards were present, monitoring of video surveillance was performed, and badge readers were required to access restricted areas.	No exceptions noted
CC06-20.1	Transferred User Review When a user changes role within the organization, the new people leader must complete an Internal Transfer Certification review within 28 days to assess prior system access.	For a selection of transferred users, inspected the Internal Transfer certification review to determine that new people leaders complete the access review within 28 calendar days of receiving the notification, or the user's prior non-birthright access was revoked.	No exceptions noted
CC06-22.1	Sensitive Area Physical Access Physical access to sensitive areas (including data centers) is restricted to users based on job responsibilities. Only approved users are granted access to the facilities.	Inspected the Physical and Environmental IT Security Standard to determine that policies and standards were in place to govern physical access to sensitive areas, including data centers. Inspected the data center physical security listing to determine that data center physical access was restricted to authorized personnel based on job functions from the company organizational chart. For a selection of new hires, inspected access request forms for data center access to determine that the access provisioning request was approved prior to access being provisioned.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-23.1	Physical Access Removal Physical access is removed within seven days upon termination.	For a selection of terminated employees, inspected the physical access listing subsequent to the time of the termination to determine that access to the Nationwide in-scope facilities was removed upon termination.	No exceptions noted
CC06-24.1	Data Center Access Review Access to the data centers is reviewed monthly by management in accordance with documented policies/procedures.	For a selection of months, inspected the results of the physical access security reviews to determine that physical access to the in-scope facilities was reviewed and approved by management. For a selection of access changes identified during the review, inspected the current physical access listings to determine that access was changed according to the results of the review.	No exceptions noted
CC06-25.1	Data Retention Procedures Formal data retention and disposal procedures are in place to guide the secure disposal of NW's and customers' data.	Inspected data retention and disposal policies and procedures to determine that formalized processes were established for the disposal of Nationwide Technology assets and data record retention.	No exceptions noted
CC06-26.1	Digital Media Sanitization Prior to removal from NW facilities, digital media is completely degaussed and sanitized to remove any data and software.	Observed the PCaaS portal to determine that a mechanism existed for tracking and inventorying of digital media assets, including their statuses. For a selection of retired digital media assets, inspected vendor audit reports to determine that the assets were degaussed and sanitized prior to disposal.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-27.1	Firewall Configurations System firewalls are configured to limit unnecessary ports, protocols, and services. The only ports open and allowable into the environment are defined.	Inspected the Configuration Management IT Security Standard to determine that policies were established to require firewalls to be configured to limit unnecessary ports, protocols, and services. For a selection of in-scope systems, inspected the firewall rules for CISCO Asa and Palo Alto to determine that firewalls were configured to limit ports, protocols, and services in accordance with management's standards.	No exceptions noted
CC06-28.1a	Firewall Annual Review Firewalls on the Nationwide network are configured based upon baseline ruleset standards. Management performs a quarterly review of the firewall secure configuration and firewall rulesets.	Inspected the Firewall Rule Review Policy to determine that firewall rule sets were to be reviewed and updated quarterly. Inspected the firewall ruleset criteria to determine that in-scope firewalls were measured against the criteria and included within the quarterly firewall review. For a selection of quarters, inspected the firewall rule set review documentation to determine that management reviewed and approved the firewall rule sets and performed updates where necessary.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-28.1b	Firewall Activity Monitoring Ingress firewalls are monitored to help ensure inbound connections are being properly filtered by an approved Web Application Firewall Policy. Ingress firewall activity is reported to Nationwide's Board of Directors on a quarterly basis.	Inspected ingress firewall configurations to determine that connections were filtered as authorized or blocked by the Web Application Firewall policy. Inspected a selection of WAF rule exceptions to determine that they were approved by management. For a selection of quarters, inspected the Board of Directors meeting documentation to determine that ingress firewall monitoring results and statuses were communicated.	No exceptions noted
