Network Better.

System and Organization Controls (SOC) 3 Report

Report on Fiberutilities Group LLC's Titan Web Application Relevant to Security

For the period September 1, 2024 to November 30, 2024

Modern Assurance

The report accompanying this description was issued by Modern Assurance, LLC.

Table of Contents

Section I: Independent Service Auditor’s Report

Modern Assurance

Independent Service Auditor’s Report

To Management of Fiberutilities Group LLC,

Scope

We have examined Fiberutilities Group LLC's (FG's) accompanying assertion, titled “Fiberutilities Group LLC's Management Assertion” (assertion) that the controls within FG's Titan Web Application (system) were effective throughout the period September 1, 2024 to November 30, 2024 to provide reasonable assurance that FG's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity,* Confidentiality, and Privacy (AICPA, Trust Services Criteria).

FG uses the subservice organization described in the “Subservice Organization” subsection of Attachment A of the report. The information included within the Boundaries of Fiberutilities Group LLC's System (Attachment A) indicates that FG's controls can provide reasonable assurance that certain service commitments and system requirements, based on the applicable trust services criteria, can be achieved only if the controls at the subservice organization, assumed in the design of FG's controls, are suitably designed and operating effectively along with related controls at the service organization. The information included within the boundaries of the system presents FG's system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at the subservice organization. Our examination did not extend to the services provided by the subservice organization and we have not evaluated whether the controls management assumes have been implemented at the subservice organization or whether such controls were suitably designed and operating effectively throughout the period September 1, 2024 to November 30, 2024.

The information included within the Boundaries of Fiberutilities Group LLC's System (Attachment A) indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at FG, to achieve the service commitments and system requirements of FG based on the applicable trust service criteria. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization’s Responsibilities

FG 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 FG's service commitments and system requirements were achieved. FG has provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, FG is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the controls were not effective to achieve FG's service commitments and system requirements based on the applicable trust services criteria.
- performing procedures to obtain evidence about whether controls within the system were effective to achieve FG's service commitments and system requirements based on the applicable trust services criteria.

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

There are inherent limitations in 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 were 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.

Opinion

In our opinion, management's assertion that the controls within FG's Titan web application were effective throughout the period September 1, 2024 to November 30, 2024 to provide reasonable assurance that FG's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Modern Assurance, LLC

December 20, 2024
Bend, Oregon

Section II: Fiberutilities Group LLC's Management Assertion

Network Better.

Fiberutilities Group LLC's Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Fiberutilities Group LLC's (FG's) Titan web application (system) throughout the period September 1, 2024 to November 30, 2024 to provide reasonable assurance that FG's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

The information included within the Boundaries of Fiberutilities Group LLC's System (Attachment A) indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at FG, to achieve FG's service commitments and system requirements based on the applicable trust services criteria. The Boundaries of Fiberutilities Group LLC's System (Attachment A) presents the types of complementary subservice organization controls assumed in the design of FG's controls, and does not disclose the actual controls at the subservice organizations.

The information included within the Boundaries of Fiberutilities Group LLC's System (Attachment A) indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at FG, to achieve the service commitments and system requirements of FG based on the applicable trust service criteria. Attachment A presents those complementary user entity controls assumed in the design of FG's controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period September 1, 2024 to November 30, 2024 to provide reasonable assurance that FG's service commitments and system requirements would be achieved based on the applicable trust services criteria, if user entities and the subservice organizations applied the complementary controls assumed in the design of FG's controls throughout that period. FG's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period September 1, 2024 to November 30, 2024 to provide reasonable assurance that FG's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A

Boundaries of Fiberutilities Group LLC's system

Attachment B

Fiberutilities Group LLC's Service Commitments and System Requirements

Attachment A: Boundaries of Fiberutilities Group LLC's System

Fiberutilities Group LLC's Titan Web Application

Overview of the Company and Types of Services Provided

Fiberutilities Group LLC (“FG” or “the Company”) has been providing transformative technology solutions to clients for over 20 years. FG provides network assessment, design and managed services while also specializing in federal funding and carrier/vendor management services. FG utilizes a proprietary, cloud-based enterprise software solution/platform, delivered as a managed service, to assist clients in effectively managing their telecom estate. This platform, integrated with managed service support, offers a centralized telecom inventory management system, proactive carrier management services—including contract administration, order coordination, invoice processing, and issue resolution.

