Tarun Kandhari & Co LLP

Chartered Accountants

Service Organisation Controls TYPE 2 INTERM REPORT ON CONTROLS PLACED IN OPERATION FOR LEASING MANAGEMENT SOFTWARE

For the Period from

01 January 2025 to 31 December 2025

WITSYNC SOFT SOLUTIONS PRIVATE LIMITED

WITSYNC SOFT SOLUTIONS PRIVATE LIMITED

Table of Contents

SECTION 1:

INDEPENDENT SERVICE AUDITOR'S REPORT

Tarun Kandhari & Co LLP
Chartered Accountants
(Formerly Known as Tarun Kandhari & Co.)

INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF A SERVICE ORGANIZATION'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

To WITSYNC Soft Solutions Private Limited:

Scope

We have examined WITSYNC Soft Solutions Private Limited's ("WITSYNC") description of its Leasing Management Software throughout the period from January 01, 2025 to December 31, 2025 and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in WITSYNC's assertion included in Section 2 of this report. The description indicates that certain control objectives specified in the description can be met only if complementary user entity controls assumed in the design of WITSYNC's controls are suitably designed and operating effectively, along with related controls of the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls. The controls and control objectives included in the description are those that management of WITSYNC believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Leasing Management Software system that are not likely to be relevant to user entities' internal control over financial reporting.

Service Organization's Responsibilities

Within Section 2 of this report, WITSYNC has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. WITSYNC is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

We are service audit firm registered with The Institute of Chartered Accountants of India, our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted by referring to the relevant attestation standards available globally established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period from January 01, 2025 to December 31, 2025. 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:

TARUN KANDHARI Digitally signed by TARUN KANDHARI Date: 2026.01.31 18:41:23 +05'30'

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.

- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- Evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations

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

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4 of this report.

Opinion

In our opinion, in all material respects, based on the criteria described in WITSYNC's assertion in the next section of this report:

a. the description fairly presents the Leasing management software system that was designed and implemented throughout the period from January 01, 2025 to December 31, 2025;

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 01, 2025 to December 31, 2025 and user entities applied the complementary controls assumed in the design of WITSYNC's controls throughout the period January 01, 2025 to December 31, 2025; and

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period January 01, 2025 to December 31, 2025 if user entities applied the complementary controls assumed in the design of WITSYNC's controls, and those controls operated effectively throughout the period January 01, 2025 to December 31, 2025.

TARUN KANDHARI
Digitally signed by TARUN KANDHARI
Date: 2026.01.31 18:42:01 +05'30'

Tarun Kandhari & Co LLP

Chartered Accountants

(Formerly Known as Tarun Kandhari & Co.)

Restricted Use

This report, including the description of tests of controls and results thereof within Section 4, is intended solely for the information and use of management of WITSYNC, and user entities of WITSYNC's Leasing management software system during some or all of the period January 01, 2025 to December 31, 2025. This report is not intended to be, and should not be, used by anyone other than these specified parties.

For Tarun Kandhari & Co LLP
Chartered Accountants
Firm Reg. No. 006108C/N500042

TARUN KANDHARI

Digitally signed by TARUN KANDHARI
Date: 2026.01.31 18:42:29 +05'30'

Tarun Kandhari
Partner
Membership No. 074852
UDIN: 26074852MBEEAC1731
Place: New Delhi
Date: January 31, 2026

SECTION 2:

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

January 05, 2026

We have prepared the description of WITSYNC Soft Solutions Private Limited's ("WITSYNC") Leasing management software system throughout the period January 01, 2025 to December 31, 2025 for user entities of the system during some or all of the period January 01, 2025 to December 31, 2025, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

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

The WITSYNC Soft Solutions Private Limited ("WITSYNC") is an ISO (9001: 2015) and ISO (27001:2013) certified company since May 11, 2019 with certification numbers ISO (9001: 2015) SISINDQ05201944 and ISO/IEC (27001:2013) Certificate No. SISINDI05201904 and WITSYNC comply with relevant standard rules.

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

a. The description fairly presents the Leasing management software system made available to user entities of the system during some or all of the period January 01, 2025 to December 31, 2025 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

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

        1. The types of services provided, including, as appropriate, the classes of transactions processed;

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

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

        4. The process used to prepare reports or other information for user entities;

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

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

    ii. Includes relevant details of changes to the service organization's system during the period covered by the description.

iii. Does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the Leasing management software system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period January 01, 2025 to December 31, 2025 to achieve those control objectives if the user entities applied the complementary controls assumed in the design of WITSYNC's controls throughout the period January 01, 2025 to December 31, 2025. The criteria we used in making this assertion were that:

   i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization;

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

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

For **WITSYNC Soft Solutions Private Limited**

Sajal Arora
Chief Executive Officer
January 31, 2026

Enclosures:

1. Appendix 1 – Image showing technical process workflow and types of serer maintained
2. Appendix 2 – ISO Quality Management Certificate & Information Protection & Security (ISO 9001:2015 (QMS) & ISO /EMS 27001:2013 (ISMS))

SECTION 3:

WITSYNC'S DESCRIPTION OF CONTROLS

SCOPE OF REPORT AND DISCLOSURES

This description of the system of controls provided by WITSYNC Soft Solutions Private Limited ("WITSYNC") management, by referring to the relevant globally accepted applicable standards available for Attestation Engagements No. 18 '*Attestation Standards: Clarification and Recodification*', specifically AT-C Section 105, "*Concepts Common to All Attestation Engagements*' and AT-C Section 320, '*Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*' considers the direct and indirect impact of risks and controls that WITSYNC management has determined are likely to be relevant to its user entities' internal controls over financial reporting. The scope of management's description of the system of controls covers the general computer controls supporting the Leasing management software system, and considers the initiation, authorization, recording, processing, and reporting of related transactions. WITSYNC is responsible for identification of risks associated with the system of controls (defined as control objectives), and for the design and operation of controls intended to mitigate those risks. This includes the applicable information technology infrastructure and the supporting processes related to the Leasing management software system. It does not include any other processes used to initiate, authorize, record, process, or report on the financial transactions of its user entities. Additionally, WITSYNC does not maintain accountability for any user entity assets, liabilities, equity, income, or expenses.

As part of its overall SOC program, WITSYNC's management sets and determines the scope and timing of each report. This description of the system of controls has been prepared by WITSYNC management to provide information on controls build exclusively for WITSYNC Leasing Management Software:

The scope of this examination included the cloud, managed, and co-location services.

Sub-Service Organizations

WITSYNC does not rely on any sub-service organizations, except for internal software and integration applications available globally as part of the Leasing management software system included in the scope of this report. The sub-service organizations are listed as below:

S. No	Company Name	Service
01.	Php Storm by JETBRAINS	Using "php" scripting language for software base development
02.	Google	Google reCAPTCHA response code, to help in stopping bots from abusing it.
03	Google & SendGrid	For Login Authentication delivering OTP (One-Time Password)
04	GO Daddy & AWS (Amazon Web-Services)	Dedicated Private Cloud Server and related services
05.	Clam Anti-Virus	To scan for virus every document uploaded on the software tool
06.	GitHub	Assist in software development code and version controls
07.	Jira by Atlassian	Assist in planning and tracking of all releases of the software applications

Significant Changes during the Examination Period

During the examination period there were below featural changes occurred in the Leasing Management Software as part of the internal procedures to keep the software upgraded from time to time:

S. No	Area	Description
01.	Current Software Version	V.7.1
02.	Upgrades during the period from January 01, 2025 to December 31, 2025	- Added a new column on “Latest Effective Modification Date” in the Consolidated Lease Liability Report.
03.	Improvements Functions	- Yes, the management is working on improving UI/UX and adding some additional features which is still in the development and testing phase.

Using the Work of the Internal Audit Function

The service auditor did not utilize any work of an Internal Audit function in preparing this report.

OVERVIEW OF OPERATIONS AND THE SYSTEM

Company Overview and Background

WITSYNC is a provider of SaaS-based (Software as a Service) Software(s) to commercial, governmental, and not-for-profit customers across the world. WITSYNC maintains its headquarters in New Delhi, India with an office in United Arab Emirates and channel associates in rest parts of the world with a data centre facilities on GoDaddy Cloud and Amazon Web Service. WITSYNC facilities are designed to provide customers with digital financial solutions duly compliant with relevant accounting GAAPs and legal framework assisting businesses to make their accounting and finance function operate effectively and efficiently. WITSYNC's FINTECH Software offerings include customized financial technology solutions designed specifically to help organizations manage their risk and improve their overall business performance.

Overview of the Leasing Management Software System

Overviews of WITSYNC ’s Leasing management software, are as follows:

WITSYNC ’s Lessee’s Leasing Management Software

WITSYNC on May 27, 2019 launched the Leasing Management Software on principles duly compliant with IFRS 16 and equivalent standards at respective country level.

WITSYNC Managed Services

WITSYNC offers Leasing Management Software for all Global GAAP’s like, IFRS 16, IND AS 116, MFRS 16, SFRS(I) 16, TFRS (I) 16, PSAK 73, HKFRS 16, AASB 16, NZIFRS 16, & EAS 49 software. Examples of optional managed services include implementation of Leasing Management Software along with reading, and evaluation of all lease contract terms existing, transition of existing leases data into the software, valuation of lease liability and asset, and related consultancy services using the Leasing Management Software.

WITSYNC Co-location

WITSYNC provides its customers the option to fully manage their own information technology environment by hosting the Lease Management Software at their own premise servers. In its co-location service offering, WITSYNC install the Leasing Software application on customer’s premise server and customer’s IT team assumes technical ongoing support and management responsibilities. Co-location services may be bundled with certain aspects of its managed service offering, and as a result, in some cases, WITSYNC may have administrative access to customer systems.

OVERVIEW OF RELEVANT INFRASTRUCTURE

WITSYNC system is comprised of the following infrastructure components:

- ➢ Infrastructure – the server, the software application programs; and IT system software that supports application programs;
- ➢ People – the key personnel involved in the governance, operation, and use of a system;
- ➢ Procedures – the automated and manual procedures; and
- ➢ Data – transaction streams, files, databases, tables, and output used or processed by the system.

Infrastructure

The following describes the in-scope components supporting the software programming and technology framework for the Leasing Management Software system:

Cloud Server Configuration:

Description	Technical Part
Server	Ubuntu 16.04
Website URL (Wildcard SSL Protected)	https://witsync.co
Website Hosted at	Go Daddy
Database Hosted at	AWS (RDS) & Go Daddy
Backup Facility	Weekly Basis
Database Encrypted	Encrypted with 256 AES
Other Technical	8 Core CPU 32 GB RAM 400 GB SSD

Software Application:

Description	Technical Part
Front End Language (within application)	HTML 5 jQuery
Back End Language (within application)	My SQL (Database)
Server-Side Scripting Language (within application)	Laravel 5.5 (PHP Based MVC Framework)
Web Server (within application)	Nginx
Preferred Browser	Google Chrome (works with IE, Firefox, Safari)
Server Anti-virus	ClamAv https://www.clamav.net
Captcha API & OTP (within application)	Google and SendGrid
Export / Import file type (within application)	Excel / PDF

Key Responsible Staff

The roles and responsibilities of key functions include the following:

- **Chief Executive Officer (CEO)**: Mr. Sajal Arora serves as the CEO of WITSYNC
- **Chief Technology Officer (CTO)**: Mr. Himanshu Rajput Serves as CTO of WITSYNC
- **Head of Operations**: Mr. Aaditya Arora Serves as Operations Head of WITSYNC
- **Chief Information's Security Officer (CISO)** : Mr. Shailendra Kaintura Serves as CISO of WITSYNC
- **Chief Legal Advisor (CLA)** : Ms. Richa Joshi as CLA of WITSYNC

Roles	Authority & Responsibility
Chief Executive Officer (CEO)	• Responsible for handling operations, Resource Management, Point of Communication for Directions.
Chief Technological Officer (CTO)	• Responsible for end-to-end handling Software Development, Technology and Operations Management.
Head of Operations	• Responsible for operations – finance, accounts, taxation, internal teams, client relations, software products etc.
Chief Information Security Officer (CISO)	• Define Information Security Policy • Ensure the communication and understanding of the Information Security Policy throughout the organization. • Monitor the implementation of security policy established
Chief Legal Advisor (CLA)	• Accomplishes compliances within the organization at all levels and statutory regulators. • Develop and monitor all policies and procedures for use of the software legal terms, privacy, and data protection. • Prepare and file for the Trademarks, Copyrights, and Intellectual Property Rights with relevant government authorities to secure company owning rights.

Overview of Teams

Dedicated teams allocation made depending on roles and responsibilities as required to serve best satisfactory and quality services to WITSYNC's Clients.

Research Team

Inhouse research team consistently research on the new compliances and developments as may be required for the existing running fintech modules and for the new products.

The team conducts detailed research analysis including technical evaluation on how a viable fintech module can be achieved.