CC06-29.1	Review of Privileged Access to Firewalls Management performs a quarterly review of privileged access to firewalls to confirm access is appropriate based upon job responsibility.	Inspected the Access Control IT Security Standard to determine that privileged access to firewalls is to be reviewed on a quarterly basis. For a selection of quarters, inspected the privileged firewall access review to determine that management reviewed users assigned privileged firewall access and implemented corrective actions where necessary.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-30.1	Internet Access Internet access is strictly controlled to only approved external web sites on company assets that have access to customer data.	Inspected system configuration policies from the Zscaler web proxy to determine that category content filtering and web categories (Dating and Personals, File Sharing, etc.) were configured to be blocked. Observed an attempt to access a blocked website to determine that the attempt was not permitted. For a selection of quarters, inspected the firewall rule set review to determine that management reviewed and approved the firewall rule sets and performed updates where necessary. Inspected ingress firewall configurations to determine that connections were filtered as authorized or blocked by the Web Application Firewall policy.	No exceptions noted
CC06-31.1	IPS and IDS Intrusion detection/prevention systems (IPS/IDS) are utilized to monitor, detect, and prevent unauthorized access to external connection attempts to Nationwide's network.	Inspected baseline server configurations for Palo Alto IDS/IPS to determine that the system was enabled to inspect inbound traffic. Inspected the DDoS response team procedures to determine that a triage, mitigation and response strategy was defined as DDoS attacks were identified. Inspected the Zscaler configuration to determine that the tool was enabled for web filtering and prevents users from accessing certain sites based on their categorization.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-32.1	DLP A DLP solution is implemented and used to scan for sensitive information in outgoing transmissions over public communication paths.	Inspected the configuration of the Microsoft Cloud Application Security (MCAS) to determine that the tool was enabled to monitor connected applications and scan for sensitive information. For a selection of email alerts for multiple types of technologies monitored, inspected system evidence to determine that sensitive information transfer was prevented and triggered alerts were communicated to the user.	No exceptions noted
CC06-33.1	Standard Encryption Technology Nationwide uses industry standard encryption technology, VPN software, or other secure communication systems for the secure transmission information over public networks.	Inspected the Nationwide Guidelines for the User of Encryption Standard, the Data Protection IT Security Standard, and the Identification and Authentication IT Security Standard to determine that procedures were in place for communicating private or confidential information through a secured messaging service. Inspected configuration settings for MFA and VPN to determine that remote and virtual access to Nationwide system components was enabled and encrypted. Observed an employee send an email to an address outside of the Nationwide network to determine that the email was sent through a secured messaging service as information was classified as private or confidential. Observed an employee remotely access the Nationwide network while on a public network to determine that an encrypted VPN connection was utilized to access the Nationwide network.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-34.1	Transmission of Information Secure file transfer protocols (SFTP) are deployed for transmission of confidential and/or sensitive information over public networks.	Inspected Nationwide IT security policies and standards to determine that data in transit was required to be encrypted. Inspected the configuration of outbound SFTP settings to determine that restrictions, permissible items, and encryption were implemented while using SFTPs. For a selected SFTP configuration, inspected the SFTP request and encryption settings to determine that setup information to establish the external secured connection was defined and configured based on company standards.	No exceptions noted
CC06-35.1	Mobile Device Passwords and Encryption Mobile devices used for company communications are password protected and configured for full device encryption.	Inspected Nationwide's Access Control IT Security Standard policy and procedure documentation to determine that password and encryption guidelines were established for mobile devices that are connected to Nationwide resources and systems. Inspected mobile device management configurations to determine that mobile devices were required to be password protected and were configured for full device encryption. For a selection of managed mobile devices, inspected the enrollment status into mobile device management to determine that devices were required to be password protected and configured for full device encryption.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-36.1	Removable Media Removable media is prohibited from being used on workstations unless an authorized and approved exception form is completed.	Inspected the Nationwide Data Security Standard to determine that employee workstations are to be configured for restricting the use of attachable devices and removable media unless provided authorization. Inspected the Active Directory Group Policy configuration to determine that removable media and attachable device usage is restricted according to corporate policy. Observed an unauthorized user attempt to use removable media and an attachable device to determine that the attempt was unsuccessful as an error message was displayed. Inspected the completed authorization form for an authorized user to use removable media and attachable devices to determine that the capabilities were approved for use.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-37.1	Mobile Device Authentication and Connection Mobile device access to production systems is permitted by authorized devices enrolled in the managed device program with multifactor authentication (MFA).	