The platform is also a comprehensive tool utilized to administer federal funding programs for healthcare providers. FG’s software solution delivers data analytics that reveal actionable insights from previously hidden network data. The platform is hosted in highly available, geographically distributed data centers and has been developed using OutSystems, a low-code/no-code PAAS, built on AWS Cloud. FG leverages Microsoft Azure Cloud Services, including Data Factory ETL pipelines for data import, Data Lake Storage for file archiving and document storage, and Azure SQL Databases to ensure data integrity throughout the data lifecycle process.

Components of the System

Infrastructure

The Titan Web Application is comprised of the following components:

Component	Description	Hosting Location
FundCapture	Customer-facing module within the Titan web application for users to manage the process to qualify for and obtain reimbursement from the Healthcare Connect Fund (HCF)	OutSystems (OutSystems' servers are hosted at AWS)
CarrierComplete	Customer-facing module within the Titan web application for users to manage the entire telecom lifecycle	OutSystems (OutSystems' servers are hosted at AWS)

Component	Description	Hosting Location
Manual processes for receipt of data sources that are presented within the web application	This includes various processes: 1) Valicom captures invoice information from carriers and feeds the data to FG through SFTP or API; 2) InvoiceIQ captures invoice information from carriers and feeds the data to FG through SFTP or API; 3) customers send payment vouchers from PeopleSoft to FG through SFTP; and 4) FG manually obtains data directly from Carrier Portals after LOA is implemented.	After intake, data is stored in Azure-hosted databases

Software

FG utilizes the following software to support the platform:

Function	Software used
Human resources	iSolved
Password management	Titan and SAML 2.0
Ticketing	Jira
Change management and deployment	Outsystems Lifetime
Monitoring and logging	Outsystems AI MentorStudio, Outsystems LifeTime, Outsystems Service Center, and Windows Defender
Vulnerability scanning	Outsystems AI Mentor Studio
Mobile device management	N-able

Data

The platform ingests data primarily through manual data feeds including SFTP and direct upload into the platform. Data is stored in SQL Server and Azure Blob Storage. The databases housing sensitive customer data are encrypted at rest **(AC-10)**. Sensitive data is not transmitted outside of FG's environment. The Company uses HTTPS, SSH, TLS, and Microsoft Managed Keys to encrypt confidential and sensitive data when transmitted over public networks **(AC-11)**. Developers utilize SQL Server Management Studio, Dbforge, and Outsystems to interact with the databases. The company uses ETL pipelines within Azure to move data into a Data Lake within Azure. Additionally, PowerBI is embedded into the Titan application for the purpose of presenting analytics on telecom data. All in-scope cloud resources containing either customer data or production infrastructure are restricted to not allow public access without first authenticating **(AC-13)**. Non-console access to infrastructure is restricted via security settings **(AC-05)**.

People

FG's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored.

FG has established an organizational structure that includes consideration of key areas of authority and responsibility, as well as appropriate lines of reporting.

Policies

FG has implemented the following policies, which serve as the basis for Company procedures, are made accessible to all relevant employees and contractors, and are reviewed annually:

- Acceptable Use Policy - defines standards for appropriate and secure use of company hardware and electronic systems, including storage media, communication tools, and internet access. This policy is acknowledged by employees and contractors upon hire **(ORG-10).**

- Access Control and Termination Policy - governs authentication and access to applications, resources, and tools **(AC-04).**

- Business Continuity and Disaster Recovery Policy - governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption **(AVA-04).**

- Change Management Policy - governs the documentation, tracking, testing, and approval of system, network, security, and infrastructure changes for applications, resources, and tools **(CM-07).**

- Employee Handbook and Code of Conduct - outline ethical expectations, behavior standards, and ramifications of non-compliance. The policy is acknowledged by employees and contractors upon hire **(ORG-01).**

- Configuration and Asset Management Policy - governs configurations for new applications, resources, and tools **(CM-06).**

- Encryption and Key Management Policy - supports the requirements for secure encryption and decryption of app secrets, and governs the use of cryptographic controls **(AC-12).**

- Written Information Security Plan - establishes the security requirements for maintaining the security of applications, resources, and tools **(ORG-12)** and outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution **(IR-01).**

- Internal Control Policy - identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies **(ORG-14).**
- Network Security Policy - identifies the requirements for protecting information and systems within and across networks **(NET-06).**
- Performance Review Policy - provides personnel context and transparency into their performance and career development processes **(ORG-15).**
- Risk Assessment and Treatment Policy - governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners **(RA-01).**
- Secure Development Policy - defines the requirements for secure software and system development and maintenance **(CM-08).**
- Vendor Management Policy - defines a framework for the onboarding and management of the vendor relationship cycle **(RA-04).**
- Vulnerability Management and Patch Management Policy - outlines the processes to identify and respond to vulnerabilities **(VM-01).**

Control Environment

The objectives of internal control as it relates to the Titan web application are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet the relevant control objectives, that assets are protected from unauthorized use or disposition, and that transactions are executed in accordance with management's authorization and client instructions. Management has established and maintains controls designed to monitor compliance with established policies and procedures. The remainder of this subsection discusses the tone at the top as set by management, the integrity, ethical values, and competence of FG employees, the policies and procedures, the risk management process and monitoring, and the roles of significant control groups. The internal control structure is established and refreshed based on FG's assessment of the risks facing the organization.

Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Integrity and ethical behavior are the products of FG's ethical and behavioral standards, how they are communicated, and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce incentives/pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of the entity's values and behavioral standards to personnel through policy statements and Code of Conduct, and by the examples the executives set. FG's executive management recognizes their responsibility to foster a strong ethical environment within FG to ensure that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct. This responsibility is characterized and reflected in the Code of Conduct, which is distributed to all applicable personnel of the organization.

Risk Assessment Process

FG has defined a risk management framework for evaluating information security risk and other relevant forms of business risk. A formal risk assessment is performed at least annually to identify, update, and assess relevant internal and external threats related to security, which also considers the potential for fraud **(RA-02).** A risk register is maintained to record the risk mitigation strategies for identified risks, and to track the development or modification of controls consistent with the risk mitigation strategy **(RA-03).**

Due to the company's heavy reliance on outside vendors for critical infrastructure, processing capabilities, and business functions, the company has developed a Vendor Management Policy that establishes the compliance and performance expectations required of vendors, and the due diligence and monitoring expectations required of the Company's personnel. Agreements, which include security requirements, are executed with vendors in accordance with the Vendor Management Policy **(RA-06).** FG collects and reviews the compliance reports (i.e. SOC 2, SOC 3, or ISO 27001) for its high-risk vendors on at least an annual basis **(RA-05).**

Monitoring Activities

FG performs several types of monitoring to assess the security and health of the in-scope environment and the related controls. The company leverages a continuous monitoring solution that monitors internal controls used in the achievement of service commitments and system requirements. The tool identifies instances of non-compliance for management to resolve **(ORG-05).**

Logging is enabled and monitoring software is configured to collect metrics from ingested logs to detect potential security threats, unusual system activity, and monitor system performance, as applicable **(NET-04).** Alerting software and weekly meetings are used to notify impacted teams of potential security events, and identified events are tracked to resolution **(NET-05).** The Security Steering Committee meets quarterly to coordinate security initiatives, review network security and management of infrastructure, and discuss security risks **(NET-07)**. Virtual machines that intake files are configured with antivirus scanning **(NET-09).**

Incident Response

The Company employs multiple mechanisms to identify potential security incidents. Confirmed incidents are documented, tracked, and responded to according to the Written Information Security Plan **(IR-02).** Following an incident, a 'lessons learned' document is created and shared with relevant internal personnel to make any required changes **(IR-03).** The Written Information

Security Plan is tested annually to assess effectiveness, and management makes changes to the Written Information Security Plan based on the test results **(IR-04).** Cybersecurity insurance has been procured to help minimize the financial impact of cybersecurity loss events **(ORG-13).**

Complementary User Entity Controls

The following user entity controls are assumed to be implemented by user entities and are necessary for the service organization's service commitments and system requirements to be achieved.

User Entity Control
User entities are responsible for understanding and complying with their contractual obligations to FG.
User entities are responsible for ensuring the supervision, management, and control of the use of FG's services by their personnel.
User entities are responsible for ensuring that only authorized and properly trained personnel are allowed access to the services.
User entities are responsible for ensuring that any data submitted to FG Network is shared in a secured manner.

Subservice Organization

The Company utilizes the subservice organization in the below tables to achieve its objectives.

Subservice Organization	Services Provided
Microsoft Corporation (Azure)	The subservice organization provides the Company with cloud-based database infrastructure. This organization was carved out of the report.

Complementary Subservice Organization Controls

- The subservice organization's data centers are protected by fire detection and suppression systems, air conditioning systems, uninterruptible power supply (UPS) units, and backup generators (CC 5.2).
- The subservice organization performs integrity checks of the data at rest (CC 5.2).
- The subservice organization ensures that logical IT access is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.1, CC 6.2, CC 6.3, CC 6.6).
- The subservice organization ensures that strong encryption keys are used to protect customer content and that master keys used for cryptographic operations are logically secured (CC 6.1).