Development and Testing Team

The team perform the following roles:

- design and development of fintech modules
- Patch Management
- Issuing fixes and addressing bugs
- Quality and security testing

Systems Team

The system team is responsible for management of WITSYNC's infrastructure components such as demo and production servers, databases, network devices, and other tools and devices as required for the business purposes from time to time.

Legal and Compliance Team

The compliance team is responsible for overall information security governance that implements security and privacy programs, policies and procedures, Master Service Agreements, Terms of Use between WITSYNC and its' users entities and ensure compliances with the regulations on a regular basis.

Deployment Team

The deployment team responsible for maintaining the source code and enforce code check standards for the builds which needs to be deployed. The team deploy the builds into production environment.

Customer Support Team

WITSYNC customer support has several tiers of customer support. User entities report clarifications or bugs via phone/chat/email to the Client Support team. The team coordinates with relevant teams to resolve timely the reported issues.

Procedures

WITSYNC has developed, and communicated to its users open policies and procedures immediately at the time of their onboarding, the policy and procedures on how to use, restricting logical access to WITSYNC's systems, data and critical areas within, as well as procedures to protect the systems from certain threats. Policies include the following:

- Pre-determined and Pre-defined set of technical conditional workflow procedures achieving compliance objectives of the GAAPs (a highly confidential document developed internally after intensive and extensive research and testing work performed by key staff which used for development and accessible only to the Limited key staff within WITSYNC);

- Data Storage & Privacy Policy (access to detailed policy weblink - https://witsync.co/information/data-storage-privacy-policy);

- Disclaimer Policy (access to detailed policy weblink - https://witsync.co/information/disclaimer-policy);

- Data Protection Policy (access to detailed policy weblink - https://witsync.co/information/data-protection-policy);

- Terms of use Policy (access to detailed policy weblink - https://witsync.co/information/terms-of-use) ; and

- Intellectual Property Rights Policy (access to detailed policy weblink - https://witsync.co/information/intellectual-property-rights).

Data

WITSYNC systems process the customer's data, the relevant key data obtained through six (6) manual steps necessary for the purpose of valuation of lease liability and lease asset to ensure compliance with the IFRS 16 / National GAAP on Leases. The key-in data as well as the system processed data of each customer is securely protected by AES 256 Encryption.

In order to secure the customer's data in transit from web browser to web server or vice versa, an SSL Certificate is deployed in place. Secure Sockets Layer, SSL in short, is a security protocol that creates an encrypted link between a web browser and a web server. SSL use the encryption algorithm to scramble data in transit, which prevents hackers from reading it as it is sent over the connections. The data includes potentially sensitive information such as names, addresses, financial values, and other details.

The physical and logical access to systems containing customer data is limited to support personnel necessary to have such access only at times when needed (usually only at exceptional times when customer faced any bug or function not working) subject to the permissions granted by the customer. The access subject to prior approvals both internally and from the respective customer, and for a limited time period only.

RELEVANT ASPECTS OF CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATIONS SYSTEMS, MONITORING, POLICIES AND PRACTICES

Control Environment

The control environment sets the culture of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal controls, providing discipline and structure. Aspects of WITSYNC's control environment that affect the services provided and / or the system of controls are identified in this section.

Integrity and Ethical Values

The effectiveness of controls is greatly influenced by the level of integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are important elements of WITSYNC's control environment, affecting the design, administration, and monitoring of other components. The communication and implementation of ethical behaviour throughout the organization is designed to reduce the likelihood of personnel to engage in dishonest, illegal, or unethical acts.

WITSYNC enforces high ethical standards in all levels of communication to and through its employees. WITSYNC continuously audits its employees' communication with customer and outside resources to ensure compliance with these standards and addresses any issues as soon as they arise. WITSYNC emphasizes high standards during all of its interpersonal communications via meetings, email and phone calls. Any questionable acts are dealt with immediately and positive acts are recognized and acknowledged in an effort to reinforce positive/constructive behaviours. Employees who violate these standards are disciplined according to company policies.

Management Committee

WITSYNC's control consciousness is influenced significantly by its Management Committee. Attributes include the Management Committee's experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management, and its interaction with internal and external auditors. The Management Committee was formed to oversee WITSYNC's risk management ownership and accountability. The committee consists of members of senior management from different operational areas including finance, executive oversight, information technology, engineering and operations, and business development. The committee identifies elements of business risk including threats, vulnerabilities, safeguards, and the likelihood of a threat, to determine the actions to be taken.

Commitment to Competence

Management has established a framework for the basic skills necessary to perform each of the jobs at WITSYNC. This framework is then augmented with more specific requirements for each position and for additional specialization within each position based upon any other skills an employee may have. The job descriptions for each position are descriptive, but remain fairly broad because of the nature of the work for which each position is responsible. The employee understands that there are general skills that all people within their given role must have and that the job description augments those skills. A skills development program is in place that provides technical training for the continued development of information technology and engineering personnel. Training practices include staff training for support specific hardware and software components, conferences, and seminars on industry developments, technical certification courses, and newsletters and discussion forums for certain technologies.

Management's Philosophy and Operating Style

WITSYNC management philosophy and operating style is ultimately responsible for the system of internal controls. Virtually all employees have some role in controlling the organization. Some controls are established at the organization level, and management of the local unit establishes others. Management has formal policies and procedures in place to guide personnel on specific information processing functions.

Organizational Structure

Management has designed the organizational structure to provide quality service and accountability in support of WITSYNC's mission. In order to achieve quality in performance, they strive for continuous improvement in all that is done, plan and commit to accomplish targets, and are empowered to perform their duties. WITSYNC's operations are highly specialized and require the ability to adapt to industry changes and best international practices. WITSYNC has a centralized, flat management framework, which allows them to quickly react to industry changes and have excellent response times to customer needs. In addition, the CEO is an active participant in day-to-day operations and managers' report directly to him. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are available to personnel via the intranet.

Human Resource Policies and Practices

WITSYNC's human resource policies and practices are clearly written HR processes covering the employee life cycle. These policies cover on-boarding, joining formalities, credential and reference checks, payroll processing, travel, leave and attendance management, rewards and recognition, performance review, employee benefits, confidentiality, social media appearance, and employee separation. Third party service provider performs background checks for WITSYNC's associates. The checks carried out include verification of educational qualifications, and criminal checks as applicable for the associates.

All joiner's whether employee or associates are required to sign a Non-Disclosure Agreement (NDA), the employee handbook covering all provisions immediately on joining the WITSYNC.

Risk Assessment

WITSYNC is committed to managing and minimizing risk by identifying, analysing, evaluating and treating exposures that may hinder, prevent or otherwise impact the organization from achieving its goals. WITSYNC recognizes the need for risk management as a strong consideration in strategic and operational planning, day-to-day management and decision making at all levels in the organization.

The HOP and CISO is charged with development, implementation, and maintenance of the risk management strategy. The HOP or CISO is also responsible for the dissemination of the corporate Risk Assessment policy at least annually, or with any changes. Annually, the organization performs a risk assessment which includes a risk ranking considering likelihood of occurrence and impact.

Annually, or as significant changes are made within the organization that affect risk, the executive management team reviews the risk assessments and plans appropriate mitigating action plans. Risk assessments at minimum address the following:

- Operational risk – changes in the environment, staff, or management personnel;
- Security risk – Security related vulnerabilities in the Corporate and Infrastructure which may impact confidentiality of client data and availability of services;
- Strategic risk – new technologies, changing business models, and shifts within the industry;
- Compliance – legal and regulatory changes.

On an annual basis, SOC 1 and ISO 27001 independent audit certification reports are obtained. In case of any non-compliances noted in the report, the compliance team follows up to take timely corrective actions.

On an annual and continuous basis, WITSYNC performs organization wide information technology Risk Assessment as part of the ISO standards. The ISO standards identifies the processes, and related information assets that are critical to ensure information security and privacy standards are adhered across the entity and suitable corrective actions is taken, if any.

Information and Communication Systems

Information System

WITSYNC has an information security policy to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time sensitive information and processes for security and system availability purposes that notify key personnel in the event of potential security issues or system outages.

Communication System

Management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities. This includes the ability to provide necessary training to the extent that personnel understand how their daily activities and roles relate to the overall support of services. WITSYNC management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and appropriately addressed.

WITSYNC has implemented an internal corporate network to disseminate information to employees. The network is the central repository for company communications. Individual departments are charged with designing and developing their procedures. Once a procedure is finalized, it is published to the internal network for company-wide distribution. Publishing to the corporate network is performed by information technology personnel who follow a two-step process to help ensure that changes are approved prior to release to the production site. Restrictive access controls are also applied if the material being published is not intended for general viewing (e.g., certain fee structures and management guidelines).

Ticketing System

WITSYNC has developed a number of means to manage customer communication and information sharing with customers; however, the most commonly used mechanism for collecting information that may be relevant to the customer is the WITSYNC online ticketing system.

The WITSYNC online ticketing system is a web-based application that provides customers with the ability to submit issues or requests for changes to their account including changes to existing transactions and orders for new services:

1. To ensure that only authorized requests are accepted, each user is assigned a unique user ID and required to set a confidential password prior to being granted access.
2. Multi-Factor authentication via One-Time Password (OTP) function is offered to customers each time of their login to the system that ensures a high degree of security in their portal experience.
3. Once an authorized service request is received via the ticketing system, an email is automatically sent to the requester with the service request number confirming WITSYNC's receipt, and the request is then assigned to the appropriate team's queue. The team associated with the queue receives notification that a new request has been submitted to the queue. The request is assigned to the appropriate team member, who attempts to resolve the request.
4. If additional information is required, the customer is contacted, via the ticket and the request is put on hold until the information is received thus creating a continual journal of dialogue and actions.
5. The ticketing system provides WITSYNC with the ability to formally capture documentation related to the request, confirmation of receipt, work performed, and the review and approval of tickets related to customers' systems.

This system is also used internally by WITSYNC to record all alerts that are generated by monitoring software installed on customer hardware devices and to document the resolution of any issues with hardware or software.

Monitoring

WITSYNC's management performs monitoring activities in order to assess the quality of internal control over time and monitors activities throughout the year and takes timely corrective actions to address deviations from company policy and procedures. Management utilizes a risk-based approach to monitor business units and other auditable units/domains/entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed in order of significance.

Management's close involvement in operations helps to identify significant variances from expectations regarding internal controls. Upper management immediately evaluates the specific facts and circumstances related to any suspected control breakdowns. A decision for addressing control's weaknesses is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. Management's ability to actively monitor customer's communications is an integral role in controlling the quality of the services provided.

The CEO holds regular meetings with the team managers to maintain oversight of team activities and company financial positioning.

Weekly operations and senior management meetings are held to discuss monitoring activities, issues, and other relevant topics pertaining to the operation of the Leasing management software. Monitoring activities are used to initiate corrective action through meetings, calls, and informal notifications.

Management has frequent involvement in WITSYNC's operations to help identify significant variances from expectations regarding internal controls. Controls addressing high-priority risks and those most essential to reducing a given risk are evaluated more often. Additionally, WITSYNC's customer support ensures that customer complaints are brought to management's attention in weekly senior management and operations meetings. Executive management immediately evaluates the specific facts and circumstances related to any suspected control breakdowns. A decision for addressing any controls weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel.

Policies and Practices

WITSYNC is responsible for maintaining and implementing information technology controls related to cloud computing supporting the Leasing Management Software and development of other upcoming FINTECH solutions. These controls provide the basis for reliance on information / data from the systems used by user entities for financial reporting.

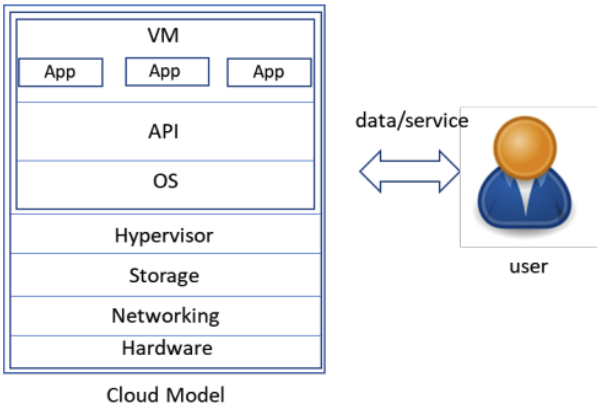
INFRASTRUCTURE MANAGEMENT

Cloud Server Security and Privacy

Cloud systems have been developed over time and conceptualized through a combination of software, hardware components, and virtualization technologies. Characteristics of the cloud, such as resource pooling, rapid elasticity, and pay-as-you-use services, have accelerated its wide adoption by industry, government, and academia. Specifically, cloud systems offer application services, data storage, data management, networking, and computing resources management to customers over a network (and the internet in general). Despite the great advancements of cloud systems, concerns have been raised about offered levels of security and privacy. The importance of these concerns becomes more evident when considering the increasing number of users that have adopted cloud services.