Inspected Nationwide's Access Control IT Security Standard to determine that establishing a multifactor authentication (MFA) mechanism was defined for mobile device access to production systems. Inspected configuration settings for MFA to determine that mobile device access to Nationwide system components was enabled and secured. Observed as a user accessed a Nationwide production system through their mobile device that was enrolled in the managed device program to determine that multifactor authentication (MFA) was enforced. Observed as a user attempted to access a Nationwide production system through their mobile device that was not enrolled in the managed device program to determine that access was not permitted.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-38.1	Software Installation Only authorized software is permitted for installation on company assets. An authorization process is in place to manage the list of approved software.	Inspected the repository of applications and software that were approved for installation to determine that only authorized software was permitted for installation on company assets. Inspected the elevated privileges request form completed for administrator access to determine that the asset details, reason for access, and approvals must be provided prior to obtain one-to-one administrator access. Observed as a normal user, without elevated permissions, attempted to perform an install of software on their machine to determine that it was blocked due to not having administrator access. Observed as a normal user, without elevated permissions, attempted to perform an install of unauthorized software on their machine to determine that it was blocked due to not being approved software.	No exceptions noted
CC06-39.1	Administrator Access on Workstations End users are prohibited from having administrator access on their workstations.	Inspected the Personal Computing User Rights policy to determine that end users were prohibited from having administrator access on their workstations. Inspected the elevated privileges request form completed for administrator access to determine that the asset details, reason for access, and approvals must be provided prior to obtain one-to-one administrator access. Observed as a normal user, without elevated permissions, attempted to perform an install of software on their machine to determine that it was blocked due to not having administrator access.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-40.1	Administrator Access Review Users with Type 2 elevated administrator access (IT Support) are reviewed on a weekly basis to assess the need and remove access as appropriate.	Inspected the configurations of the Windows global group and elevated access permission that permits 1-to-many Administrator access to determine that access permissions required to install software on a company asset were configured. For a selection of weeks, inspected the weekly review packages of the L1 to L3 support users with 1-to-many Administrator access to determine that the users with administrator access were reviewed and removed access, if necessary, in accordance with management's standards.	No exceptions noted
CC06-41.1	Antimalware Technology Antimalware technology is deployed for environments commonly susceptible to malicious attack. This software is used to scan assets prior to being placed into production.	Inspected malware scanning and responses procedures to determine that antimalware technology was in place and protocols for responding to detections were defined. Inspected system evidence of the antimalware scanning, schedule for definition updates, and installation to determine that antimalware mechanisms were deployed for production environments.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-42.1	Antivirus Software Antivirus software is installed on employee workstations and laptops. Antivirus definitions for daily updates for the software provider.	Inspected the antivirus tool dashboard to determine that data was available for management to monitor the deployment of antivirus agents on workstations and servers. Inspected the antivirus policy configuration to determine that the software was configured to update virus definitions daily. Inspected the antivirus policy configuration to determine that alerting was configured for employee workstations when any noncompliant items identified and blocked. Inspected the antivirus policy configuration to determine that sensors for monitoring of viruses were automatically pushed to employee machines. Observed an employee's workstation for antivirus definitions to determine that the sensor and updated definitions were installed as managed by the antivirus software.	No exceptions noted
CC06-43.1	Phishing and Spoofing Attempts Emails received by Nationwide's corporate email accounts are scanned for spam, malicious internet links, and other types of phishing and spoofing attempts.	Inspected a selection of Cisco, Area 1, and Office 365 configurations to determine that emails received by Nationwide's corporate email accounts were scanned for spam, malicious internet links, and other types of phishing and spoofing attempts. Inspected a selection of Cisco, Area 1, and Office 365 logs of malicious items removed from email to determine that email accounts were scanned for spam, malicious internet links, and other types of phishing and spoofing attempts.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC06-44.1	Workstation Administrator Access Provisioning and Deprovisioning Users are provisioned Type 1 elevated administrator access through an authorization approval workflow and have access automatically revoked based on a timebox constraint within IIQ.	