Subservice Organization	Services Provided
Microsoft Corporation (Azure)	The subservice organization provides the Company with cloud-based database infrastructure. This organization was carved out of the report.

Complementary Subservice Organization Controls

- The subservice organization ensures that physical access to the data centers is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.4).
- The subservice organization ensures that data is encrypted in transit (CC 6.6, CC 6.7).
- The subservice organization 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 (CC6.5).

Subservice Organization	Services Provided
OutSystems	The subservice organization provides the Company with application hosting. This organization was carved out of the report.

Complementary Subservice Organization Controls

- The subservice organization is responsible for scanning the infrastructure for potential vulnerabilities and remediating in a timely manner (CC2.1, CC3.2, CC4.1, CC4.2, CC7.1).
- The subservice organization performs periodic vulnerability assessments (CC 3.2).
- The subservice organization's data centers are protected by fire detection and suppression systems, air conditioning systems, uninterruptible power supply (UPS) units, and backup generators (CC 5.2).
- The subservice organization applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved (CC 5.2, CC 8.1).
- The subservice organization performs integrity checks of the data at rest (CC 5.2).
- The subservice organization implements redundancy and replication to ensure that the system is able to sustain the loss of a data center facility without interruption to the service (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains contingency planning and incident response procedures to reflect emerging continuity risks and lessons learned from past incidents (CC 5.2, CC 7.4, CC 7.5).
- The subservice organization maintains a capacity planning model to periodically assess infrastructure usage and demands (CC 5.2).
- The subservice organization ensures that logical IT access is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.1, CC 6.2, CC 6.3, CC 6.6).
- The subservice organization is responsible for configuring the firewall rules (CC6.1,

Subservice Organization	Services Provided
OutSystems	The subservice organization provides the Company with application hosting. This organization was carved out of the report.

Complementary Subservice Organization Controls

CC6.6, CC7.1, CC7.2).

- The subservice organization ensures that strong encryption keys are used to protect customer content and that master keys used for cryptographic operations are logically secured (CC 6.1).
- The subservice organization ensures that physical access to the data centers is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.4).
- The subservice organization ensures that data is encrypted in transit (CC 6.6, CC 6.7).
- The subservice organization has implemented monitoring to identify and notify personnel of potential issues and/or incidents (CC 7.1, CC 7.5).
- The subservice organization monitors the operating systems and applies patches as needed (CC7.1, CC8.1).
- The subservice organization has implemented incident response procedures to identify, track, and respond to incidents (CC 7.3, CC 7.4, CC 7.5).
- The subservice organization ensures that customer information, including personal information, and customer content are not used in test and development environments (CC 8.1).
- The subservice organization maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact business objectives, regulatory requirements, and customers (CC 9.2).
- The subservice organization 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 (CC6.5).

Attachment B: Fiberutilities Group LLC's Service Commitments and System Requirements

Fiberutilities Group LLC's Service Commitments and System Requirements

FG and its customers have a shared responsibility in maintaining the security of the Titan web application. FG has established principal service commitments, which are communicated to customers and consist of the following:

- Defines and documents roles and responsibilities related to the Company’s Information Security Program and the protection of customer data. Requires team members to review and accept all of the security policies.
- Requires team members to go through employee security awareness training covering industry standard practices and information security topics such as phishing and password management.
- Performs background checks on all new team members in accordance with local laws.
- Follows the principle of least privilege with respect to identity and access management.
- Requires all team members to adhere to a minimum set of password requirements and complexity for access, and utilizes 2-factor authentication (2FA) where available.
- Enrolls all company-provided workstations in Mobile Device Management (MDM) to enforce security settings including full-disk encryption, screen lock, and strong password policy.
- Encrypts all databases at rest.
- Encrypts data in transit using transport layer security (TLS) or other technologies over public networks.
- Performs vulnerability scanning and actively monitors for threats.
- Performs an independent third-party penetration test at least annually to ensure that the security posture of services is uncompromised.
- Evaluates vendor risk and performs the appropriate vendor reviews prior to authorizing a new vendor.
- Undergoes at least annual risk assessments to identify any potential threats, including considerations for fraud.
- Actively monitors and logs various cloud services.
- Establishes a process for handling information security events which includes escalation procedures, rapid mitigation and communication.

FG has established system requirements, which are communicated to customers and consist of the following:

- User access reviews
- Logical access controls, such as the use of user IDs and passwords to access systems
- Encryption standards for data at rest and in transit
- Risk assessment standards
- Change management controls
- Incident response plan
- Business continuity and disaster recovery plan