The architecture of a cloud system is composed, in general, by layers of functions:

- VM (Virtual Machine) including
  - Applications
  - Application Programming Interface (API)
  - Operating System (OS)
- Hypervisor
- Data Storage
- Networking
- Hardware



Cloud computing security and privacy or, more simply, cloud security refers to a broad set of policies, technologies, applications, and controls utilized to protect the virtualized IP, data, applications, services, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security, and more broadly, information security.

Cloud computing and storage provide users with capabilities to store and process their data in third-party data centre. WITSYNC use the private dedicated virtual cloud deployment model for all of their SaaS based FINTECH software.

Security concerns associated with cloud computing are typically categorized in two ways:

1) security issues faced by cloud providers (cloud server owners - Go Daddy and Amazon AWS, as deployed by WITSYNC); and
2) security issues faced by WITSYNC (hosting applications and store data on the cloud).

WITSYNC team ensures that the cloud service provider ensure that their infrastructure is secure and their client's data and applications are protected, while WITSYNC placed measures to fortify the applications

and data hosted on cloud service providers and using strong passwords and dual authentication measures restricting access only to limited key staff.

WITSYNC structured their cloud servers for demo applications separate from live production applications together with strong measures in place to restrict access to demo cloud server as well as the live production server, prior automated approval is necessary for the staff at every time accessing the server, server access is time bound, any changes migrated to live production server is accessible only after successful testing on demo server and migration possible only through the demo server application, placed strong passwords for accessing the server, and require dual authentication.

All changes to the applications and to the server are electronically maintained and are kept using a tracker with automated sequential numbering using GitHub and Jira. All changes to the application and server are passed through only after management approval and assessment following the Change Management policies and procedures as discussed below in detail.

The technical process work flow, the type of servers, and the system architect as maintained by WITSYNC is depicted in the image in Appendix 1 at the end of this report.

WITSYNC also got audited by the independent third-party ISO team who conducted the detailed audit on the "Information Protection and Security of Client Data in relation to the provision of Professional Consultancy Services including Financial Process Automation Software and E-Learning Solutions" during the period and has obtained a renewal Information Security ISO Certification in compliance with ISO/EMS 27001:2013 (ISMS) standards. Both the ISO Quality Management and Information Security Certification attached herewith in Appendix 2 of this report as a reference.

During the period of the report, there were no cloud security issues faced and reported.

Customer Provisioning

Type of Customers:

WITSYNC utilizes Master Service Agreements (MSAs) to define the terms of services provided by WITSYNC to each customer. Based on customer specific requirements, WITSYNC document the agreed upon services and communicates these service requirements to customers prior to their onboarding to the software application.

In today's dynamic digital world, WITSYNC give flexibility to their customers to choose which IT infrastructure for accessing the software application is right fit for them either On-Premise or Cloud Access, considering the time, cost, in-house IT infrastructure setup and the team etc.

WITSYNC with the aim to make the highly technically skilled FINTECH software access quick, easy, affordable, huge time saving, solving hidden problems and challenges, allowing businesses of any size having personnel with prior experience or not, inbuilt with pre-defined knowledge and logical-based checks and controls ensuring 100% compliance, developed and build the software accessible also on WITSYNC's cloud platform https://witsync.co.

Hence, the WITSYNC's customers are classified as below based on the election made by the customers accessing the WITSYNC's services:

1) **Cloud-based Access** – customers elect to access the software 24x7x365 at web link https://witsync.co hosted on WITSYNC's dedicated private cloud.
2) **On-Premise Access** – customers elect to install the software application on their in-house premise server, accessible only within their business network

Customer On-boarding Procedure:

Cloud customers upon satisfaction from preliminary demo and assessment of the WITSYNC's software application, signup by themselves on the online portal https://witsync.co agreeing to the terms of service at the time of registration and immediately upon successful registration by the customer, WITSYNC presumed an electronic contract is signed on the date and time when the successful registration completed.

For each cloud customer a unique business account created separated from other customers on the cloud server itself. Post successful registration either the customer by-self choose the appropriate plan available and complete the settings or can get in touch with the WITSYNC's team who assist in configuration and settings for use. Instantly upon one-time settings completion (estimated time assumed at or less than ten (10) minutes), the software application become ready to use for the cloud customers.

For **On-Premise customers** a formal contract with mutually decided terms is signed in case where customer demands premise installation of the software.

A "Provisioning Form" with initial customer system specifications is completed. Based on the requirements defined by the contract for premise installation, WITSYNC after assessment may require the client to purchase the required systems or equipment to support the application installation and up-running, including hardware, support software, digital certificates, or applications.

Senior Management reviews the Provisioning Form. The Network Engineering staff members enter the preliminary information from the form onto the specific checklist needed for the implementation. Once Engineering personnel have completed the initial part of the checklist, they open an internal ticket and assign it to Project Management or Senior Management for review. At this point, the Client Services Team compares the Provisioning Form with the executed contract to ensure that contractual obligations are addressed, and that the implementation plan checklist matches the Provisioning Form.

After review by the Client Services Team, the Engineering staff sets up the new system(s) on the Client's In-house premise server according to the implementation checklist and get the Quality Assurance test of the installed software application to ensure the application is up and running, complying all the parameters. They document the actual project implementation details. The completed checklists are stored electronically.

The engineering staff then opens another ticket to send the primary contact person the introductory implementation information, turning over their login credentials and thus making it a live implementation for the customer and schedule a software demo training for all concerned users thereafter.

Physical Security

WITSYNC has defined and documented Physical Security Policy which is reviewed and approved by the CTO and CEO on an annual basis. The policy includes the physical access restrictions to the WITSYNC development center.

Entry/exit points are manned 24x7 by the security personnel restricting access to authorized individuals.

Logical Security

WITSYNC has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities.

Encryption

WITSYNC follows the encryption methods as communication to the customers. WITSYNC employs the following methods of encryption:

- Encryption of data in transit
- Encryption of data at rest
- Application-level encryption

System Availability

WITSYNC has designed its network and has implemented monitoring controls to provide a 24x7x365 availability of operating system to its cloud customers accessible through web portal at https://witsync.co. Policy and procedure manuals are in place and maintained for internal network infrastructure availability, backup, and recovery.

High availability is the ultimate goal of moving to the cloud. The idea is to make the cloud services available to cloud customers at anytime from anywhere using any device (with compatible browser except mobile device) with an internet connection.

Cloud availability, cloud reliability, and cloud scalability together allow to achieve the high availability. This means that the cloud services are accessible anywhere and anytime, function reliably, and as expected, and that the system can seamlessly scale up or down to accommodate customer's demand without compromising the performance.

WITSYNC's dedicated staff keep monitoring the system availability at all times and any service interruption if arises or planned for any changes to system, have a mechanism in place to notify all the cloud customers well in advance by issuing service interruption notice.

During the period of this report, only 1 time service interruption of 3 hours at the maximum happened during the month of September 2025 in order to upgrade the cloud server configuration and an advance notice was issued to all customers.

Vulnerability Scanning & Penetration Testing

WITSYNC performs on a monthly basis vulnerability scanning to ensure application security for its cloud based software products. In case of any deviations identified, timely corrective action is taken.

On an annual basis, the security team performs penetration testing to ensure application security for its cloud software products. In case of any deviations identified, timely corrective action is taken.

The following measures taken immediately as part of the incident response:

1. Assessment of the deviations occurred
2. Notification to external and internal stakeholders
3. Development and bug fixes patch
4. Release of patch update to rectify the vulnerability
5. Complete review of authentication mechanism
6. Internal security testing and source code review
7. Re-scanning for vulnerability, if any exists

Change Management

WITSYNC performs hardware, operating system, and specific managed service changes from time to time to keep the cloud services technologically advanced and available 24x7x365 and also undertake changes on behalf of its premise customers upon receipt of a properly authorized request.

To understand the process for submission and tracking of cloud customer-requested changes, please refer to the Ticket System section of this report.

WITSYNC occasionally required to perform emergency hardware, operating system, and other specific managed changes to its cloud server in order to keep server updated time to time with the technological advancement. This typically occurs as a result of continuous advancement, monitoring functions and activities for high-risk alerts that WITSYNC determines can only be fixed by implementing a change. Such alerts arise from external security vulnerabilities, issues with hardware, services (for instance, protocols such as HTTP, FTP, SMTP, and DNS), and availability.

Customer organizations are ultimately responsible for controls that ensure the appropriate approval of changes they have requested WITSYNC to make to their business needs. The customer is also responsible for controls over the adoption and implementation of and changes to business process software applications.

WITSYNC installs standard vendor-supplied operating system updates (commonly known as patching) for on-premise customers.

WITSYNC center refers to a physically segregated and access controlled work area located in WITSYNC development center occupied by members of the WITSYNC development team. The work area refers to the physically segregated areas within the WITSYNC development center containing Laptops/desktops.

Logical access to the servers is provided through an isolated and dedicated network and is highly secured and monitored. The accessing machines are securely hardened so that no data can be copied or transferred from the data center. No visitors are allowed inside the dedicated areas within the WITSYNC centers. Only a verified restricted number of associates have the access to the servers to carry out emergencies.

Steps Followed in Change Management Process by WITSYNC:

Step 1: Initiation

A change inquiry launch by WITSYNC or any of its customer, who completes a form specifying the type of change, its potential impact, and proposed date of implementation through email. The user provides details to the reviewer of the change inquiry to ensure an appropriate action can be taken.

Step 2: Categorization

The CTO, reviews the change inquiry and allocates a unique number that designates it as a change request. This change request number enables tracking of a specific request at any time and at any stage of the process.

A change management forum's decision about a change request may categorized as one of three classes:

Accepted. The change request has some business benefit underlying with the change in the GAAPs if any, and it is worthwhile for further investigation or work to be undertaken.

Rejected. There is no business benefit and the change request are declined.

On hold/further work is needed. The forum requires further information to decide.

Based on the change requests that have been accepted, a further categorization based on a risk assessment is undertaken by the change manager and endorsed by the forum:

Type A. Change impacts multiple systems and has a customer impact. There is high technical complexity.

Type B. Change impacts one system and has a customer/business impact. There is a medium level of complexity.

Type C. Change impacts one system and there is a low level of complexity.

Step 3: Prototype Development

Once a change request has been accepted, the detailed process flow designed together with changes in functions and outcomes. Based on such technical study, a prototype is developed by the Engineering team.

Step 4: Testing

Once a prototype developed based on change request assessment, the changes pushed to the demo server for the technical team to make simulation testing and evaluate whether the changes meeting the requirements and desired outcomes.

Step 5: Quality Testing

Once the developed code is tested, the Quality Assurance team executes the quality tests on the build in the local (testing) environment.

Step 6: Release Decision

Once a prototype developed based on change request assessment, it is presented to the management forum to ascertain whether the change meeting the requirements can be released to the live production environment. This release decision is based on the risk assessment decision made in step 2.

Step 7: Migration

The actual migration of the change is completed by a person who is independent from the development team to mitigate risk that unauthorized changes may be made to production code after detailed testing and assessment.

Step 8: Emergency Changes

At times, urgent emergency changes may be needed as an exception but such requests require to pass through minimum assessment and approvals to work and deploy. WITSYNC has developed an emergency change management process, with authorization from CTO and CEO. Once the change is implemented, the key participants in the change conducts a post-implementation review to ascertain the impact of the change to the process and system and report the findings to the forum.

Step 9: Reporting and Tracking

All change inquiries and requests are reported to WITSYNC's CTO and CEO on a regular basis. An automated change management system can track and report on each unique change request number at any point in time.

Incident Handling

WITSYNC has defined an Incident Management System Policy, which is reviewed annually.

Based on the inputs received via email/chat/phone/desk, the incident management team coordinates with relevant stakeholders to analyze the potential impact of the security incident. The relevant team performs root cause analysis (RCA) and updates the security incident in the Ticketing Management tool. The corrective actions are taken on a timely basis and preventive measures are deployed to prevent future incidents.

The alerts are triggered by the monitoring tools and once an alert is triggered an automated entry of an event is created and a downtime post is made to notify the stakeholders, where necessary. The relevant product team performs RCA and the action points are identified for implementation. The incident ticket is updated.

Information Security

Access to the company network is restricted to organizational workstations and other approved devices. Unique accounts requiring user name and password are required to access workstations. Passwords to log on to user accounts are managed by Active Directory, and maintain minimum length and complexity requirements.

Remote support of customer systems can be performed through use of an authenticated VPN. User name and password are required for employees to authenticate to the secured VPN.

WITSYNC uses commercially available firewall applications for Managed Services (Firewall) customer systems. WITSYNC monitors and manages logical access to the managed firewalls on both a preventative and a detective level through the use of detective controls, processes, and technology.

WITSYNC also maintains logging (syslog) servers on a continuous basis to monitor each activity (24x7x365). They are configured to retain a minimum of 90 days of activity.

Backup Processes

WITSYNC's standard backup configuration for cloud hosted services is to automatically perform weekly backups of systems database. On-premise server customers receive no backups from WITSYNC unless contracted and they shall be taking backups at their premise server itself. Customers' production data and operating system files are automatically backed up daily on an incremental basis and weekly on a full basis. Operations staff members use commercially viable backup software systems.