Inspected the User Rights Rule standard to determine that an authorization workflow process was defined to obtain Type 1 elevated access and de-provisioning occurred automatically through expiration rule within IIQ. Inspected the provisioning approval workflow configuration within IIQ to determine that Type 1 elevated access requested were administered after approval was obtained through the workflow. Inspected the de-provisioning expiration rule within IIQ to determine that Type 1 elevated access expired as the specified time period elapsed based on the access request for Type 1 elevated access. For a selection of Type 1 elevated users during the period, inspected supporting documentation and system evidence to determine that access was provisioned based on the authorization approval workflow and access revoked per the IIQ expiration rule in accordance with management's standards.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC07-01.1	Continuous Detection for Unauthorized Components Automated mechanisms are used to continuously detect the connection/addition of unauthorized components/devices into the environment system.	Inspected the monitoring tool configuration to determine that unknown or unauthorized connections to the network were detected and addressed following the incident management process. Observed a successful connection attempt to the network to determine that based on the policies set that the connection was permitted as expected. Observed an unsuccessful connection attempt to the network to determine that based on the policies set that the connection was rejected as expected.	No exceptions noted
CC07-02.2	Review of Information Security Metrics Report On a monthly basis, the Defense Optimization team meets to discuss and review the Information Security Metrics report, including open and actioned security and availability incidents.	Inspected the detection planning procedures to determine that Nationwide has defined a process for detecting security and availability incidents. For a selection of months, inspected supporting documentation of the Defense Optimization's Monthly Dashboard reviews to determine that the dashboard did not display unusual trends in the number of open and actioned security and availability incidents.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC07-03.1	Internal Vulnerability Scanning Rapid7 software is utilized for internal vulnerability scanning and is performed at least on a weekly basis. A remediation plan is developed, and changes are implemented to remediate critical/high/medium vulnerabilities.	Inspected the Rapid7 Dashboard to determine that software was utilized for internal vulnerability scanning and was performed at least on a weekly basis. Inspected the configurations over the import, assignment, and risk rating of vulnerabilities for ServiceNow to determine that tickets were auto-generated for resolution when vulnerabilities were identified. Inspected the scanning configuration and schedule for a selection of servers and Nationwide Technology products scanned by Rapid7 software to determine that scanning was configured to run. For a selection of vulnerabilities identified by Rapid7, inspected ServiceNow tickets to determine vulnerabilities were identified and remediated within the required SLA.	No exceptions noted
CC07-04.1	Computer Hardening Standards Computer hardening standards have been documented and reviewed annually, and are followed during the initial build and when modifications to laptop, desktops, and servers are made.	Inspected the baseline configuration standards to determine that the standards existed. For a selection of Nationwide technology components (databases, operating systems, and network), inspected the secure baseline configurations and the configuration review documentation to determine that the configuration baselines were established and reviewed annually. For a selection of databases, inspected secure configuration scan results to determine that baseline database configurations were scanned, and abnormalities were worked towards resolution.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC07-05.1	Real-Time Monitoring of Information Nationwide's Cyber Security Operations Center (CSOC) provides real-time monitoring of information related to the security of systems.	Inspected policies and procedures for the SOC to determine that criteria outlining Service Level Agreements (SLAs) for responding to security incidents/events were established. Inspected the dashboard and system configurations within CrowdStrike to determine that the alerting mechanism was configured for notifying individuals in the event of a security event. For a selection of CrowdStrike alerts, inspected the email notifications to determine that responsible personnel were notified in the instance of a security incident. For a selection of weeks, inspected email communications to determine that the Cyber Security Operations Center (CSOC) team communicated identified emerging threats.	No exceptions noted
CC07-06.2	Incident Response Policies and Escalation Plans Nationwide has incident response policies and procedures in place that includes an escalation plan based on the nature and severity of the incident.	Inspected the Nationwide Incident Response IT Security Standard and the Event Management Policy and Procedures and Security Incident Response Run Book to determine that procedures were defined for assisting with the identification, reporting, and resolution of security and availability incidents.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC07-07.2	Security Incident Alerting and Analysis The IR Threat Mitigation team monitors for security incident alerts and follows a process of analyzing the security incident. The process begins with detailing what specific attack occurred, which system(s) were affected, and what happened during the attack. If root cause cannot be determined, it is routed to the IR Threat Response team for further analysis.	Inspected the Nationwide Incident Response IT Security Standard and Event Management policy to determine that incident response procedures were defined. For a selection of IT security incidents, inspected supporting incident ticket documentation to determine that an incident response plan was initiated by authorized personnel, threats were mitigated, corrective action plans were documented, and incidents were tracked until resolved.	No exceptions noted
CC07-08.2	Security Incident Response A security incident response exercise is performed at least annually to help validate the effectiveness of the incident response process.	Inspected the Nationwide Incident Response policy and procedure to determine that a process was established for security incident response and that process exercised annually. Inspected the EDO Data Classification standard to determine that the identification of data classifications during a security incident was performed to evaluate the impact and significance of the incident. Inspected the annual security incident response exercise documentation to determine that management performed a security incident response exercise at least annually and implemented revisions to the policy based upon the outcomes of the exercise.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC07-09.1	Workstation Updates and Testing Workstation software, including internet browsers, and production servers are kept current, tested, and approved for use by the Infrastructure and Operations and IRM teams to avoid possible security problems.	Inspected the Information Security Policy, the Nationwide Risk Assessment IT Security Standard, and run books for Windows, Linux, and problem server patching to determine that established processes existed for patch management for identifying, triaging, testing, and deploying updates to NW system components. Inspected the configurations for auto-updating NW system resources with latest noncritical patches from vendors to determine that patches identified were prepared for installation. For a selection of security patches made to NW system software and components, inspected the patch supporting documentation to determine that the patches were identified, triaged, tested, and deployed.	No exceptions noted
CC08-01.1	Change Management Process and Tools Changes to system components are tracked, tested, and approved prior to being implemented into production through the use of development and migration tools to determine that security and availability commitments are met.	Inspected the change management policy to determine that a process was defined for testing changes according to security and availability commitments prior to being approved and moved into production. For a selection of production changes to in-scope systems, inspected the supporting documentation to determine that the change was tested and approved prior to implementation in production.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC08-02.1	Change Development and Testing Changes to system infrastructure and software are developed and tested in a separate development or test environment before implementation and are implemented to production following the segregation of duties principle.	Inspected the IT Operations Capability Policy and Standards Guide to determine that test environments were established within the change management process. Inspected system evidence to determine that separate testing and production environments existed.	No exceptions noted
CC08-03.1	Baseline Configurations Nationwide developed, documented, and maintained a baseline configuration of system infrastructure.	Inspected the Secure Configuration Documentation Process and Secure Configuration Baseline template configuration documentation to determine that Nationwide develops, documents, and maintains a baseline configuration of system infrastructure (servers and databases). Inspected annual review documentation of baseline configurations for a selection of system infrastructure to determine that Nationwide maintained baseline configuration through an annual review in alignment with the process.	No exceptions noted
CC08-04.1	Secure Development Program A secure development program is in place that sets standards for embedding security into the software development life cycle.	Inspected the secure coding standards to determine that security standards were established for code development activities. Observed as a developer displayed secure coding standards used in practice within a recent program change to determine that secure coding standards were in use. For a selection of developers, inspected the training certificates to determine that the developers completed the required developer trainings.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC08-05.1	Change Management Procedures Formally documented change management procedures (including emergency procedures) are in place to govern the modification and maintenance of production systems and address security and availability requirements.	Inspected the IT Change Management Process Owner Reference Guide and IT Run Capability Policy to determine that change management procedures (including emergency procedures) were in place to govern the modification and maintenance of production systems.	No exceptions noted
CC08-06.1	Secure Coding Tools Secure coding tools are utilized to scan web-based applications' code for known flaws and vulnerabilities.	Inspected the configuration settings and schedule of the vulnerability scanning tools used for a selection of in-scope web-based applications to determine that the criteria scanned for and determination of severity on identified vulnerabilities was configured. For a selection of production deployments, inspected the supporting documentation and scan evidence to determine that vulnerability scanning was completed, and vulnerabilities were resolved.	No exceptions noted