Backup jobs are configured to send either daily reports or real-time error notifications to WITSYNC's Engineering and Operations staff. Engineering staff members monitor the error notifications and start a ticket to notify the Engineering staff to review the operations log from the backup servers to diagnose the issue. If necessary, the Engineering Staff completes a ticket to document backup job restarts and corrections and route the ticket as appropriate based on the nature of the relationship with the customer.

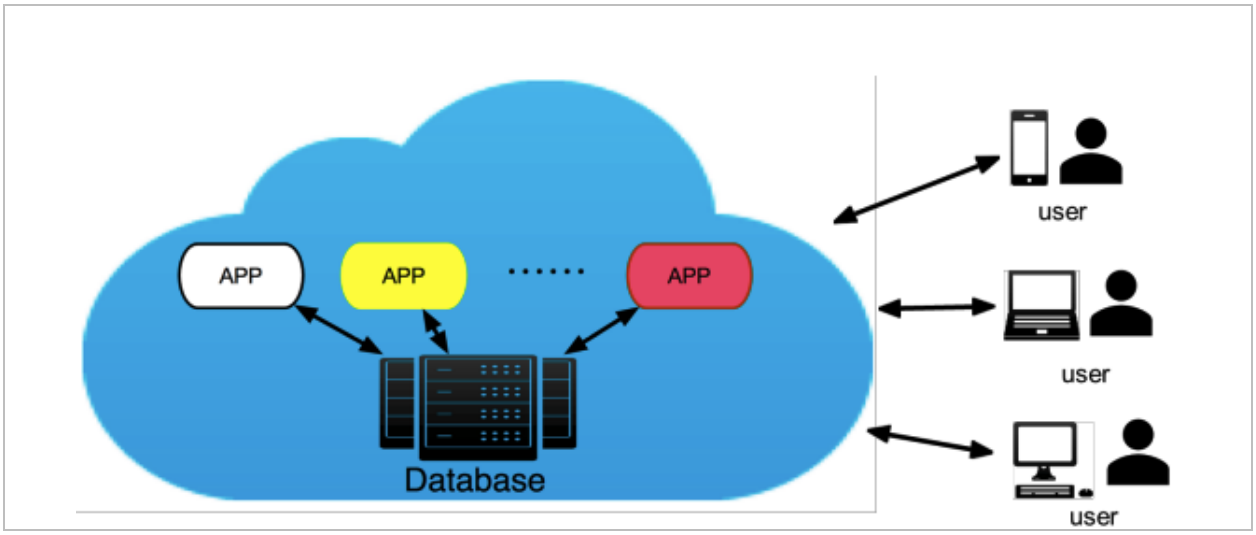
Network Monitoring

Network monitoring is performed by WITSYNC to monitor the availability of network connections to customers hosted on WITSYNC facilities. WITSYNC management has documented the incident response policies and procedures in place to guide personnel in network outage response, escalation, and resolution activities.

WITSYNC utilizes an enterprise monitoring application to monitor the status of the networking systems provided to WITSYNC's customers. The monitoring application monitors considerations such as, availability of the network, host services and ports, IP packet transmissions and loss. The enterprise monitoring application is configured to send e-mail alert notifications to IT personnel when predefined thresholds are exceeded on monitored systems and provides statistical reports to monitoring personnel. The monitoring personnel of WITSYNC are available 24x7x365 to monitor and resolve networking issues affecting WITSYNC customers. A ticketing system is utilized to manage system incidents, response, and resolution.

Data Access Controls to Cloud-based SaaS Applications

In SaaS based business operating model, WITSYNC delivers an application as a service to its cloud customers through a network such as the internet. Thus, there is no need for cloud customers to install and execute applications locally on their own computers. As shown below, cloud customers have access to the cloud-based SaaS application via internet from anywhere anytime through any device (except mobile) to store data for processing transactions to obtain a desired outcome.



WITSYNC takes all measures to secure and protect the data in the cloud-based applications stored and processed by the cloud customers from any unauthorized access. WITSYNC implemented AES 256 Encryption Layer to encrypt the data in the cloud system.

Note that data entered and processed by the application layer is owned and controlled by the cloud customer only. WITSYNC is responsible for the access controls of all operation layers except the customers application data entered by the cloud customers. However, WITSYNC responsible for data retention, data backups providing data access only to data owners via system front-end application.

Multiple Tenancy

The SaaS system introduces additional consideration with regard to the management of access to software applications. An immediate necessity is to focus on user's access to software applications. The access rights are granted to end users using the access control policy and procedures based on predefined attributes or roles.

The SaaS model is a typical, multi-tenancy platform that supports multiple customers and their multiple users simultaneously accessing an application with the data of different customers residing on the same server. WITYSNC implemented multiple tenancy segregating data of one customer from different customer accessing the software application during the design of an access controls.

Attribute and Role Management

In the SaaS system, attribute or role-based access control management employs policies and predefined roles to manage access rights to applications and underlying databases.

WITSYNC designed the role-based access controls to the software application where customer's super admin can create multiple roles defining which sections access to be granted.

User Administration

Setting up User Access Management on WITSYNC Leasing Management Software Solution is simple—the new client user can be up and running in ten (10) minutes.

1. When any new client's user signup a new unique business account gets created and emailed to the respective user, the Leasing Software allot the access for the new client user with super admin rights by default and the user will get access to the Leasing Software only post email verification.
2. Once the email verified for the admin user, every time access to the Leasing Software requires every user to authenticate their access via OTP (One Time Password) send on their email address.
3. Upon first access, the client's admin user requires to setup his account and can add multiple sub-users as requested to WITSYNC.
4. WITSYNC authenticate every new business account on the Leasing Software Platform and cross verify the company details so that the company on board is with valid credentials and upon any misleading information from client, WITSYNC holds right to cancel the account.
5. User Administrators have access to a single console for all of WITSYNC's products. Here, user can manage sub-users, what sections they have access to, and which applications user run within WITSYNC.
6. Other features include changing username formats, and even creating new users to include in your company that don't already exist within WITSYNC's database or can remove any sub-user at any time. You can do this under the settings user's management and my profile.
7. Under the history section of the respective lease under the valuation menu tab allows you to see user when submitted the lease with date and time.

That means you can rest assured that your bases are covered, your teammates can be efficient, and everyone has access to the tools they need.

All users added by the client's admin including the admin itself on the Leasing Software shall become part of authorized users list who can only be allowed to access the Software.

Privilege Access Management

WITSYNC developed the privilege management system involving adding, removing, and changing the privileges for both WITSYNC's staff accessing the cloud computing server, systems, applications, and for customers accessing the front-end software application. The privilege management system designed as flexible and on real-time mechanism for assigning and revoking privileges to maintain the usability of the SaaS service.

WITSYNC's for their internal staff designed hierarchy-based privilege access management. The CEO and CTO with dual authentication only has the final authority to approve or disapprove any actions.
The customers super admin user can define privilege access of adding, removing, and changing the privileges of sub-users under the user's management settings section of the software application.

Each sub-user restricted with the access to the leasing software as defined by the respective customer's super admin user.

Any changes to the settings of the software application shall be allowed only to the customer's super admin user and sub-users can access only section allowed except settings.

Authentication Controls to the Leasing Software Application & Operating Systems:

Leasing Software every time authenticate access of every authorized user only after validation of a One-Time Password (OTP) send to respective user's email id.

Leasing Software will never allow the user to access the software with wrong OTP. Every OTP shall be valid only for a period of 10 Minutes and expires after 10 minutes.

Every access to the operating systems and database is allowed only to the WITSYNC's authorized internal staff by following the access controls placed.

Every access by the authorized staff to the operating systems and database is inbuilt with 2-step authentication controls that also requires access approval from the Head of IT.

Security settings for account lockout, password minimum length and password history are configured for authentication into Domain and also for the server infrastructure. Users are required to use two-factor authentication to connect to the server and applications.

The compliance officer established a "Data Access Request Policy" that defines authentication of data subjects into system and how the entity personnel are to respond to requests by data to access their information which is also subject to prior written approval of the client's owning the data.

Patch Management

Patch management is the process of distributing and applying updates to software. These patches are often necessary to correct errors (also referred to as "vulnerabilities" or "bugs") in the software.

WITSYNC policy on patch management serves to address :

Security	Patch management use to fix vulnerabilities in the software and applications that are susceptible to cyber-attacks, help in reducing the security risk.
System Uptime	Patch management ensures the software and applications are kept up-to-date and run smoothly, supporting system uptime.
Compliance	With the continued rise in cyber-attacks, businesses are often required by regulatory bodies to maintain a certain level of compliance. Patch management is a necessity in adhering to compliance standards.
Feature Improvements	Patch management can go beyond software bug fixes to also include feature/functionality updates. Patches can be critical in ensuring to have the latest up-to-date software and application.

WITSYNC follow the below step-by-step procedure complying with its patch management policy:

S No	Activity	Description
01	**Up-to-date Software Versions**	A proper system is in place to monitor each single change in the software by maintaining and defining versions in a sequential and chronological order for every change pushed. This helps to keep the track of all changes with date and time, description of change, and up-to-date software.
02	**Standardizing**	Although difficult to execute on, standardizing makes patching faster and more efficient. Standardizing accelerate the remediation process as new patches are released. This helps in saving time spent on remediating.
03	**Security Controls**	Keeping track of all firewalls, antivirus, and vulnerability management tool.
04	**Compare reported vulnerability against version**	Using the vulnerability management tool time to time to assess which vulnerabilities exist under which type of version in the ecosystem. This helps in understanding the security risk at which level. The latest Vulnerability check was run on December 27, 2025 where 11,221 total checks run, passed 11,191 checks, medium level issues 0, low level issues 12, noise 16, failed 3. The issues reviewed by the technical team and appeared as by-default normal. However, management shall consider the address issues in the due course of time.
05	**Classify the risk**	The vulnerability management tool allows to easily manage which software, application, and version to be consider critical, and accordingly, prioritize what needs to be remediated.
06	**Develop a Patch and Test**	Develop the patch as and when the necessity arises for the concerned area and apply in the demo testing environment. Stress test the software application to ensure that the patch will not cause issues in the live production environment.

07	**Apply the patch**	After intensive successful stress testing passing through all the test parameters, checks and controls checklist, achieving the desired outcome – a new version type defined and approved by the management and push the relevant patch to the live production environment. An immediate stress test of the live production environment also conducted by the Compliance team ensuring the smooth operations.
08	**Track progress**	Reassess from time to time the software applications to ensure patching was successful.

Business Continuity:

WITSYNC has defined Business Continuity Plan and Disaster Recovery procedures which is reviewed and approved by the management on an annual basis.

WITSYNC has a Disaster Recovery Data Center (DR DC) to ensure the business continuity. On a periodic basis, the team switches the applications and services between the Main DC and DR DC to check and evaluate the Business Continuity Plan readiness and also perform DC maintenance operations, if required.

CONTROL OBJECTIVES AND RELATED CONTROLS

The control objectives and related controls are included in Section 4 of this report, “Control Descriptions, Related Controls and Tests of Operating Effectiveness”, to eliminate the redundancy that would result from listing them in this section and repeating them in Section 4. Although the control objectives and related controls are included in Section 4, they are, nevertheless, an integral part of the service organization’s description of controls.

COMPLEMENTARY CONTROL CONSIDERATIONS

Transaction processing support for user entities as performed by WITSYNC's software application and the control activities at WITSYNC cover only a portion of the overall internal control for each user entity. It is not feasible for the control objectives related to the cloud computing software system to be solely achieved by WITSYNC. WITSYNC's controls over the systems and infrastructure supporting the Leasing management software system were designed with the assumption that certain controls would be in place and in operation at the user entities. User entity internal controls must be evaluated, taking into consideration WITSYNC's controls and their own internal controls. WITSYNC does not make any representations regarding responsibility related to or provide any assurance in regard to any such internal control or regulatory requirements for which the client must assess or comply.

This section describes some of the control considerations for the user entities, or "complementary controls", which should be in operation at the user entities to complement the controls at the service organization. User auditors should determine whether the user entities have established controls to ensure that control objectives within this report are met. The "complementary controls" presented below should not be regarded as a comprehensive list of all controls that should be employed by the user entities. There may be additional control objectives and related controls that would be appropriate for the processing of user transactions that are not identified in this report.

Control Considerations for User Entities

Physical Security

1. User entities are responsible for determining whether WITSYNC 's security infrastructure is appropriate for its needs and for notifying WITSYNC of any requested modifications.
2. User entities are responsible for establishing and adhering to security procedures to prevent the unauthorized or unintentional use of WITSYNC's facilities, information systems and infrastructure.
3. User entities are responsible for providing and maintaining a list of authorized personnel, vendors, and contractors as well as changes to technical or administrative contact information.
4. User entities are responsible for terminated employees with access to the WITSYNC's software application within a timely manner.