CC08-07.1a	Segregation of Duties – Change Management Nationwide has designed application-enforced segregation of duties to define what privileges are assigned to users within applications.	Inspected system generated listings of users with application development roles and users with privileged level roles to determine that access is segregated based on job responsibilities.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC08-07.1b	Segregation of Duties – UrbanCode Deploy Configuration The UrbanCode Deploy change tool is configured to require independent approval of changes prior to code promotion to the production environment.	Inspected the UrbanCode Deploy configuration to determine that approval is required prior to promotion to the production environment. Inspected a system generated listing of users with the ability to modify UrbanCode Deploy configurations to determine that user's access was segregated from users with development and approval privileges based on job responsibilities. Observed an unapproved change request in UrbanCode Deploy to determine that the system prevented selection of the promote action. Observed an approved change request in UrbanCode Deploy to determine that the system allowed selection of the promote action.	No exceptions noted
CC08-07.1c	Segregation of Duties – Harness Configuration The Harness change tool is configured to require independent approval of changes prior to code promotion to the production environment.	Inspected the ChangeMan configuration to determine that approval is required prior to promotion to the production environment. Inspected a system generated listing of users with the ability to modify ChangeMan configurations to determine that user's access was segregated from users with development and approval privileges based on job responsibilities. Observed an unapproved change request in ChangeMan to determine that the system prevented selection of the promote action. Observed an approved change request in ChangeMan to determine that the system allowed selection of the promote action.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC08-07.1d	Segregation of Duties – GitHub Configuration The GitHub Code Repository tool is configured to require independent approval of changes prior to code merger to the production environment.	Inspected the GitHub configuration to determine that approval is required prior to code merger to the production environment. Inspected the GitHub Repository Settings to determine that repository administrators are unable to modify Branch Protection rules to override the approval configuration. Observed an unapproved change request in GitHub to determine that the system prevented selection of the merge action. Observed an approved change request in GitHub to determine that the system allowed selection of the merge action.	No exceptions noted
CC08-07.1e	Segregation of Duties – GitHub Configuration Log Review From 1/1/2023-7/30/2023, GitHub configuration logs are reviewed by management to verify branch policy override actions were appropriate for changes committed to the main branch. Any overrides that occur are researched and documented by the team leads. Evidence of review is documented via signoff and date by management.	Inspected management's review performed on configuration changes associated branch policy override actions to determine the review was documented. Reviewed management's approval for any configuration overrides to determine changes were approved by management.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC09-01.2	System Recovery Plans System recovery (disaster) plans have been developed, are updated routinely, certified annually, and are required to perform either a walk-through or validation test annually. The system plans criticality is established from the results of the Business Impact Analysis.	Inspected the Disaster Recovery Standards and Plans to determine that plans were developed and updated periodically, certified annually, and validated via testing annually based on the business impact analysis performed by each business unit.	No exceptions noted
CC09-02.1	Contingency Planning Contingency Planning standards are defined and periodically reviewed and approved by management.	Inspected the Contingency Planning IT Security Standard and Contingency Planning Handbook to determine that a standard was developed, updated periodically, and reviewed and approved every other year. Inspected the Contingency Plan Exercise Report to determine that a tabletop walkthrough of the contingency plan was performed based on the standard and handbook.	No exceptions noted
CC09-04.1	Business Continuity Plans Business continuity plans have been developed, are updated routinely, certified annually, and are required to perform either a walk-through or validation test annually.	Inspected the Nationwide Business Continuity Handbook and Contingency Planning IT Security Standard to determine that the plans were developed and updated during the period. Inspected the RSGIB Business Continuity Plan Report to determine that a tabletop walkthrough of the business continuity plan was performed based on the standard and handbook.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC09-05.1	Business Impact Analysis The enterprise-wide Business Impact Analysis (BIA) is performed at least every four years, and considers internal and external risks to determine the impact of a disruption on business functions/processes.	Inspected the most recent business impact analysis and current year business recovery plan results to determine that procedures supporting system recovery were defined to help meet availability commitments and requirements.	Exception noted The BIA was not performed during the four-year cycle as required by the policy.
Management's Response: Due to adoption of a new framework (ACORD Capability Framework) and changes in tooling, Nationwide's Business Impact Analysis (BIA) was not completed in 2023. This was documented as a finding and tracked and communicated to appropriate parties. The lack of BIA outcomes in 2023 did not impact the 2023 business continuity plans or plan testing/walkthroughs.			
CC09-06.1	Cyber-Related Insurance The risk management program includes the use of insurance to minimize the financial impact of cyber-related loss events.	Inspected evidence of Nationwide's cybersecurity liability insurance to determine a cybersecurity liability insurance package was in place.	No exceptions noted
CC09-08.1	Third-Party Risk Management Program Nationwide has established a third-party risk management program that classifies their third-party and potential third-party vendors based upon a risk assessment. Periodic audits are performed on third parties based upon their risk classification, and issues identified by the audits are communicated and monitored through resolution.	Inspected the Nationwide Third-Party IT Security Standard to determine that policies and procedures were in place to select, review, and manage vendors, third-party suppliers, and business partners, including a fair selection process and evidence of financial, technical, and operational controls. For a selection of third-party assessments and reassessments performed, inspected evidence to determine that a risk classification was assigned, vendor questionnaires were completed, vendor assessments were completed, and any identified issues were remediated.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC09-09.1	Third-Party Vendor Information Security Policies Nationwide's third-party vendors are required to have information security policies in place that adhere to those at Nationwide. Information security policies are obtained and reviewed as part of Nationwide's third-party assessment process.	Inspected security policies to determine Nationwide has established defined roles and responsibilities to oversee the SRQ process to obtain and review information security policies as part of the vendor risk assessment process.	No exceptions noted
CC09-10.1	Third-Party Monitoring Various tools are used by management to monitor third-party activity to identify potential threats to operations.	Inspected the annual risk assessment documentation to determine that they included the significant aspects of operations. Inspected system evidence of the configurations for a selection of tools established to determine the tools monitored third-party activity to identify potential threats to operations.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
CC09-11.1	Third-Party Periodic Risk Assessments Third-Party suppliers and service providers are assessed on a periodic basis based on a risk rating scale.	Inspected the Nationwide Enterprise Supplier Risk Management Policy to determine that policies and procedures were in place to review and manage third-party suppliers/service providers. Inspected the supplier risk questionnaire template to determine that factors and assessment criteria were established for risk ranking a third-party supplier and service provider. Inspected the Ariba assessment configuration for suppliers to determine that requirements were set to enforce an initial assessment and a scheduled recertification based on risk ranking grade. For a selection of supplier and service provider assessments, inspected the recertification schedule to determine that the supplier assessment was completed and was scheduled for recertification based on the risk ranked grade during initial assessment.	No exceptions noted
A01-01.1	Processing Capacity Processing capacity is monitored continuously to enable service delivery real-time for adherence to negotiated Service Level Agreements.	Inquired of management and inspected the processing monitoring capacity and consumption documentation to determine that processing capacity metrics such as CPU usage, storage capacity, and server uptime were monitored.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
A01-02.2	Systems Validation and Recovery Exercise Every other year, a systems/application validation exercise of failing from production to a recovery environment occurs for critical applications, critical infrastructure, and key services.	Inspected the CIKs (Critical Infrastructure and Key Services) listing from ServiceNow to determine the frequency that relevant systems needed to be updated and that validation exercises were performed as scheduled. For a selection of in-scope systems, inspected the Disaster Recovery Technical Sequencing document to determine that the recovery plan and recovery time objective were specified and met.	No exceptions noted