Network Monitoring

5. User entities are responsible to ensure there internal systems are connected to network -internet or intranet to access the software application

Customer Provisioning

6. User entities are responsible for securing appropriate approval of new implementation.
7. User entities are responsible for establishing logical access controls to limit their employees' access to WITSYNC's ticket system for the purpose of requesting any changes to customer environments and requesting changes to physical access controls.
8. User entities are responsible for providing and maintaining a list of authorized customer contacts with the ability to initiate changes to subscribed services.
9. User entities are responsible for creating and communicating specific escalation procedures for problems with their services and for notifying WITSYNC of changes to their escalation procedures.

System Availability and Monitoring

10. User entities are responsible for maintaining network connectivity to the WITSYNC's cloud application.
11. User entities are responsible for initiating any requests for WITSYNC to verify it has met the agreed-upon levels of availability for a given month.

Change Management

11. User entities are responsible for obtaining appropriate approval of requested changes to their environments.
12. User entities are responsible for implementing and changing business process software applications policies and procedures.
13. User entities are responsible for providing updated contact information for their designated primary and secondary emergency-level contact personnel.
14. User entities are responsible for providing updated contact information for their designated primary and secondary standard version update contact personnel for Managed Service systems.
15. User entities are responsible for obtaining appropriate approval of security-related emergency changes within Managed Service systems.
16. User entities are responsible for notifying WITSYNC if it chooses to opt out of standard version updates for Managed Service systems.
17. User entities are responsible for requesting any modifications to the existing access control lists (ACLs) or firewall policies within Managed Service systems.
18. User entities are responsible for providing specific workstation and/or network addresses it authorizes to access system management ports within Managed Service systems.

Information Security

19. User entities are responsible for monitoring user accounts and administrative activity on WITSYNC’s systems.
20. User entities are responsible for establishing logical access controls that define authorizations and security profiles within Hosted and Managed Service systems and for ensuring the assignment of users to these profiles.
21. User entities are responsible for creating, maintaining, and disseminating their own Information Security Policy for their environment(s).

Backup Processes

22. User entities are responsible for requesting data restorations through the ticketing system for premise hosted applications.
23. User entities are responsible for securing approval of restorations for premise hosted application.

SECTION 4:

CONTROL DESCRIPTIONS, RELATED CONTROLS AND TESTS OF OPERATING EFFECTIVENESS

INFORMATION PROVIDED BY THE SERVICE AUDITOR

This report is intended to provide user entities with information about controls that may affect the Leasing management software system provided by WITSYNC and to provide information about the operating effectiveness of controls that were tested. This report, when combined with an understanding of the internal controls in place at user entities, is intended to assist the preparation of the financial statements. It may be used in assessing control risk associated with user entity financial statement assertions that could be impacted by the Leasing Management Software system provided by WITSYNC.

The scope of our testing of WITSYNC's controls was limited to the control objectives and the related controls specified by WITSYNC and contained within Section 4 of this report, which management believes to be the relevant key controls for the objectives stated. Our review was not extended to controls in place at any user entities or any other third-party vendors.

The examination was performed by referring to globally accepted relevant standard available as was issued by the American Institute of Certified Public Accountants ("AICPA") Standards for Attestation Engagements No. 18 '*Attestation Standards: Clarification and Recodification*', specifically AT-C Section 105, '*Concepts Common to All Attestation Engagements*' and AT-C Section 320, '*Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*.' It is each interested party's responsibility to evaluate this information in relation to controls in place at user entities and sub-service organizations (if applicable) to obtain an overall understanding of internal control and to assess control risk. Controls in place at user entities, sub-service organizations (if applicable), and WITSYNC's controls must be evaluated together. A general, but not inclusive, listing of control considerations is provided in Section 3, "Complementary Control Considerations." If an effectively operating user entity or sub-service organization (if applicable) internal control is not in place, the controls at WITSYNC may not sufficiently compensate the deficiency.

Tests of Operating Effectiveness

Our tests of the operating effectiveness of the controls specified by WITSYNC included such tests as we considered necessary in the circumstances to obtain reasonable, but not absolute, assurance that the controls operated in a manner that achieved the specified control objectives during the period from January 01, 2025 to December 31, 2025. In selecting particular tests of the operating effectiveness of controls we considered:

1) the nature of the controls being tested;
2) the types and completeness of available evidential matter;
3) the nature of the control objectives to be achieved;
4) the assessed level of control risk;
5) the expected efficiency and effectiveness of the test; and,
6) the testing of other controls relevant to the stated control objectives.

Testing exceptions, if any, and information about specific tests of the operating effectiveness performed that may be relevant to the interpretation of testing results by user entities for the controls specified to achieve the stated objective are presented in this section under the column heading "Results of Testing". Exceptions identified herein are not necessarily considered significant deficiencies or material weaknesses in the total system of internal controls of WITSYNC, as this determination can only be made after consideration of controls in place at user entities. Control considerations that should be exercised by user entities in order to complement the controls of WITSYNC to attain the stated objectives are presented in relation to the nature of services being audited and the controls specified by WITSYNC.

Types of Tests Performed

The table below describes the nature of our audit procedures and tests performed to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Test Types	Description of Tests
Inquiry	Inquired of appropriate personnel seeking relevant information or representation to obtain the following information about the control: ➢ Knowledge and additional information regarding the policy or procedure; and ➢ Corroborating evidence of the policy or procedure.
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: ➢ Examination / Inspection of Leasing Management Software to verify sample transactions processing; ➢ Examination / Inspection of systems documentation, configurations and settings; and ➢ Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.
Observation	Observed the implementation, application or existence of specific controls as represented.
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed.

Sampling Methodology

The table below describes the sampling methodology utilized in our testing to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

S.No	Type of Control and Frequency	Test Samples	Transitional Valuation Approaches			
			Modified Retrospective Approach (Without Adjusting Opening Equity)	Modified Retrospective Approach (By Adjusting Opening Equity)	Full Retrospective Approach	Post Transition Leases
01.	**Organization Controls**	Systems and policies review	-	-	-	-
02.	**GAAP Compliance**					
02.1	Short-Term Lease	At least 1	-	-	-	-
02.2	Long-term Lease		At least 1	At least 1	At least 1	At least 1
02.3	Users Access & Controls	At least 1	-	-	-	-
02.4	Lease & Non-Lease Components		At least 1	At least 1	At least 1	At least 1
02.5	Subsequent Modifications		At least 1	At least 1	At least 1	At least 1
02.6	Valuation of Dismantling Provision		At least 1	At least 1	At least 1	At least 1
02.7	Consolidated Lease Report, Lease Accounting Report, and Maturity Analysis Report		At least 1	At least 1	At least 1	At least 1
03.	**Cloud Server Security**	Test at least one operation of each relevant control	-	-	-	-
04.	**Customer Provisioning**		-	-	-	-
05.	**Systems Availability**		-	-	-	-
06.	**Change Management**		-	-	-	-
07.	**Information Security**		-	-	-	-
08.	**Backup Processes**		-	-	-	-
09.	**Network Monitoring**		-	-	-	-

TARUN KANDHARI Digitally signed by TARUN KANDHARI Date: 2026.01.31 18:45:54 +05'30'

TESTING MATRICES

01. Organization Controls

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that, relevant to user entities' internal control over financial reporting, the Leasing Management Software ensures compliance with the relevant Generally Accepted Accounting Principles (GAAP).

S No	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.1	WITSYNC has a defined organizational structure establishing the key areas of authority and responsibility, lines of reporting and defined roles which is reviewed and approved by Senior Manager-HR on an annual basis.	Inspected the Organizational chart and the email communication for aspects such as 'name of the document', 'contents of the organizational chart', 'document prepared by', 'prepared on', 'approved by' and 'approved on' to ascertain whether WITSYNC had a defined organizational structure establishing the key areas of authority and responsibility, lines of reporting and defined roles which was reviewed and approved by Senior Manager-HR on an annual basis.	No relevant exceptions noted.
1.2	WITSYNC HR Team has defined job descriptions specifying the responsibilities for key job positions and approved by the Senior Manager- HR on an annual basis.	Inspected the Policy Description Manual for the aspects such as 'Name of the document', 'details of the policy', 'version no.', 'number of jobs defined', 'prepared by', 'prepared on', 'approved by' and 'approved on' to ascertain whether WITSYNC HR Team had defined job descriptions specifying the responsibilities for key job positions and approved by the Senior Manager-HR on an annual basis.	No relevant exceptions noted.
1.3	Upon a new associate joining, an induction training is conducted by the Training Team and HR Team to make the associate aware of the information security practices and various policies of WITSYNC. The attendance for the training is captured in WITSYNC people.	Inspected the attendance register in WITSYNC People for sample newly joined associates for aspects such as 'employee name', 'date of attendance (issued time)', 'date of joining' and 'contents of induction deck' to ascertain whether upon a new associate joining, an induction training was conducted by the Training Team and HR Team to make the associate aware of the information security practices and various policies of WITSYNC and whether the attendance for the training was captured in WITSYNC people.	No relevant exceptions noted.

TARUN KANDHARI
Digitally signed by TARUN KANDHARI
Date: 2026.01.31 18:46:30 +05'30'

1.4	WITSYNC has constituted a Privacy Team which is responsible for implementing and maintaining the data privacy program at WITSYNC. Privacy team report to the Director of Compliance who in- turn reports to the CTO/CEO.	Inspected the RACI Matrix on aspects such as such as 'preparer', 'version no.', 'reviewer', 'approver' and 'version history' to ascertain whether WITSYNC had constituted a Privacy Team which was responsible for implementing and maintaining the data privacy program at WITSYNC. Inspected the Employee Tree Structure within application on aspects such as 'organization structure', 'employee name', 'role name' and 'reporting details' to ascertain whether privacy team reported to the Director of Compliance who in-turn reported to the CTO/CEO.	No relevant exceptions noted.
1.5	Upon joining WITSYNC, the associates are required to sign a Non-Disclosure Agreement (NDA), Acceptable Use Policy, Anti-Harassment Policy and Social Media Policy on their first day of employment.	Inspected for the sample newly joined employees the documents signed by associates for aspects such as 'employee ID', 'Full name', 'date of joining', and 'date of signing the document' to ascertain whether upon joining WITSYNC, the associates were required to sign a Non-Disclosure Agreement (NDA), Acceptable Use Policy, Anti-Harassment Policy and Social Media Policy on their first day of employment.	No relevant exceptions noted.
1.6	A contract is defined, documented and approved between WITSYNC and third parties for services in relation to hosting of servers. Any changes to the contracts are agreed by WITSYNC and the third parties. The contract includes the scope of services to be provided, confidentiality and other related commitments / clauses.	Inspected for sample third parties the agreement document signed between WITSYNC and third party vendor for aspects such as 'scope', 'confidentiality clause', 'validity', 'type of service', 'agreement signed by' and 'agreement signed on' to ascertain whether a contract was defined, documented and approved between WITSYNC and third parties for services in relation to hosting of servers and any changes to the contracts were agreed by WITSYNC and also whether the contract included the scope of services to be provided, confidentiality and other related commitments/clauses.	No relevant exceptions noted.
1.7	WITSYNC has defined an organization wide "Integrated Information Security & Privacy Manual" which specifies the information security and privacy requirements and also defines the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team). It is prepared by Compliance / Privacy Team and approved by the Management team and is reviewed by Information Compliance Manager on an annual basis.	Inspected Integrated Information Security and Privacy Manual document for aspects such as 'name of the policy', 'contents of policy', 'version no.', 'prepared by', 'approved by', 'reviewed by', 'reviewed on', 'approved on' and 'contents of the policy' to ascertain whether WITSYNC had defined an organization wide "Integrated Information Security & Privacy Manual" which specified the information security and privacy requirements and also defined the related roles and responsibilities (Information Security team, Compliance team, Data Protection Officer, Privacy team, IT Service management team) and whether it was prepared by Compliance / Privacy Team and approved by the management team and was reviewed by	No relevant exceptions noted.