A01-03.1	Computer Operations and Job Processing Computer operations, including job processing, are monitored to validate key tasks, scheduled jobs, and events, and expected outcomes are achieved.	Inspected the configuration and mapping process flow between in-scope system job schedulers and the BigPanda monitoring tool to determine that failed job tickets were set for automatic creation in ServiceNow. Inspected the monitoring and alert configuration in BigPanda to determine that the monitoring, logging, and alerting were enabled for ServiceNow ticket creation. For a selection of failed jobs, inspected supporting documentation and job rerun evidence to determine that failed jobs were investigated and worked toward resolution.	No exceptions noted
A01-04.1	Traffic Management and Redundancy Traffic management capabilities, such as redundancy, are in place to meet business requirements.	Observed the load-balance server configuration and supporting monitoring documentation to determine traffic management capabilities were in place to meet management's standards and any processing capacity concerns were raised, followed up on, and resolved.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
A01-05.1	Environmental Protections Monitoring 24/7 operations personnel monitor the status of environmental protections during each shift. Alarm mechanisms have been installed within the data center and operations room to communicate any discrepancies in environmental thresholds for resolution.	Inspected Nationwide data center monitoring work instructions and emergency operating procedures to determine that procedures were established for data center operations personnel for responding to environmental alerts and alarms. Inspected data center and operations room alert configurations to determine that alarms for abnormal thresholds on temperature, humidity, and power readings were set on environmental equipment. For a selection of days, inspected daily maintenance logs from the Agnus Anywhere system to determine that required daily maintenance checks were performed on all shifts (1st, 2nd, and 3rd).	No exceptions noted
A01-06.1	Environmental Systems Maintenance Environmental systems at the data center are scheduled for periodic maintenance checks throughout the year and include the following: • Cooling systems units • UPS • Backup generators • Fire extinguishers	Inspected the periodic maintenance schedule for data center environmental systems to determine that periodic maintenance and physical checks were scheduled. For a selection of months, inspected the maintenance summary reports for routine maintenance performed to determine that periodic maintenance was completed for environmental systems.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
A01-07.1	Environmental Protections Environmental protections have been installed including the following: • Cooling systems (water tank and chillers) • UPSs (uninterruptible power supply) • Generators • Batteries • Smoke detectors • Sprinklers • Fire extinguishers	Inspected the blueprints of the fire suppression and alarm systems to determine that fire suppression environmental protections were installed. Observed through a walk-through of the data center to determine that environmental protections within Nationwide facilities and the data center were implemented.	No exceptions noted
A01-08.1	Backup and Recovery Standards Nationwide maintains backup and recovery standards and procedures with a backup schedule as defined by the business organizations for data backup and retention. Failures are monitored to resolution.	Inspected the server backup policy and IT contingency planning standard to determine that backup procedures and schedules and recovery processes were defined and documented. For a selection of in-scope application environments, inspected the server replication and backup schedule configurations to determine that in-scope application processing environments and related production data were scheduled to perform replication or backups according to policy. Inspected the automated alert configuration for in-scope applications to determine that upon failure of a scheduled backup an alert is sent to IT Operations Support personnel for resolution.	No exceptions noted

Control Reference	Nationwide's Control Activity	Tests Performed by KPMG	Test Results
A01-09.1	Production Data Backup and Replication Application processing environments and related production data are replicated or backed up to a secondary facility in accordance with the management recovery strategy.	Inspected the IT contingency planning standard to determine that recovery processes were defined and documented. For a selection of in-scope application environments, inspected the replication configurations to determine that the system is configured to replicate the data near real-time to a secondary facility in accordance with the management recovery strategy.	No exceptions noted