		Information Security Compliance Manager on an annual basis.	
1.8	Risk assessment is performed annually by WITSYNC Privacy Team to assess the risk of sub processors identified by them and identify suitable risk treatment plan on an annual basis.	Inspected for sample sub-processors the Risk Assessment performed for aspects such as 'name of vendor', 'service description' and 'applicable services' and 'Risk assessment details' to ascertain whether Risk assessment was performed annually by WITSYNC Privacy Team to assess the risk of sub processors identified by them and identify suitable risk treatment plan on an annual basis.	No relevant exceptions noted.
1.9	WITSYNC has defined organization wide Privacy policy that covers aspects such as limitation of collection, processing of information, notice, uses and disclosure. The Policy is prepared by Legal Team, approved by Compliance and is reviewed by Management on an annual basis.	Inspected Privacy Policy document for aspects such as 'name of the policy', 'contents of policy', 'version no.', 'preparer', 'reviewer', 'approver' and 'date of approval' to ascertain whether WITSYNC had defined organization wide Privacy policy that covers aspects such as limitation of collection, processing of information, notice, uses and disclosure and whether the Policy was prepared by Legal Team, approved by Compliance and was reviewed by Management on an annual basis.	No relevant exceptions noted.
1.10	Support documents including the system flow diagrams and other design documents for the products are maintained and are made available to the respective team members of WITSYNC.	Inspected the supporting documents for the sample products for aspects such as 'Product details', 'Category' and 'availability' to ascertain whether support documents including the system flow diagrams and other design documents for the products were maintained and also whether they were made available to the respective team members of WITSYNC.	No relevant exceptions noted.
1.11	Product descriptions, help documents and terms of usage / service are defined and are made available for to the customers via corporate website.	Inspected the corporate website for sample products for aspects such as 'Product name', 'website - URL where the document is hosted' and 'contents' to ascertain whether product descriptions, help documents and terms of usage / service were defined and were made available for to the customers through corporate website.	No relevant exceptions noted.
1.12	Security settings for account lockout, password minimum length and password history are configured for authentication into Domain, WITSYNC accounts, and also for infrastructure. Users are required to use two-factor authentication to connect to infrastructure from authorized IP network.	Inspected the password configuration in Domain Controller, WITSYNC accounts and infrastructure for aspects such as 'Password Configuration and Complexity', 'Session Configuration', and 'authorization upon every logon' and 'Multi-factor Authentication' to ascertain whether security settings for account lockout, password minimum length and password history were configured for authentication into Domain, for WITSYNC accounts, and also whether users are required to use two-factor authentication to connect to the infrastructure	No relevant exceptions noted.

TARUN KANDHARI
Digitally signed by TARUN KANDHARI
Date: 2026.01.31 18:47:45 +05'30'

		from authorized network.	
1.13	Antivirus software is installed in the user work stations and the latest updates and definitions are pushed automatically to the workstations on a periodical basis.	Inspected for sample workstations the antivirus installation and configuration for aspects such as 'workstation ID', 'AV version', 'Synchronization interval', 'AV last update date' and 'AV release date' to ascertain whether antivirus software was installed in the user work stations and the latest updates and definitions were pushed automatically to the workstations on a periodical basis.	No relevant exceptions noted.
1.14	WITSYNC has defined and documented policies for retention and disposal of client information upon discontinuation of WITSYNC services, which is hosted in the corporate website as part of WITSYNC policies available to end users.	Inspected Privacy Policy document hosted in WITSYNC corporate website for aspects such as 'policy name', 'contents of policy' and 'availability of policy' to ascertain whether WITSYNC had defined and documented policies for retention and disposal of client information upon discontinuation of WITSYNC services, which was hosted in the corporate website as part of WITSYNC policies available to end users.	No relevant exceptions noted.
1.15	WITSYNC has defined Business Continuity Plan and Disaster Recovery procedures which is reviewed and approved by the Compliance Leadership team on an annual basis.	Inspected Business Continuity & Disaster Recovery Plan document for aspects such as 'name of the document', 'Contents', 'Prepared by' and 'reviewed and approved by' to ascertain whether WITSYNC had defined Business Continuity Plan and Disaster Recovery procedures which was reviewed and approved by the Compliance Leadership team on an annual basis.	No relevant exceptions noted
1.16	On an annual and continuous basis, WITSYNC performs organization wide Information Technology Risk Assessment as part of the ISO standards (27001 and 9001). The ISO standards identifies the processes, and related information assets that are critical for WITSYNC to ensure information security and privacy standards are adhered across the entity and suitable corrective action is taken, if any.	Inspected Information Technology (IT) Risk Assessment report for aspects such as 'ISO Assessment performed on', 'Location', 'Criteria', 'Domains' 'Validity' and 'Corrective action' to ascertain whether on an annual and continuous basis, WITSYNC performed organization wide Information Technology Risk Assessment as part of the ISO standards (27001 and 9001) and also whether the ISO standards identified the processes, and related information assets that were critical for WITSYNC to ensure information security and privacy standards were adhered across the entity.	No relevant exceptions noted
1.17	In case of an associate leaving WITSYNC, the HR team disables the account in WITSYNC People (Control Panel). The HR notifies the SysAdmin team and the SysAdmin team disables all the logical access of the associate.	Inspected for sample associates leaving WITSYNC, the IT Incident Request ticket for aspects such as 'associate name', 'last working day', 'request ID', 'requested by', 'requested on' 'date of leaving' and 'Date of disabling' to ascertain whether when an associate was leaving WITSYNC, the HR team disabled the account in WITSYNC People (Control Panel) and notified the SysAdmin team who disabled all the logical access of the associate.	No relevant exceptions noted

TARUN KANDHARI Digitally signed by TARUN KANDHARI Date: 2026.01.31 18:48:10 +05'30'

1.18	The policies and procedures covering the logical access and network operations are defined by the Senior Engineer as part of the Network Operations - Policies and Procedures document and is approved by the CTO on an annual basis. This policy available to the designated team members.	Inspected Network Operations- Policy and Process for aspects such as 'contents of policy', 'version no.', 'prepared by', 'approved by' and 'approved on' to ascertain whether the policies and procedures covering the logical access and operations of network were defined by the Network Project Coordinator/ Senior Engineer as part of the Network Operation - Policies and Procedures document and is approved by the CTO on an annual basis. Inspected WITSYNC Network intranet site for aspects such as 'policy name' and 'availability of policy' to ascertain whether this policy available to the designated team members.	No relevant exceptions noted
1.19	Logical access to the tools (managed by team) used for performing daily operations are granted by Senior network member based on approval by CTO and revoked on a timely manner based on the approval of the CTO in the WITSYNC tool where the request is raised by the Senior Network Member.	Inspected sample access requests for aspects such as 'ID', 'Added time', 'Name', 'Access required to tool' and 'approver mail ID' and 'Approval status' to ascertain whether logical access to the tools (managed by Network team) used for performing daily operations were granted based on the approval of the member in the WITSYNC tool where the request was raised by the Senior Member. Inspected sample access revocation for aspects such as 'ID', 'Name', 'Access to tool', 'request date', 'disabled time' to ascertain whether logical access to the tools (managed by team) used for performing daily operations were revoked by the Senior Member based on the approval of the CTO in the WITSYNC tool where the request was raised by the Senior Member.	No relevant exceptions noted
1.20	Network diagram detailing the network devices such as firewalls and switches is maintained by the Network Manager. Further, access to the network devices are restricted to designated members to prevent unauthorized access.	Inspected the network diagram and email communication between Senior Engineer- Network and Manager- Network for aspects such as 'scope', 'network devices', 'prepared by', 'approved by' and 'roles provided to the users' to ascertain whether network diagram detailing the network devices such as firewalls and switches was maintained by the Manager. Inspected the access listing of users having access to network devices for aspects such as 'user', 'role' and 'rationale for access' to ascertain whether access to the network devices were restricted to designated members to prevent unauthorized access.	No relevant exceptions noted

1.21	WITSYNC maintains an asset register for its IT Assets. In case of any additions, replacements or removal of IT Assets including the software, workstations, network devices, storage etc., a ticket is raised and is approved by the Manager or SysAdmin.	Inspected the assets register for aspects such as 'Location', 'asset details captured', 'responsibility' to ascertain whether WITSYNC maintained an asset register for its IT Assets. Inspected the approval for sample tickets for aspects such as 'request ID', 'asset type', 'requestor type', 'description', 'approver email' and 'approval status' to ascertain whether in case of any additions, replacements or removal of IT Assets including the workstations, network devices, storage etc., a ticket was raised and was approved by the Manager or SysAdmin.	No relevant exceptions noted
1.22	Patches and upgrades in relation to the infrastructure (Operating System and Databases) are initially tested in a local environment/ test lab, then moved to production following which these changes are implemented after obtaining approval from the CTO/CEO.	Inspected for sample patches the tickets for aspects such as 'patch ticket ID', 'requestor name', 'patch tested by- local environment' and 'approval details' to ascertain whether patches and upgrades in relation to the infrastructure (Operating System and Databases) were initially tested in a local environment/ test lab, then implemented after obtaining approval from the CTO/CEO.	No relevant exceptions noted
1.23	On a half-yearly basis, the Network Engineers review the existing firewall rules and the same is approved by the Manager. In the case of any deviations noted during the firewall review, the Engineer makes the necessary changes in the firewall ruleset and tracks the deviations to closure.	Inspected for a sample half-year the request ticket raised for firewall rule review for aspects such as 'ID', 'ticket type', 'subject', 'approved by', 'approved on', 'deficiencies observed in the review', 'action taken' and 'ticket closed date' to ascertain whether on a half-yearly basis, the Network Engineers reviewed the existing firewall rules and the same was approved by the Manager and whether in case of any deviations noted during the firewall review, the Engineer made the necessary changes in the firewall ruleset and tracked the deviations to closure.	No relevant exceptions noted
1.24	When the Network team undertakes configuration/ device changes, the Senior Engineer raises a request via the Change Control Form in the WITSYNC tool which is approved by the Manager.	Inspected for sample change requests the change request ticket raised for aspects such as 'subject', 'change', 'Backup plan available', 'tested by', 'approved by', 'servers and sites impacted', 'availability of completion notes', 'implementer' and 'close date' to ascertain whether the team undertook configuration/ device changes, the Senior Engineer raised a request through the Change Control Form in the WITSYNC Creator tool which was approved by the Manager.	No relevant exceptions noted

TARUN KANDHARI

Digitally signed by TARUN KANDHARI
Date: 2026.01.31 18:48:58 +05'30'

1.24	On a weekly basis, the central security team performs vulnerability scanning to ensure application security for its products. In case of any deviations identified, corrective action is taken. On a yearly basis, the product security team performs penetration testing to ensure application security for its products. In case of any deviations identified, corrective is taken.	Inspected for sample weeks the vulnerability report / email containing vulnerability scan details for sample products for aspects such 'scan run by', 'date of scan', 'email sent to', 'email sent on', 'subject', 'corrective action' and 'count of deviations identified' to ascertain whether on a weekly basis, the central security team performed vulnerability scanning to ensure application security for its products and in case of any deviations identified, a corrective action was taken. Inspected for sample products the penetration testing report for aspects such as 'risk category', 'scope', 'test cases handled', 'date performed', 'conclusion' and 'action taken' to ascertain whether on a yearly basis, the product security team performed penetration testing to ensure application security for its products and in case of any deviations identified, corrective action was taken.	No relevant exceptions noted
1.25	The WITSYNC Compliance team has developed a Risk Management Policy that covers the operational, strategic and IT risks related to the infrastructure and services provided by WITSYNC. The Risk Management Policy is reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.	Inspected Risk Management Policy document for aspects such as 'policy name', 'contents of policy' and 'prepared by', 'approved by', and 'version no.' to ascertain whether the WITSYNC Compliance team had developed a Risk Management Policy that covers the operational, strategic and IT risks related to the WITSYNC infrastructure and services provided by WITSYNC and whether the Risk Management Policy was reviewed and approved by Compliance Manager on an annual basis or upon any changes to the policy.	No relevant exceptions noted
1.26	WITSYNC has defined procedures for periodic performance appraisals including the review and assessment of professional development activities.	Inspected process flow for aspects such as 'policy name', 'version', 'performance appraisal procedures defined', 'prepared by', 'approved by' and 'approved date' to ascertain whether WITSYNC had defined procedures for periodic performance appraisals and review and assessment of professional development activities.	No relevant exceptions noted

TARUN KANDHARI

Digitally signed by TARUN KANDHARI
Date: 2026.01.31 18:49:23 +05'30'

1.27	Based on the support requested by the customer via email / phone / chat, an automated ticket is generated in the WITSYNC Desk Portal which is assigned to the WITSYNC Product Support Engineer / WITSYNC Technical Support Engineer for resolution within the SLA agreed with the customers.	Inspected for sample requests the automated email containing Query ticket for aspects such as ‘query ticket no.’, ‘query received via’, ‘description’, ‘ticket raised by’, ‘ticket raised on’, ‘assigned to’, ‘assigned by’, ‘assigned on’ and ‘SLA details’ to ascertain whether based on the support requested by the customer via email / phone / chat, an automated ticket was generated in the WITSYNC Desk Portal and assigned to the WITSYNC Product Support Engineer / WITSYNC Technical Support Engineer for resolution within the SLA agreed with the customers.	No relevant exceptions noted
1.28	Based on the request from customers, WITSYNC enters into a Master Service Agreements (‘MSA’) with them for WITSYNC applications. The agreement covers the scope, definition of services and confidentiality requirements related to hosting and support services of the WITSYNC Applications.	Inspected for sample customers the MSA signed between WITSYNC and the customer for aspects such as ‘name of customer’, ‘type of service’, ‘agreement signed by’ and ‘agreement signed on’ to ascertain whether WITSYNC entered into a Master Service Agreements (‘MSA’) with customers for hosting WITSYNC Cloud applications on Cloud and the agreement covered the scope, definition of services and confidentiality requirements related to hosting and support services of the WITSYNC Cloud Applications.	No relevant exceptions noted
1.29	The team monitors the performance of the servers using the tool for monitoring of hard-drive failures, application availability, storage requirements etc. In case an error is detected in the tool, action is taken by the Engineers.	Inspected the tool for aspects such as 'Dashboard URL', 'Services Monitored' to ascertain whether team monitored the performance of the servers using the tool for monitoring of hard-drive failures, application availability, storage requirements etc. Inspected the alerts on sample dates for aspects such as 'Date', 'Type of error' and 'Status' to ascertain whether in case an error was detected in the tool, action was taken by the engineers.	No relevant exceptions noted
1.30	WITSYNC has defined Software Development Circular Life Cycle document prescribing the lifecycle of all its products through the stages of design, development, testing and implementation. The documents are reviewed and approved by the respective Product Teams on an annual basis.	Inspected Development Life Cycle document for aspects such as ‘name of policy’ ‘version no.’, prepared by’, ‘approved by, and ‘approved on’ to ascertain whether WITSYNC had defined Development Life Cycle document prescribing the lifecycle of the software through the stages of design, development, testing and implementation and whether this document was reviewed and approved by the respective product Teams on annual basis.	No relevant exceptions noted

TARUN KANDHARI

Digitally signed by TARUN KANDHARI
Date: 2026.01.31 18:49:47 +05'30'

1.31	A comprehensive privacy incident identification and breach response procedure is documented by Privacy team and approved by the Director of Compliance. The policy is reviewed on an annual basis and it provides examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constitutes a breach. The incident management procedures are communicated to personnel who handle personal information.	Inspected Privacy Incidents and Breach Response Procedure document for aspects such as 'name of document', 'contents of policy', 'version no.', 'prepared by', 'approved by' and 'date of approval' to ascertain whether comprehensive incident identification and breach response procedure was documented by Privacy team; approved by the Director of Compliance; reviewed by Privacy lead on an annual basis and provided examples of unauthorized uses and disclosures, as well as guidelines to determine whether an incident constituted a breach.	No relevant exceptions noted
1.32	The code created by the development team is maintained in a centralized repository by the Configuration Management (CM) team. The code developed by the Developers is pushed into the CM tool, which is an in-house tool used by the CM team.	Inspected for sample builds the Code Review details for aspects such as 'Reviewed by', 'details of the URL's/Paths of codes', 'repository' and 'review date' to ascertain whether the code created by the development team was maintained in a centralized repository by the Configuration Management (CM) team and the code developed by the Developers was pushed into the CM tool, which was an in-house tool used by the CM team.	No relevant exceptions noted
1.33	The developed code is tested using the in-house CM tool prior to check- in. Once the code is checked-in, the Quality Assurance (QA) team executes the quality tests on the build in the local (testing) environment.	Inspected for sample builds the build workflow details for aspects such as 'configuration check completed by', 'configuration team approval details', 'details of the URL's/Paths', 'QA tested by' 'and 'QA tested on' to ascertain whether the Developed code was tested systematically using the in-house CM tool prior to check-in and also to ascertain whether once the code was checked-in, the Quality Assurance (QA) team executed the quality tests on the build in the local (Testing) Environment.	No relevant exceptions noted

TARUN KANDHARI

Digitally signed by TARUN KANDHARI
Date: 2026.01.31 18:50:11 +05'30'

02. GAAP Compliance

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that, relevant to user entities' internal control over financial reporting, the Leasing Management Software ensures compliance with the relevant Generally Accepted Accounting Principles (GAAP).

S No	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	The system whether auto classify leases into very short-term, short-term, and long-term leases based on the original lease tenure.	Inspected the system auto classification leases into very short-term, short-term, and long-term leases based on the original lease tenure and the classification does not change even at subsequent modification level.	No relevant exceptions noted.
2.2	The system provides one-time election of transitional valuation approach either full retrospective or modified retrospective approach without any future option for change.	Inspected the system one-time election of transitional valuation approach either full retrospective or modified retrospective approach without any future option for change.	No relevant exceptions noted.
2.3	The system allows to segregate the lease payments into lease and non-lease components.	Inspected the system conditions to allow to segregate the lease payments into lease and non-lease components.	No relevant exceptions noted.
2.4	The methodology, formulation and logical basis for the present value computation of lease liability and valuation of lease asset in compliance with the Accounting Standard on Leases at initial and subsequent modifications.	Inspected the methodology, formulation and logical basis for the present value computation of lease liability and valuation of lease asset whether are in compliance with the Accounting Standard on Leases at initial and subsequent modifications.	No relevant exceptions noted.
2.5	The period-based reporting logic with all relevant details consolidated	Inspected the period-based reporting logic with all relevant details consolidated	No relevant exceptions noted.
2.6	The automated generation of the unique lease reference number and the subsequent modification numbering controls in the system.	Inspected the automated generation of the unique lease reference number and the subsequent modification numbering controls in the system.	No relevant exceptions noted.

03. Cloud Server Security

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that, relevant to user entities' internal control over financial reporting, business premises and information systems are protected from unauthorized access, damage and interference.

S No	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	Documented security policies and procedures are in place to guide employees' activities for granting, controlling, monitoring, and revoking control access.	Inspected the security policy to verify that documented security policies and procedures were in place to guide employees' activities for granting, controlling, monitoring, and revoking control access.	No relevant exceptions noted.
3.2	Personnel are required to attend annual security, confidentiality, and privacy training.	Inspected the training completion report for a sample of personnel employed during the examination period to verify that personnel were required to attend annual security, confidentiality, and privacy training.	No relevant exceptions noted.
3.3	Predefined security measures are utilized to assign role-based access to and throughout the cloud server management.	Inspected the onsite personnel to verify that predefined security measures were utilized to assign role-based access to and throughout the cloud server management.	No relevant exceptions noted.
3.4	Administration of the access control system is restricted to IT, Management, and Operations personnel.	Inspected to verify that administration of the access control system and facility physical access was restricted to IT, Management, and Operations personnel.	No relevant exceptions noted.
3.5	The access control system logs ingress activity by each user and secured point. Logs are retained for a minimum of 90 days.	Inspected to verify that the access control system logged ingress activity by each user and secured point and logs were retained for a minimum of 90 days.	No relevant exceptions noted.
3.6	Requests for the modification of access privileges are made by management.	Inspected Engineer to verify that requests for the modification of access privileges were made by management.	No relevant exceptions noted.
3.7	A list of authorized customer contacts with the ability to initiate customer modifications to access privileges is maintained and reviewed when access requests are received from customers.	Inspected the authorized customer contact listing to verify that a list of authorized customer contacts with the ability to initiate customer modifications to access privileges was maintained and reviewed when access requests were received from customers.	No relevant exceptions noted.

3.8	Physical access privileges are reviewed for accuracy annually.	Inspected the access review communications for each location from within the examination period to verify that physical access privileges were reviewed for accuracy within the past 12 months.	No relevant exceptions noted.
3.9	Management / HR notify access administrators of employee terminations as part of the off-boarding process. On duty access administrators revoke access privileges for the terminated employee and confirm to management.	Inspected the access removal communications for a sample of employees terminated during the examination period to verify that management / HR notified access administrators of employee terminations as part of the off-boarding process and on duty access administrators revoked access privileges for the terminated employee and confirmed to management.	No relevant exceptions noted.

04. Customer Provisioning

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that relevant to user entities' internal control over financial reporting, new client environments are provisioned according to standardized methodologies and to mutually agreed upon criteria and contractual obligations. (included for Managed Services facilities)

S No	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.1	Service agreements are executed with customers prior to onboarding which define the terms of services provided including, but not limited to, the following: ➢ Nature, timing, and extent of services provided ➢ Roles and responsibilities ➢ Service warranties ➢ Confidentiality requirements	Inspected executed MSAs for a sample of customers onboarded during the examination period to verify that service agreements were executed with customers prior to onboarding which defined the terms of services provided including, but not limited to, the following: ➢ Nature, timing, and extent of services provided ➢ Roles and responsibilities ➢ Service warranties ➢ Confidentiality requirements	No relevant exceptions noted.
4.2	WITSYNC maintains policy and procedure manuals for user organization-requested changes to existing systems.	Inspected the Client Requested Changes Procedures and Customer Information Guide to verify that WITSYNC maintained policy and procedure manuals for user organization-requested changes to existing systems.	No relevant exceptions noted.
4.3	Senior management verifies the receipt of a signed services agreement prior to the creation of a provisioning form.	Inspected signed Service Agreements for a sample of customers on-board during the examination period to verify that Senior Management verified the receipt of a signed services agreement prior to the creation of a provisioning form.	No relevant exceptions noted.
4.4	New client procedures are documented in a new client checklist to guide personnel during the new client process.	Inspected the new client checklists for a sample of customers on-boarded during the examination period to verify that new client procedures were documented in a new client checklist to guide personnel during the new client process	No relevant exceptions noted.
4.5	A client authorized requestor list is maintained for each client that lists the authorized client contacts with the ability to initiate changes to subscribed services.	Inspected the authorized client contact listing to verify that a client authorized requestor list was maintained for each client that listed the authorized client contacts with the ability to initiate changes to subscribed services.	No relevant exceptions noted.

05. Systems Availability

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that production systems relevant to user entities' internal control over financial reporting are designed and maintained to ensure system availability.

S No	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.1	Documented incident response procedures are in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided. The procedures include defined severity levels, escalation procedures, and response time requirements for service alerts.	Inspected the incident response procedures to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No relevant exceptions noted.
5.2	An incident ticketing system is utilized to document, prioritize, escalate, and help resolve problems affecting services provided.	Inspected the incident tickets to verify that an incident ticketing system was utilized to document, prioritize, escalate, and help resolve problems that affected services provided.	No relevant exceptions noted.
5.3	Applications are utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	Observed the monitoring systems during on-site activities to verify that applications were utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	No relevant exceptions noted.
5.4	In the event predefined thresholds monitoring systems are exceeded, the systems are configured to generate onscreen alerts and e-mail notifications.	Inspected the monitoring event dashboard, threshold alert configurations, and an example alert to verify that in the event predefined thresholds monitoring systems were exceeded, the systems were configured to generate onscreen alerts and e-mail notifications.	No relevant exceptions noted.
5.5	Technical support staff are available 24x7x365 to manage cloud server monitoring systems.	Inquired of Chief Information Security Officer, to verify that technical support staff were available 24x7x365 to manage monitoring. The staff is available through ticketing system and try to resolve the issues within 4 to 6 working hours of any complain received.	No relevant exceptions noted.

06. Change Management

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that changes to applications and system software relevant to user entities' internal control over financial reporting are authorized and tested before being moved to live production and that access to migrate changes to production is restricted to authorized personnel.

S No	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.1	WITSYNC maintains policy and procedure manuals for user organization-requested changes to existing systems.	Inspected the Client Requested Changes Procedures and Customer Information Guide to verify that WITSYNC maintained policy and procedure manuals for user organization-requested changes to existing systems.	No relevant exceptions noted.
6.2	Requests for the modification of badge access privileges are made by management, or an authorized customer requestor.	Inspected customer access change request communications for a sample of customer badge access change requests during the examination period to verify that requests for the modification of badge access privileges were made by management, or an authorized customer requestor.	No relevant exceptions noted.
6.3	A ticketing system is used to document and track to resolution, client requests.	Inspected the client change tickets to verify that a ticketing system was used to document and track to resolution, client requests.	No relevant exceptions noted.
6.4	Upon closing a ticket, the ticketing system automatically emails the primary client contact person notifying them of the issue and actions taken by WITSYNC.	Inspected the ticket configurations to verify that upon closing a ticket, the ticketing system automatically emailed the primary client contact person notifying them of the issue and actions taken by WITSYNC.	No relevant exceptions noted.
6.5	Modifications to existing user organization firewall rule sets are performed by WITSYNC only after receiving a modification request from authorized user organization personnel.	Inspected the firewall change tickets for a sample of client firewall changes requested during the examination period to verify that modifications to existing user organization firewall rule sets were performed by WITSYNC only after receiving a modification request from authorized user organization personnel.	No relevant exceptions noted.
6.6	Upgrades to the application performed following a detailed step by step procedure as laid in the policy.	Inspected the sample upgrades performed during the examination period of the report to ensure steps compliant, approvals were in place. Review of remarks and how fixes addressed, if any, throughout the development team, quality and assurance team, configuration team, and compliance team.	No relevant exceptions noted.

07. Information Security

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that logical access to applications, data, and system resources relevant to user entities' internal control over financial reporting is restricted to authorized users and such users are restricted to performing authorized actions.

S No	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.1	WITSYNC maintains policy and procedure manuals for internal network infrastructure and user organization system availability and monitoring.	Inspected the Information Security Policy and Standards Manual to verify that WITSYNC maintained policy and procedure manuals for internal network infrastructure and user organization system availability and monitoring.	No relevant exceptions noted.
7.2	WITSYNC maintains a documented Information Security Policy which identifies the Chief Information Security Officer as accountable for the development and implementation of the policies and procedures required by this subpart for the entity or business associate.	Inspected the Information Security Policy and Standards Manual to verify that WITSYNC maintained a documented Information Security Policy which identified the Chief Information Security Officer as accountable for the development and implementation of the policies and procedures required by this subpart for the entity or business associate.	No relevant exceptions noted.
7.3	WITSYNC maintains policy and procedure manuals for firewall event logging, review, and escalation.	Inspected the Change Control policy to verify that WITSYNC maintained policy and procedure manuals for firewall event logging, review, and escalation.	No relevant exceptions noted.
7.4	Workstations are restricted to authorized employees via unique user names and passwords.	Inspected the Default Domain Policy to verify that workstations were restricted to authorized employees via unique user names and passwords.	No relevant exceptions noted.
7.5	Employee access to customer networking devices is logically restricted to specific workstations.	Inspected the firewall configurations to verify that employee access to customer networking devices was logically restricted to specific workstations and allowed employees only.	No relevant exceptions noted.

7.6	Logical access to technical workstations is restricted by the following password requirements: ➢ Minimum of 5 characters in length ➢ Expire after 60 days ➢ Mix of alpha numeric, upper, and lower- case characters	Inspected the Default Domain Policy to verify that logical access to technical workstations was restricted by the following password requirements: ➢ Minimum of 5 characters in length ➢ Expire after 60 days ➢ Mix of alpha numeric, upper, and lower-case characters ➢ One Time Password (OTP) access.	No relevant exceptions noted.
7.7	Employee system administrator access to customer operating systems is limited by IP address to specific technical workstations.	Inspected the firewall configurations to verify that employee system administrator access to customer operating systems was limited by IP address to specific technical workstations	No relevant exceptions noted.
7.8	Remote access to technical workstations that enable the ability for WITSYNC to provide remote support to customer systems is restricted by secure VPN connectivity.	Inspected the VPN configurations and authentication to verify that remote access to technical workstations that enabled the ability for WITSYNC to provide remote support to customer systems was restricted by secure VPN connectivity.	No relevant exceptions noted.
7.9	VPN sessions require unique user names and password authentication.	Inspected the VPN client to verify that VPN sessions required unique user names and password authentication.	No relevant exceptions noted.
7.10	Network policies are configured to lock workstations after 15 minutes of inactivity.	Inspected to verify that network policies were configured to lock workstations after 15 minutes of inactivity.	No relevant exceptions noted.
7.11	A monitoring system is in place to monitor the firewalls for warnings, errors, and alarms.	Inspected the monitoring system log summary to verify that a monitoring system was in place to monitor the firewalls for warnings, errors, and alarms.	No relevant exceptions noted.
7.12	Access to the WITSYNC system is restricted through a unique username and password logins.	Inspected the Databank portal login screen to verify that access to the WITSYNC system was restricted through a unique username and password logins.	No relevant exceptions noted.

TARUN KANDHARI
Digitally signed by TARUN KANDHARI
Date: 2026.01.31 18:53:46 +05'30'

08. Backup Processes

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data relevant to user entities' internal control over financial reporting is backed up and available for restoration in the event of processing errors or unexpected processing interruptions.

S No	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.1	WITSYNC maintains policy and procedure manuals for backup, storage, and restoration procedures.	Inspected the Information System Contingency Plan to verify that WITSYNC maintained policy and procedure manuals for backup, storage, and restoration procedures.	No relevant exceptions noted.
8.2	WITSYNC standard backup configuration is set to automatically perform daily backups of customer systems.	Inspected the backup configurations to verify that WITSYNC standard backup configurations were set to automatically perform daily backups of customer systems.	No relevant exceptions noted.
8.3	The backup software configurations are configured to send notification to the technical support staff in the event of a job error.	Inspected the backup alert configurations and example alert notifications to verify that the backup software configurations were configured to send notification to the technical support staff in the event of a job error.	No relevant exceptions noted.
8.4	Technical Support staff confirms the successful completion of customer-requested restorations.	Inspected job tickets for a sample of customer-requested restorations during the examination period to verify that Technical Support staff confirmed the successful completion of customer-requested restorations.	No relevant exceptions noted.
8.5	The engineering staff reviews and monitors the backup job error notifications to ensure successful completion.	Observed the engineering staff monitor backup notifications during onsite activities for the sample of sites visited to verify that the engineering staff reviewed and monitored the backup job error notifications to ensure successful completion.	No relevant exceptions noted.

09. Network Monitoring

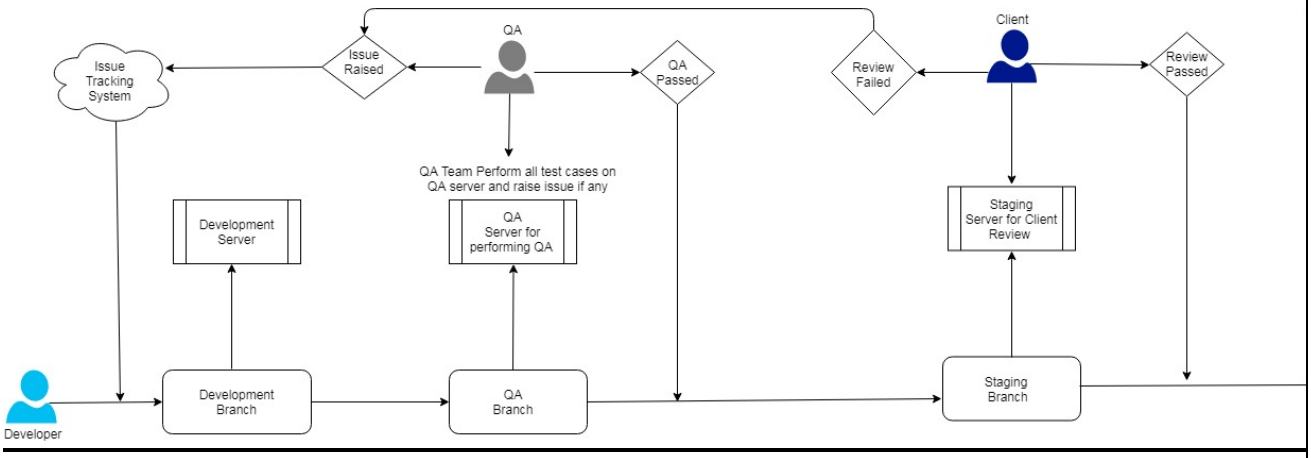
Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that network service relevant to user entities' internal control over financial reporting is monitored, and problems are tracked, escalated, and resolved in accordance with service level agreements.

S No	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
9.1	Documented incident response procedures are in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided. The procedures include defined severity levels, escalation procedures, and response time requirements for service alerts.	Inspected the incident response procedures to verify that documented incident response procedures were in place to guide personnel in monitoring, documenting, escalating, and resolving problems affecting services provided and the procedures included defined severity levels, escalation procedures, and response time requirements for service alerts.	No relevant exceptions noted.
9.2	Technical support staff are available 24x7x365 to manage virtual dedicated cloud server monitoring systems.	Inspected the on-call schedule to verify that technical support staff were available 24x7x365 to manage virtual dedicated cloud server monitoring systems.	No relevant exceptions noted.
9.3	Applications are utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	Observed the monitoring systems to verify that applications were utilized to monitor the following performance, availability, and controlled events for managed services infrastructure: ➢ Availability of the network ➢ Host services and ports ➢ CPU and hard disk utilization	No relevant exceptions noted.
9.4	An incident ticketing system is utilized to document, prioritize, escalate, and help resolve problems affecting services provided.	Inspected the incident tickets to verify that an incident ticketing system was utilized to document, prioritize, escalate, and help resolve problems that affected services provided.	No relevant exceptions noted.

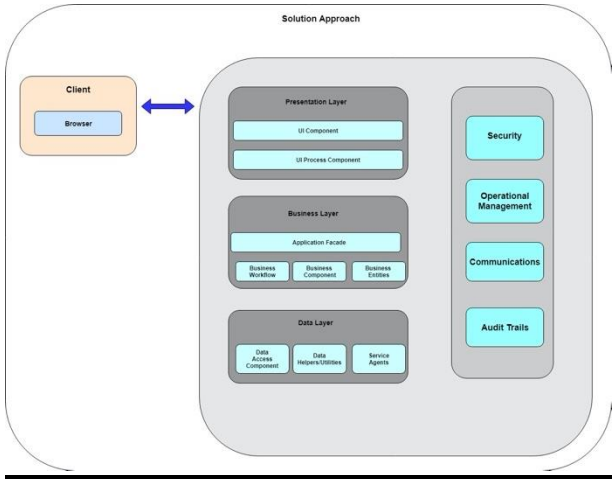
Appendix 1

Image showing Technical Process Work Flow and Type of Servers Maintained and System Architecture

Technical Work flow and Type of Servers – Image 1



WITSYNC Solution Architecture – Image 2



Appendix 2

ISO Certification Obtained

ISO 9001:2015 (QMS)	ISO/IEC 27001:2013 (ISMS)

CERTIFICATE OF REGISTRATION

SIS CERT.™

We Do Not Sell, We Certify!

This Certificate has been awarded to

WITSYNC Soft Solutions Private Limited
40B, LP Block, Ground Floor, Maurya Enclave,
Pitampura, New Delhi-110034, India.

In recognition of the organization's Management System which complies with

ISO 9001:2015
(Quality Management System)

The scope of activities covered by this certificate is defined below

The Protection and Security of Client Data in Relation to the Provision of Professional Consultancy Services Including Financial Process Automation Software and E-learning Solutions.

IAF Code:- 33 & 35

SYNDICATE OF INTERNATIONAL SYSTEM CERTIFICATIONS

Certificate Number: **SISINDQ05201944**
Date of Initial Registration: **11.05.2019**
Latest Date of Issue: **25.01.2025**
Expiry Date: **10.05.2025**
Re-certification Due on: **11.04.2025**

Managing Director

SIS CERTIFICATIONS PVT. LTD.

Note: The certificates is the property of SIS Certifications & the Validity of the Certificate is subject to the successful completion of Surveillance Audit on or before the due date. (In case Surveillance Audit is not allowed to be conducted, this Certificate shall be suspended and must be returned immediately upon request.)

Certified Organization is responsible for maintaining the compliance of the relevant standard rules. Any significant changes in the scope of the certification or standard referred above render this certificate invalid

Corporate office- **SIS Certifications Pvt. Ltd.**
Unit No. 514, 5th Floor, Vipul Business Park, Sector-48, Sohna Road, Gurgaon-122018, Haryana, India.
International Subcontractor Key Locations: **Qatar, Egypt, Italy, Canada & USA.**
Email us:- support@siscertifications.com, Call /Whatsapp: +91-9643073391
The status of this certificate can be verified on "https://siscertifications.com"
Web:- www.siscertifications.com

Issue No.: **06**

IAS ACCREDITED Management Systems Certification Body MSCB-131

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT

CERTIFICATE OF REGISTRATION

SIS CERT.™

We Do Not Sell, We Certify!

This Certificate has been awarded to

WITSYNC Soft Solutions Private Limited
40B, LP Block, Ground Floor, Maurya Enclave,
Pitampura, New Delhi-110034, India.

In recognition of the organization's Management System which complies with

ISO/IEC 27001:2013
(Information Security Management System)

The scope of activities covered by this certificate is defined below

The Protection and Security of Client Data in Relation to the Provision of Professional Consultancy Services Including Financial Process Automation Software and E-learning Solutions.

Statement of Applicability Details: WIT/ISO/SOA_Dated:- 30.09.2023

SYNDICATE OF INTERNATIONAL SYSTEM CERTIFICATIONS

Certificate Number: **SISINDI05201904**
Date of Initial Registration: **11.05.2019**
Latest Date of Issue: **25.01.2025**
Expiry Date: **10.05.2025**
Re-certification Due on: **11.04.2025**

Managing Director

SIS CERTIFICATIONS PVT. LTD.

Note: The certificates is the property of SIS Certifications & the Validity of the Certificate is subject to the successful completion of Surveillance Audit on or before the due date. (In case Surveillance Audit is not allowed to be conducted, this Certificate shall be suspended and must be returned immediately upon request.)

Certified Organization is responsible for maintaining the compliance of the relevant standard rules. Any significant changes in the scope of the certification or standard referred above render this certificate invalid

Corporate office- **SIS Certifications Pvt. Ltd.**
Unit No. 514, 5th Floor, Vipul Business Park, Sector-48, Sohna Road, Gurgaon-122018, Haryana, India.
International Subcontractor Key Locations: **Qatar, Egypt, Italy, Canada & USA.**
Email us:- support@siscertifications.com, Call /Whatsapp: +91-9643073391
The status of this certificate can be verified on "https://siscertifications.com"
Web:- www.siscertifications.com

Issue No.: **06**

IAS ACCREDITED Management Systems Certification Body MSCB-131

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT