SOC 2 Type II Report

For the Period May 1, 2024 to July 31, 2024

REPORT ON CONTROLS PLACED IN OPERATION AT SYNQUP LTD. RELEVANT TO SECURITY, CONFIDENTIALITY AND PRIVACY WITH THE INDEPENDENT SERVICE AUDITOR'S REPORT INCLUDING TESTS PERFORMED AND RESULTS THEREOF.

Table of Contents

SynqUp

Section I - SynqUp Ltd.’s Management Assertion

August 28, 2024

We have prepared the accompanying "Description of the SynqUp Platform relevant to Security, Confidentiality and Privacy for the period May 1, 2024 to July 31, 2024" (Description) of SynqUp Ltd. (Service Organization) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria). The Description is intended to provide report users with information about the SynqUp Platform (System) that may be useful when assessing the risks arising from interactions with the System , particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality and Privacy set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria*.

Carved-out Unaffiliated Subservice Organization: SynqUp Ltd. uses Amazon Web Services ('AWS') to provide infrastructure management services. The Description indicates that complementary controls at Amazon Web Services that are suitably designed and operating effectively are necessary, along with controls at SynqUp Ltd. to achieve the service commitments and system requirements. The Description presents SynqUp Ltd.’s controls and the types of complementary subservice organization controls assumed in the design of SynqUp Ltd.’s controls. The Description does not disclose the actual controls at the carved-out Amazon Web Services.

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

a. The Description presents the System that was designed and implemented throughout the period May 1, 2024 to July 31, 2024 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed throughout the period May 1, 2024 to July 31, 2024 to provide reasonable assurance that SynqUp Ltd. service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively and if the carved-out subservice organization applied the controls assumed in the design of SynqUp Ltd.’s controls throughout that period.

c. The SynqUp Ltd. controls stated in the Description operated effectively throughout the period May 1, 2024 to July 31, 2024 to provide reasonable assurance that SynqUp Ltd.’s service commitments and system requirements were achieved based on the applicable trust services criteria, if the carved-out subservice organization applied the controls assumed in the design of SynqUp Ltd.’s controls throughout that period.

Signature 

Title Yaniv Nizan, CEO

Kost Forer Gabbay & Kasierer
144 Menachem Begin Road, Building A
Tel-Aviv 6492102, Israel

Tel: +972-3-6232525
Fax: +972-3-5622555
ey.com

Section II - Independent service auditor's report

To the Board of Directors
SynqUp Ltd.

Scope
We have examined SynqUp Ltd.'s accompanying description titled "Description of the SynqUp Platform relevant to Security, Confidentiality and Privacy for the period May 1, 2024 to July 31, 2024" (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report, (Description Criteria) and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period May 1, 2024 to July 31, 2024 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality and Privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

Carved-out Unaffiliated Subservice Organization: SynqUp Ltd. uses Amazon Web Services (subservice organization) to provide infrastructure management services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SynqUp Ltd., to provide reasonable assurance that SynqUp Ltd.'s service commitments and system requirements are achieved based on the applicable trust services criteria. The description presents SynqUp Ltd.'s system; its controls relevant to the applicable trust services criteria; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and are operating effectively at Amazon Web Services. The Description does not disclose the actual controls at Amazon Web Services. Our examination did not include the services provided by Amazon Web Services and we have not evaluated whether the controls management assumes have been implemented at Amazon Web Services have been implemented or whether such controls were suitably designed and operating effectively throughout the period May 1, 2024 to July 31, 2024.

Complementary user entity controls: The Description indicates that SynqUp Ltd.'s controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of SynqUp Ltd.'s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

SynqUp Ltd.'s responsibilities
SynqUp Ltd. is responsible for its service commitments and system requirements and for designing**,** implementing, and operating effective controls within the system to provide reasonable assurance that its service commitments and system requirements were achieved. SynqUp Ltd. has provided the accompanying assertion titled, SynqUp Ltd.'s Management Assertion (Assertion) about the presentation of the Description based on the Description Criteria and the suitability of design and operating effectiveness of controls stated therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. SynqUp Ltd. is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) selecting the trust services categories addressed by the engagement and stating the applicable trust services criteria and related controls in the Description; (5) identifying the risks that threaten the achievement of the service organization's service commitments and system requirements; and (6) designing**,** implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Building a better working world

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of design and operating effectiveness of controls stated therein to achieve the service organization's service commitments and system requirements based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period May 1, 2024 to July 31, 2024. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have 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:

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

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

We are required to be independent of SynqUp Ltd. and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

We apply International Standard on Quality Management 1, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services engagements, which requires that we design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Inherent limitations

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls at a service organization may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system

requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria, is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in the accompanying Description of Criteria, Controls, Tests, and Results of Tests (Description of Tests and Results).

Opinion

In our opinion, in all material respects:

a. The Description presents the SynqUp Platform system that was designed and implemented throughout the period May 1, 2024 to July 31, 2024 in accordance with the Description Criteria.
b. The controls stated in the Description were suitably designed throughout the period May 1, 2024 to July 31, 2024, to provide reasonable assurance that SynqUp Ltd.'s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of SynqUp Ltd.'s controls throughout that period.
c. The controls stated in the Description operated effectively throughout the period May 1, 2024 to July 31, 2024 to provide reasonable assurance that SynqUp Ltd. service commitments and system requirements were achieved based on the applicable trust services criteria [if the complementary subservice organization and user entity controls assumed in the design of SynqUp Ltd.'s controls operated effectively throughout that period.

Restricted use

This report , including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of SynqUp Ltd., user entities of SynqUp Ltd.'s SynqUp Platform system during some or all of the period May 1, 2024 to July 31, 2024 and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

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

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

Very truly yours,

Kost Forer Gabbay and Kasierer

Kost Forer Gabbay and Kasierer
A member firm of Ernst & Young Global
August 28, 2024
Tel-Aviv, Israel

SynqUp

Section III - Description of SynqUp Platform Relevant to Security, Confidentiality, and Privacy for the period May 1, 2024 to July 31, 2024

Company Overview and Background

Synq-Up is dedicated to eliminating unproductive meetings by leveraging AI technology to optimize scheduling, enhance productivity, and streamline meeting processes. Founded by experienced professionals with a deep understanding of meeting inefficiencies, Synq-Up aims to transform how companies conduct meetings, saving time and resources while boosting engagement and effectiveness. The company mission is to help organizations save time and resources while enhancing employee engagement by optimizing meeting practices.

Synq-Up has developed a sophisticated AI platform that addresses the common pain points associated with meetings, such as scheduling conflicts, lack of engagement, and inefficient use of time. The platform uses advanced algorithms to analyze meeting patterns and provide actionable insights to improve overall productivity. The company innovative solutions are designed to adapt to various organizational needs, ensuring that the company tools are flexible and scalable.

Purpose and Scope of the Report

This report focuses on the controls supporting the Synq-Up platform and services specifically related to security, availability, confidentiality, processing integrity, and privacy. The scope includes Synq-Up's internal processes and their implementation in AWS environments, ensuring alignment with industry standards and regulatory requirements. This report covers the period from May 1, 2024, to July 30, 2024.

The purpose of this report is to provide stakeholders with an in-depth understanding of the measures Synq-Up has implemented to safeguard its platform and data. It highlights the robust internal controls and risk management strategies that ensure the security and reliability of Synq-Up's services. This report also demonstrates Synq-Up's commitment to transparency and accountability in its operations, reinforcing trust with customers and partners.

Note: *Parenthetical references have been included in the following narrative as a cross-reference to the applicable control procedures included in the Description of Criteria, Controls, Tests and Results of Tests section of this report.*

Products and Services

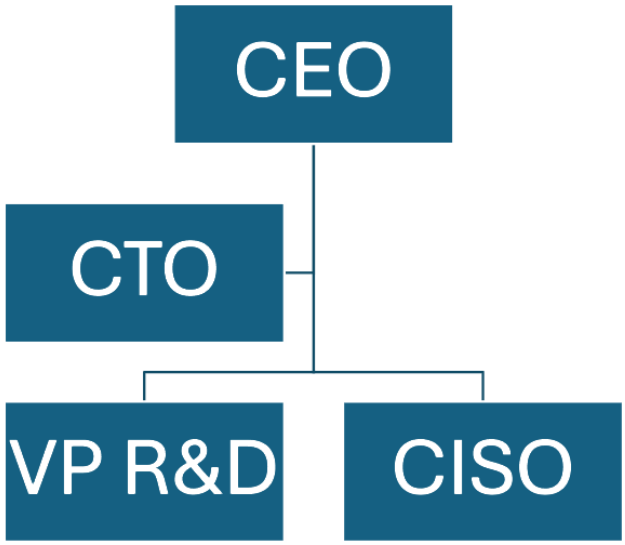
Synq-Up offers a suite of tools designed to improve meeting productivity, including:

- **Meeting Productivity Dashboard:** Provides insights into meeting efficiency and helps identify areas for improvement. This tool collects data from various sources to give a comprehensive view of how meetings are conducted within an organization. Users can track metrics such as meeting duration, participant engagement, and follow-up actions. The dashboard allows managers to identify bottlenecks and streamline processes, ultimately enhancing overall productivity.
- **Customizable Meeting Culture Controls:** Allows companies to tailor their meeting practices to align with organizational goals and individual preferences. This feature enables organizations to set guidelines and best practices for meetings, such as limiting meeting lengths, encouraging agendas, and promoting inclusive participation. By customizing these controls, companies can foster a productive and engaging meeting culture that aligns with their values and objectives.
- **AI-Driven Meeting Analysis:** Offers actionable tips and automation to enhance meeting outcomes, ensuring that meetings are productive and effective. The AI analyzes meeting transcripts and feedback to provide suggestions on improving communication and decision-making processes. This tool helps organizations identify patterns and trends, enabling them to make data-driven decisions to improve meeting quality.
- **Participant Preferences Configuration:** Ensures that meetings align with individual preferences, maximizing participant engagement and productivity. This tool takes into account factors like preferred meeting times, topics of interest, and communication styles to optimize scheduling and participation. By considering these preferences, Synq-Up ensures that meetings are more engaging and effective for all participants.

Synq-Up's products and services are designed to integrate seamlessly with existing systems, providing a unified solution for meeting management. SynqUp platform supports various integrations, allowing organizations to leverage their current tools while benefiting from Synq-Up's advanced features.

Organizational Structure

Synq-Up's organizational structure ensures effective planning, direction, and control of operations. An organization chart is documented that clearly defines management authorities and reporting hierarchy **(4).** The organization chart of the Company is defined as below:



Key roles include:

- **Yaniv Nizan:** Co-Founder & CEO
- **Matan Protter:** Co-Founder & CTO
- **VP R&D:** Oversees research and development activities.
- **CISO:** Manages information security and compliance.

Key departments include:

- **Sales:** Focuses on optimizing sales to Synq-Up customers through targeted strategies and customer engagement. The sales team works closely with marketing and product teams to ensure that customer needs are met and that the benefits of the Synq-Up platform are effectively communicated. Sales strategies are data-driven, leveraging analytics to identify opportunities and optimize performance.
- **Business Development & Marketing:** Manages partnerships, builds the company's brand, and generates sales opportunities through innovative marketing strategies. This department also oversees public relations and customer outreach initiatives to build and maintain a positive company image. Marketing efforts include content creation, social media engagement, and event participation to increase brand awareness and attract new customers.
- **Product:** Defines product lines, incorporates client feedback into the product roadmap, and ensures that products meet market needs. The product team works on continuous improvement and innovation, aligning product development with customer expectations and industry trends. This team also conducts market research to identify emerging trends and opportunities for new features and enhancements.
- **Research & Development (R&D):** Develops and validates products, ensuring that they are innovative and meet customer requirements. This includes dedicated teams for various aspects of development and support, such as

software engineering, AI development, and quality assurance. The R&D team uses agile methodologies to ensure rapid iteration and continuous delivery of high-quality products.

- **Technical Services:** Includes IT Security, Application Security, Service Center, Solution Engineering, and Security Compliance, providing comprehensive technical support. These teams ensure the seamless operation of the Synq-Up platform and address any technical issues that arise. Technical Services also collaborates with customers to implement and optimize Synq-Up solutions, providing training and support as needed.
- **Customer Support:** Provides 24/7 support to customers, working closely with Operations, R&D, QA, and Professional Services to resolve issues promptly. The support team is trained to handle a wide range of customer inquiries and technical problems, ensuring high levels of customer satisfaction. Customer support uses a multi-channel approach, including phone, email, and chat, to provide timely and effective assistance.
- **Finance & Admin Team:** Manages legal, financial, and control activities, including financial planning and administrative tasks. This team ensures that Synq-Up operates within budget and complies with all regulatory requirements. Finance & Admin also oversees corporate governance, ensuring transparency and accountability in all financial and administrative processes.

Overview of Synq-Up's Internal Control

Synq-Up's internal control processes are designed to achieve objectives in financial reporting reliability, operational effectiveness, and compliance with applicable laws and regulations.

Control Environment

Authority and Responsibility: Clearly established and communicated through management style, organizational structure, job descriptions, and policies. This ensures that all employees understand their roles and responsibilities in maintaining security and compliance. Clear lines of authority and responsibility help prevent conflicts of interest and ensure accountability.

Board of Directors: Engaged in governance, strategic direction, and monitoring of company performance and compliance. The Board plays a crucial role in setting the tone for the organization's commitment to security and ethical standards. SynqUp Board of Directors (BOD) meets on a quarterly basis and has a fixed agenda. Meeting minutes are retained. The board establishes oversight responsibilities, applies relevant expertise and operates independently from management **(1).** Regular board meetings and strategic reviews ensure alignment with the company's mission and objectives.

Management Philosophy: The management team, led by the CEO, meets regularly to manage daily operations, assign responsibilities, and ensure that all activities align with the company's strategic goals. There is a Management to the company that meets on a monthly basis. The Management meeting has a fix agenda with (1) financial aspects details, (2) HR, (3) Pipeline of clients, (4) SynqUp issues review, (5) the product discussion with new features. Meeting minutes are retained **(2).** This collaborative approach fosters a culture of transparency and continuous improvement. Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and available to SynqUp's employees within the SynqUp internal portal **(3).**

Integrity and Ethical Values: Fostered by the Board and Management to ensure business is conducted with integrity and high standards. This includes a strong commitment to ethical behavior and compliance with all relevant laws and regulations. Synq-Up's Code of Conduct outlines the ethical principles and standards expected of all employees.

Human Resources Policy: Focused on hiring, training, and evaluating competent personnel. This ensures that employees are well-equipped to perform their roles effectively and contribute to the company's security and operational goals. HR policies include comprehensive onboarding programs, ongoing training, and performance evaluations. Job descriptions are documented and maintained using an external platform. Candidates go through screening and appropriate background and reference checks **(5).** New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different SynqUp policies and work procedures **(6).** In addition, new

employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses **(7).**

Commitment to Competence: Ensures employees have the necessary training and information to perform their jobs effectively. Continuous professional development is encouraged to keep skills and knowledge up-to-date. Security awareness training is performed on an annual basis by SynqUp management **(12).** Synq-Up provides access to training resources, certifications, and career development opportunities.

Control Activities

Control activities are the policies and procedures that enable management directives to be carried out to address risks to the achievement of the entity's objectives. Synq-Up's operating and functional units are required to implement control activities that help achieve business objectives associated with:

- **Reliability of Financial Reporting:** Ensuring accurate and reliable financial reporting through robust internal controls. This includes regular audits and reconciliations to detect and correct errors or discrepancies. Financial controls are designed to prevent fraud and ensure the integrity of financial data.
- **Effectiveness and Efficiency of Operations:** Implementing processes and controls to enhance operational efficiency and effectiveness. This involves continuous process improvement initiatives and the use of performance metrics to track progress. Operational controls help optimize resource allocation and improve productivity.
- **Compliance with Applicable Laws and Regulations:** Ensuring that all activities comply with relevant laws and regulations, reducing the risk of legal or regulatory issues. Compliance audits and training programs are conducted regularly to keep employees informed of their responsibilities. Synq-Up maintains a compliance calendar to track regulatory deadlines and requirements.

Risk Assessment

Synq-Up's risk assessment process identifies, assesses, and manages risks that could affect the achievement of objectives. This includes:

Risk Identification

Key SynqUp stakeholders evaluate risks and threats during a risk assessment meeting, takes place on an annual basis. The meeting minutes are documented within the SynqUp internal tool **(14).** Identifying key business processes and information assets, assessing their criticality, and analyzing potential threats and vulnerabilities. This process involves input from various stakeholders, including management, employees, and external auditors. Risk identification workshops and surveys are conducted regularly to gather comprehensive risk data.

Risk Assessment

A comprehensive risk assessment that identifies and evaluates changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives is performed periodically. As part of this process, threats to system security are identified, evaluated and the risk from these threats is formally assessed. The process is documented and maintained and all remediation activities must be approved by management **(13).** Ongoing monitoring and risk assessment procedures are built into daily activities, ensuring that risks are continuously identified and managed. This includes regular reviews of risk management policies and procedures to ensure they remain effective. Risk assessment tools and software are used to quantify and prioritize risks.

Risk Mitigation: Implementing necessary actions to reduce the severity or likelihood of risks occurring, including developing and enforcing policies and procedures to address identified risks. This involves a combination of preventive, detective, and corrective controls. Synq-Up uses risk mitigation strategies such as diversification, redundancy, and insurance to manage and mitigate risks. Moreover, SynqUp assesses, on an annual basis, the risks that vendors and

business partners (and those entities' vendors and business partners) represent to the achievement of the SynqUp's objectives **(15).** SynqUp performs a review of the SOC 2 report of the datacenter on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at SynqUp to address the CUECs **(30).**

Information and Communication

A description of the SynqUp system and its boundaries is documented and communicated to SynqUp employees within the internal platform and to customers through the SynqUp website **(8).** Information and communication are integral components of Synq-Up's internal control system. Information is identified, captured, processed, and reported by various information systems as well as through conversations with clients, vendors, regulators, and employees. Weekly management meetings are held to discuss operational efficiencies, and general updates to organization-wide security policies and procedures are communicated to the appropriate personnel via email and the internal communication tool.

- **Information Systems:** Synq-Up uses advanced information systems to capture and process data accurately and efficiently. These systems include ensuring seamless information flow across departments.
- **Internal Communication:** Regular internal newsletters, emails, and meetings keep employees informed about company policies, security updates, and organizational changes. An internal portal provides access to company resources, documentation, and training materials.
- **External Communication:** Synq-Up maintains open communication channels with clients, vendors, and regulators, ensuring transparency and compliance. Regular updates and reports are provided to stakeholders, fostering trust and collaboration.

Monitoring

SynqUp uses a suite of monitoring tools to monitor its production environment. Alerts are sent to relevant stakeholders based on pre-defined rules **(16).** Regular monitoring and risk assessment procedures are built into daily activities with management and supervisory activities ensuring the accuracy of operations. Performance reports and statistics are generated regularly and presented to executive management for evaluation. Analysis of root causes is performed, and corrective measures are communicated to relevant groups.

- **Continuous and Production Monitoring:** Synq-Up employs continuous monitoring tools to track system performance, security events, and operational metrics. These tools provide real-time insights and alerts, enabling prompt response to any issues. Audit trail are produced automatically after every access to AWS, machines and to clients confidential information within the SynqUp production and Application. The logs are review on a monthly basis. Logs are retained for 6 months **(50).**
- **Internal Audits:** Regular internal audits are conducted to assess the effectiveness of internal controls and compliance with policies and regulations. Audit findings and recommendations are reviewed by management and the Board of Directors.
- **Performance Metrics:** Key performance indicators (KPIs) and metrics are tracked to measure the success of business processes and initiatives. These metrics are used to identify areas for improvement and drive strategic decisions.

Logical and Physical Access

Synq-Up has an organization-wide information security policy designed to protect information commensurate with its value. Key components include:

Access Control

Access to system resources is protected through a combination of firewalls, VPN, native operating system security, database management system security, application controls and intrusion detection monitoring software **(19).** Strict firewall rules are configured to protect network access and allow access to approved services. Access to the firewall management tool is restricted to authorized personnel **(28).** Using AWS services, firewall configurations, and VPN access with two-factor authentication to ensure secure access to systems and data. Access controls are regularly reviewed and

updated to address new threats and vulnerabilities. Role-based access controls (RBAC) are implemented to ensure that employees have the appropriate level of access based on their roles and responsibilities. Users are identified through the use of a user ID/ password combination using Google Workspace. Strong password configuration settings, where applicable, are enabled on the domain, application and database including: (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of attempts to enter a password before the user ID is suspended, and (4) password complexity **(20).** Several controls are in place to ensure that access management is properly done:

- The console access to the AWS is restricted to authorized personnel and is performed using a two-factors authentication method **(22).**
- Administrative access to the change management tool is restricted to authorized personnel using a two-factor authentication method **(25).**
- Access to the source control tool is restricted to authorized users and is performed using two-factor authentication **(26).**
- The access to the backup and database storage is restricted to authorized individuals **(27).**
- Single sign-on (SSO) is used for identity and access management that enables users to securely authenticate with multiple applications and websites by logging with one set of credentials **(72).**

Recertification of Access Permissions

Permissions with the different environments (servers, database, and application) are reviewed and approved on an annual basis **(24).** Ensuring only authorized personnel have access to production environments through regular reviews and audits. This process helps prevent unauthorized access and ensures that permissions are granted based on current roles and responsibilities. Access logs are maintained and reviewed regularly to detect any unauthorized attempts to access the environment.

Revocation Process

Terminated employees who had access to the production environment have their permissions removed in a timely manner **(31).** Ensuring that terminated employees' access permissions are revoked promptly to prevent unauthorized access. This includes disabling user accounts and recovering access cards and other credentials. A standardized offboarding process ensures that all access is revoked in a timely manner.

Production Environment Access

Restricted to authorized personnel using SSH keys and VPN, with strict access controls in place. Access logs are maintained and reviewed regularly to detect any unauthorized attempts to access the environment. Multi-factor authentication (MFA) is required for access to critical systems. Developers have not access to the production environment **(23).**

Remote Access

Monitored and screened using firewalls and monitoring tools to prevent unauthorized access. Remote access policies are enforced to ensure that only approved devices and networks can connect to the production environment. Secure remote access solutions, such as virtual private networks (VPNs) and zero-trust architectures, are used to protect data and systems.

Physical Access

Controlled via access cards and monitored by the administrative manager to secure physical premises. Physical security measures include surveillance cameras, alarm systems, and security personnel. Data centers and office premises are equipped with advanced physical security controls to prevent unauthorized access.

Software Development Lifecycle (SDLC)

Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the management team within the Change Management application. Change Management tickets are prioritized and labeled based on development phase and urgency **(36).** Synq-Up's SDLC includes stages from requirements definition to general availability release with rigorous testing, code review, and quality assurance processes. Sprint Planning meetings take place at least on a bi weekly basis, where tasks and planning are discussed and prioritized. Meeting minutes are retained **(38).** Product requirements are collected from customers and market research, converted into a Product Requirements Document (PRD), reviewed, and prioritized. Each feature undergoes unit testing, code review, automated testing, and QA cycles before release to ensure high quality and security.

- **Requirements Definition:** Requirements are gathered from customers, stakeholders, and market research to ensure the product meets user needs and industry trends. Detailed requirement specifications are created to provide a clear roadmap for development.
- **Design:** The design phase involves creating detailed specifications and architectural plans for the new feature or product. This includes both high-level architecture and detailed component designs. Design reviews are conducted to ensure that the proposed solution meets all requirements and adheres to best practices.
- **Implementation:** Changes in the change management tool are connected to the source control tool in order to link the request to the code change **(37).** Code changes are reviewed (on front-end changes) along with the pull request performed by authorized personnel. The code review is documented on the version control System. Code review is mandatory in order to continue in the SDLC process and deploy a version to the production environment **(39).** Developers write code according to the specifications and design documents. Each code module undergoes peer review to ensure it adheres to coding standards and best practices. Version control systems are used to manage code changes and facilitate collaboration.
- **Testing and Review:** Manual tests are performed on each version and documented before deployment in order to identify issues within the application. A successful test status is required to continue in the SDLC process **(42).** The QA team performs rigorous testing, including unit tests, integration tests, and system tests, to identify and fix bugs. Automated testing tools are used to ensure comprehensive coverage and quick feedback. Continuous integration and continuous deployment (CI/CD) pipelines are used to automate testing and deployment processes. Vulnerability scans are performed on all the code, using a dedicated tool in order to identify issues within the application **(41).**
- **Deployment:** Once testing is complete, the feature is deployed to a staging environment for final validation. After approval, it is released to the production environment. Deployment processes are automated to ensure consistency and reduce the risk of errors.
- **Post-Deployment Monitoring:** The deployed feature is monitored to ensure it operates as expected. Any issues are logged and addressed promptly. Performance metrics and user feedback are analyzed to identify areas for improvement.

Monitoring and Change Management

Weekly change management meetings assess risks and review required changes. Infrastructure changes are documented, reviewed, and approved as part of the change management process. Metrics reports are regularly issued to the management team to provide key indicators regarding the change management process.

- **Change Requests:** Change requests are logged in a centralized system and reviewed by the change management board. Change requests are prioritized based on their impact and urgency.
- **Impact Analysis:** Each change request undergoes an impact analysis to determine its potential effects on the system and operations. This includes evaluating the risks and benefits associated with the change.
- **Approval:** Changes are approved based on their impact, risk, and alignment with business objectives. Emergency changes are handled through a fast-track process. Approval workflows ensure that all stakeholders are informed and have the opportunity to review proposed changes.

- **Implementation:** Approved changes are implemented according to a detailed plan that includes rollback procedures in case of issues. Implementation plans are reviewed and tested before deployment to minimize the risk of disruptions.
- **Post-Change Review:** Changes are reviewed after implementation to ensure they achieved the desired outcomes without adverse effects. Post-change reviews include an analysis of any issues encountered and lessons learned to improve future change management processes.

Security and Architecture

Synq-Up employs a multi-layered approach to security encompassing application security, network infrastructure, operational security, and data encryption. Key measures include:

Application Security

External penetration test is performed on an annual basis. High issues are investigated and taken care of as part of the SDLC process or by any necessary means **(32).** Vulnerability scans are performed in the infrastructure in order to detect potential security breaches **(33).** Regular penetration testing and vulnerability management to identify and mitigate security risks. The application is designed following secure coding practices and regularly updated to address new vulnerabilities. Security testing is integrated into the SDLC to ensure that vulnerabilities are identified and addressed early in the development process.

Infrastructure Security

Utilizing AWS's infrastructure and implementing strict access controls to protect data and systems. Security configurations are regularly reviewed and updated. Infrastructure security includes network segmentation, intrusion detection systems (IDS), and firewalls to protect against external and internal threats.

Data Encryption

Encryption between SynqUp customers and the SynqUp application is enabled using a minimum HTTPS TLS 1.2 authenticated tunnel **(48).** Encrypting data in transit and at rest using TLS and AWS encryption policies to ensure data confidentiality and integrity. Encryption keys are managed using AWS Key Management Service (KMS). Data encryption is implemented for all sensitive information, including customer data and communications.

Sensitive information and PII encrypted within the SynqUp application database according to the SynqUp security policy **(47).** SynqUp database disks and backups are encrypted within the Cloud. The encryption is executed by AWS. SynqUp end-point disks that have access to the sensitive environment are encrypted as well **(49).**

Operational Security

Implementing best practices for configuration and patch management, security incident response, and antivirus protection. An antivirus/malware solution is installed on employees' laptops that have access to the sensitive environment. An antivirus/malware solution is installed in order to detect and prevent infection of unauthorized or malicious software. All employees' laptops should be assessed and documented as part of the company's risk assessment **(34).** Patch management is in process for the company's laptops and servers. Security settings are hardened and cannot be changed by users. Alerts and remediation are triggered automatically when deficiencies are discovered **(35).** Regular security awareness training ensures that employees are aware of their responsibilities. Operational security measures include regular vulnerability assessments, security audits, and incident response drills.

Support and Incident Management

Synq-Up provides 24/7/365 support through various channels, managing issues and incidents using a ticketing system. The incident management process includes predefined steps and escalation procedures, with incident notifications sent to customers in case their data has been impacted.

- **Ticketing System:** All support issues are logged in a ticketing system, categorized by severity, and assigned to the appropriate team for resolution. The ticketing system provides a centralized platform for tracking and managing support requests.
- **Incident Response:** The company has developed an Incident Management Process in order to respond to Security Incidents and Personal Data Breaches in accordance with applicable laws and regulations **(17).** The incident response team follows a defined process to handle security incidents, including identification, containment, eradication, recovery, and lessons learned. Incident response plans are regularly tested and updated to ensure effectiveness.
- **Communication:** Customers are kept informed throughout the incident resolution process, and detailed reports are provided once the incident is resolved. Communication protocols ensure timely and accurate updates to all stakeholders during an incident.

Availability and Business Continuity

Synq-Up's production environment is managed by AWS services with monitoring and backup procedures ensuring data integrity and availability. A Business Continuity Plan (BCP) is in place to maintain critical services in case of disaster. This includes regular backups, data restoration procedures, and measures to ensure service continuity during disruptions.

Database Backup

Databases are backed up regularly using AWS S3 versioning features. Backup data is stored in multiple locations for redundancy. Backup procedures are automated to ensure consistency and reliability.

Disaster Recovery

SynqUp has implemented a Disaster Recovery Plan and a Business Continuity Plan. The plans are reviewed annually **(46).** Disaster recovery plans are tested regularly to ensure that data can be restored quickly and accurately in the event of a system failure. Disaster recovery tests include simulations of various scenarios to validate the effectiveness of the recovery processes.

Redundancy

Key systems are designed with redundancy to prevent single points of failure. This includes load balancing, failover mechanisms, and geographically dispersed data centers. Redundant systems ensure high availability and resilience against hardware failures, network outages, and other disruptions. Synq-Up's infrastructure is designed to provide continuous operation, even in the event of localized failures.

Infrastructure Management

Synq-Up relies on AWS for its infrastructure, ensuring compliance with industry standards and security measures. AWS provides secure, reliable services that meet the high standards required for Synq-Up's operations, including various compliance certifications such as SOC 2, ISO 27001, and more.

- **AWS Security:** AWS's security measures include physical security, network security, and data encryption, ensuring that Synq-Up's infrastructure is protected against a wide range of threats. AWS regularly undergoes independent audits to maintain its compliance certifications.
- **Compliance Monitoring:** Synq-Up regularly reviews AWS's compliance certifications and reports to ensure continued alignment with security and regulatory requirements. Continuous monitoring of AWS services helps identify and address any compliance gaps or security concerns promptly.

Confidentiality Procedures

Strict measures are implemented to ensure customer data confidentiality, including secure access methods and encryption. Connections to Synq-Up's network and databases are secured using IPSEC tunnels to prevent unauthorized access and ensure data privacy. New vendors, business partners and subcontractors are required to sign a standard NDA agreement outlining the confidentiality and the intellectual property clauses **(51).**

- **Data Access Controls:** Access to customer data is restricted based on the principle of least privilege. Regular audits are conducted to ensure compliance with access policies. Data access is monitored, and anomalies are flagged for investigation to prevent unauthorized access or data breaches.
- **Non-Disclosure Agreements (NDAs):** All employees and contractors are required to sign NDAs to protect customer data and proprietary information. NDAs ensure that all parties understand their responsibilities and the importance of maintaining confidentiality.
- **Data Masking:** Sensitive data is masked in non-production environments to prevent exposure during development and testing. Data masking techniques ensure that developers and testers can work with realistic data sets without accessing actual sensitive information.

Privacy Procedures

Management

Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating SynqUp's privacy policies. The names of such person or group and their responsibilities are defined **(53).** To help ensure that SynqUp employees are aligned with security practices and are aware of their duties with regards to data privacy, SynqUp has implemented a security and privacy awareness training detailing the secure handling of company confidential information, including customer data. The mandatory training is conducted for new and existing employees.

Information Lifecycle

Personal information is collected consistent with the SynqUp's objectives related to privacy **(57).** SynqUp customers sign on contracts that address how their personal information will be securely handled **(56).** SynqUp collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy **(70).** Access to personal information in databases is restricted to authorized SynqUp personnel including help desk personnel **(58).** In addition, SynqUp retains personal information consistent with the entity's objectives related to privacy **(59).** SynqUp securely disposes of personal information to meet the entity's objectives related to privacy **(60).**

Notice

SynqUp provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy **(69).** The SynqUp privacy policy is available on its website and fully discloses the type of information the company may collect from the SynqUp application and website, as well as how SynqUp may use this information **(54).** The SynqUp privacy policy is reviewed and updated by management on at least an annual basis **(55).**

Privacy by Design

To help ensure the delivery of highly secure services to customers, security and privacy by design are an inherent part of the SynqUp Secure Software Development Life-Cycle. For applications to be designed and implemented with proper security requirements, secure coding practices and focus on privacy and security risks are integrated into day-to-day operations and in the development processes. Changes affecting the level of security, privacy, availability and confidentiality issues within the production environment are reviewed with a higher level of scrutiny, including dedicated review by the security team where applicable, as part of the development process.

Data Subject Rights and Dispute Resolution

SynqUp implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner **(71).** SynqUp grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy **(61).** In addition, SynqUp corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy **(62).**

Disclosure to Third Parties

SynqUp creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy **(64).** SynqUp obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary **(66).** Also, SynqUp discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy **(63).**

Breach Management

SynqUp creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy **(65).** SynqUp obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy **(67).** SynqUp provides notification of data breaches and incidents to the affected data subjects, regulators, and others to meet the entity's objectives related to privacy **(68).**

Conclusion

Synq-Up demonstrates a strong commitment to security, availability, confidentiality, and privacy. Through comprehensive internal controls, rigorous risk assessment and management processes, and adherence to industry standards, Synq-Up ensures the highest level of service and security for its customers. The information provided in this report reflects Synq-Up's dedication to maintaining a secure, reliable, and compliant platform for optimizing meeting productivity. Synq-Up continuously seeks to improve its security posture and operational efficiency through ongoing investments in technology, training, and best practices.

Subservice Organization carved-out controls: Amazon Web Services ('AWS')

The subservice organization is expected to:

- Implement controls to enable security and monitoring tools within the production environment.
- Implement logical access security measures to infrastructure components including native security or security software and appropriate configuration settings.
- Restrict the access to servers, software, firewalls, and storage to authorized individuals and to review the list of users and permissions on a regular basis.
- Implement controls to:
    - Provision access only to authorized persons.
    - Remove access when no longer appropriate.
    - Secure the facilities to permit access only to authorized persons.
    - Monitor access to the facilities.
- Be consistent with defined system security as it relates to the design, acquisition, implementation, configuration modification and management of infrastructure and software.
- Maintain system components, including configurations consistent with the defined system security, related policies.
- Provide that only authorized tested and documented changes are made to the system.

SynqUp' customers' responsibilities

SynqUp's services are designed with the assumption that certain controls would be implemented by user organizations. SynqUp makes control recommendations to user organizations and provides the means to implement these controls in several instances. This section describes controls that should be in operation at user organizations to complement SynqUp's controls:

- Implementing sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with SynqUp .
- Ensuring timely removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with SynqUp' services.
- Maintaining authorized, secure, timely, and complete transactions for user organizations relating to SynqUp services.
- Protecting data that is sent to SynqUp by using appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.
- Implementing controls requiring additional approval procedures for critical transactions relating to SynqUp services.
- Reporting to SynqUp in a timely manner any material changes to their overall control environment that may adversely affect services being performed by SynqUp .
- Notifying SynqUp in a timely manner of any changes to personnel directly involved with services performed by SynqUp . These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by SynqUp .
- Adhering to the terms and conditions stated within their contracts with SynqUp .
- Developing, and if necessary, implementing a business continuity and disaster recovery plan (DRP) that will aid in the continuation of services provided by SynqUp.

Section IV - Description of Criteria, Controls, Tests and Results of Tests

Testing Performed and Results of Tests of Entity-Level Controls

In planning the nature, timing and extent of its testing of the controls specified by SynqUp Ltd., Kost Forer Gabbay and Kasierer (KFGK) considered the aspects of SynqUp's control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE, including Electronic Audit Evidence (EAE) (e.g., controls requiring system-generated populations for sample-based testing), we performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspect the source of the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) tie data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity. In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), we inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Criteria and Controls

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of SynqUp Ltd. The testing performed by KFGK and the results of tests are the responsibility of the service auditor.

Control Environment

CC1.1 / COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3	Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and available to SynqUp's employees within the SynqUp internal portal.	Inspected SynqUp's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the SynqUp management on an annual basis. Inspected SynqUp's internal portal and determined that policies and procedures were available to SynqUp employees within the internal portal.	No deviations noted.
7	New employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses.	Inspected the NDA template and determined that new employees were required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses.	No deviations noted.
9	A security policy is documented by SynqUp management, reviewed and approved on an annual basis by the CTO. The security policy is available to SynqUp employees and reviewed annually within the shared folders.	Inspected SynqUp's security policy and determined that a security policy was documented, reviewed and approved by SynqUp management on an annual basis by the CTO. The security policy was available to SynqUp employees and reviewed annually within the shared folders.	No deviations noted.

CC1.2 / COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	SynqUp Board of Directors (BOD) meets on a quarterly basis and has a fixed agenda. Meeting minutes are retained. The board establishes oversight responsibilities, applies relevant expertise and operates independently from management.	Inspected the board meeting minutes and invitations for a sample of quarters and determined that the board met at least on a quarterly basis and had a fixed agenda.	No deviations noted.

CC1.3 / COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	SynqUp Board of Directors (BOD) meets on a quarterly basis and has a fixed agenda. Meeting minutes are retained. The board establishes oversight responsibilities, applies relevant expertise and operates independently from management.	Inspected the board meeting minutes and invitations for a sample of quarters and determined that the board met at least on a quarterly basis and had a fixed agenda.	No deviations noted.
2	There is a Management to the company that meets on a monthly basis. The Management meeting has a fix agenda with (1) financial aspects details, (2) HR, (3) Pipeline of clients, (4) SynqUp issues review, (5) the product discussion with new features. Meeting minutes are retained.	Inspected the management meeting minutes and invitations for a sample of months and determined that the Management of SynqUp met on a monthly basis to discuss on-going issues and updates. Meeting had a fixed agenda.	No deviations noted.
3	Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and available to SynqUp's employees within the SynqUp internal portal.	Inspected SynqUp's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the SynqUp management on an annual basis. Inspected SynqUp's internal portal and determined that policies and procedures were available to SynqUp employees within the internal portal.	No deviations noted.
53	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating SynqUp's privacy policies. The names of such person or group and their responsibilities are defined.	Inspected the privacy and information security policies and determined that responsibility and accountability was assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies.	No deviations noted.

CC1.4 / COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
5	Job descriptions are documented and maintained using an external platform. Candidates go through	Inspected the HR policy and determined that job descriptions were documented and maintained within the SynqUp website and on external tools.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	screening and appropriate background and reference checks.	Inspected the HR policy and determined that reference checks documentation and determined that candidates went through screening and appropriate reference checks.	
6	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different SynqUp policies and work procedures.	Inspected the onboarding checklist template and determined that new employees went through an onboarding process during which, among others, were communicated their responsibilities and the different SynqUp policies and work procedures.	No deviations noted.

CC1.5 / COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3	Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and available to SynqUp's employees within the SynqUp internal portal.	Inspected SynqUp's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the SynqUp management on an annual basis. Inspected SynqUp's internal portal and determined that policies and procedures were available to SynqUp employees within the internal portal.	No deviations noted.
4	An organization chart is documented that clearly defines management authorities and reporting hierarchy.	Inspected SynqUp's organizational chart and determined that an organization chart was documented and approved by management that clearly defines management authorities and reporting hierarchy.	No deviations noted.
12	Security awareness training is performed on an annual basis by SynqUp management.	Inspected the security awareness training documentation and determined that SynqUp employees went through security awareness training on an annual basis.	No deviations noted.

Communication and Information

CC2.1 / COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
9	A security policy is documented by SynqUp management, reviewed and approved on an annual basis by the CTO. The security policy is available to SynqUp employees and reviewed annually within the shared folders.	Inspected SynqUp's security policy and determined that a security policy was documented, reviewed and approved by SynqUp management on an annual basis by the CTO. The security policy was available to SynqUp employees and reviewed annually within the shared folders.	No deviations noted.

CC2.2 / COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3	Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and available to SynqUp's employees within the SynqUp internal portal.	Inspected SynqUp's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the SynqUp management on an annual basis. Inspected SynqUp's internal portal and determined that policies and procedures were available to SynqUp employees within the internal portal.	No deviations noted.
6	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different SynqUp policies and work procedures.	Inspected the onboarding checklist template and determined that new employees went through an onboarding process during which, among others, were communicated their responsibilities and the different SynqUp policies and work procedures.	No deviations noted.
8	A description of the SynqUp system and its boundaries is documented and communicated to SynqUp employees within the internal platform and to customers through the SynqUp website.	Inspected SynqUp's website and determined that a description of the SynqUp system and its boundaries was documented and communicated to external users through the SynqUp's website. Inspected SynqUp's internal system description and determined that a description of the SynqUp system and	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		its boundaries was documented and communicated to SynqUp employees within the company internal portal.	
9	A security policy is documented by SynqUp management, reviewed and approved on an annual basis by the CTO. The security policy is available to SynqUp employees and reviewed annually within the shared folders.	Inspected SynqUp's security policy and determined that a security policy was documented, reviewed and approved by SynqUp management on an annual basis by the CTO. The security policy was available to SynqUp employees and reviewed annually within the shared folders.	No deviations noted.

CC2.3 / COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
8	A description of the SynqUp system and its boundaries is documented and communicated to SynqUp employees within the internal platform and to customers through the SynqUp website.	Inspected SynqUp's website and determined that a description of the SynqUp system and its boundaries was documented and communicated to external users through the SynqUp's website. Inspected SynqUp's internal system description and determined that a description of the SynqUp system and its boundaries was documented and communicated to SynqUp employees within the company internal portal.	No deviations noted.

Risk Assessment

CC3.1 / COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
14	Key SynqUp stakeholders evaluate risks and threats during a risk assessment meeting, takes place on an annual basis. The meeting minutes are documented within the SynqUp internal tool.	Inspected the risk assessment meeting invitations and minutes and determined that risks and threats were evaluated by key SynqUp stakeholders during an annual meeting. The meeting minutes were documented within the SynqUp internal tool.	No deviations noted.

CC3.2 / COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	SynqUp Board of Directors (BOD) meets on a quarterly basis and has a fixed agenda. Meeting minutes are retained. The board establishes oversight responsibilities, applies relevant expertise and operates independently from management.	Inspected the board meeting minutes and invitations for a sample of quarters and determined that the board met at least on a quarterly basis and had a fixed agenda.	No deviations noted.
2	There is a Management to the company that meets on a monthly basis. The Management meeting has a fix agenda with (1) financial aspects details, (2) HR, (3) Pipeline of clients, (4) SynqUp issues review, (5) the product discussion with new features. Meeting minutes are retained.	Inspected the management meeting minutes and invitations for a sample of months and determined that the Management of SynqUp met on a monthly basis to discuss on-going issues and updates. Meeting had a fixed agenda.	No deviations noted.
13	A comprehensive risk assessment that identifies and evaluates changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives is performed periodically. As part of this process, threats to system security are identified, evaluated and the risk from these threats is formally assessed. The process is documented and maintained and all remediation activities must be approved by management.	Inspected the risk assessment documentation and determined that a comprehensive risk assessment that identified and evaluated changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives was performed annually . As part of this process, threats to system security were identified, evaluated and the risk from these threats was formally assessed. The process was documented and maintained and all remediation activities must be approved by management.	No deviations noted.
14	Key SynqUp stakeholders evaluate risks and threats during a risk assessment meeting, takes place on an annual basis. The meeting minutes are documented within the SynqUp internal tool.	Inspected the risk assessment meeting invitations and minutes and determined that risks and threats were evaluated by key SynqUp stakeholders during an annual meeting. The meeting minutes were documented within the SynqUp internal tool.	No deviations noted.
46	SynqUp has implemented a Disaster Recovery Plan and a Business Continuity Plan. The plans are reviewed annually.	Inspected the disaster recovery plan and determined that SynqUp had implemented a Disaster Recovery Plan	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		and a Business Continuity Plan. The plans were reviewed annually.	

CC3.3 / COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	SynqUp Board of Directors (BOD) meets on a quarterly basis and has a fixed agenda. Meeting minutes are retained. The board establishes oversight responsibilities, applies relevant expertise and operates independently from management.	Inspected the board meeting minutes and invitations for a sample of quarters and determined that the board met at least on a quarterly basis and had a fixed agenda.	No deviations noted.
2	There is a Management to the company that meets on a monthly basis. The Management meeting has a fix agenda with (1) financial aspects details, (2) HR, (3) Pipeline of clients, (4) SynqUp issues review, (5) the product discussion with new features. Meeting minutes are retained.	Inspected the management meeting minutes and invitations for a sample of months and determined that the Management of SynqUp met on a monthly basis to discuss on-going issues and updates. Meeting had a fixed agenda.	No deviations noted.
13	A comprehensive risk assessment that identifies and evaluates changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives is performed periodically. As part of this process, threats to system security are identified, evaluated and the risk from these threats is formally assessed. The process is documented and maintained and all remediation activities must be approved by management.	Inspected the risk assessment documentation and determined that a comprehensive risk assessment that identified and evaluated changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives was performed annually . As part of this process, threats to system security were identified, evaluated and the risk from these threats was formally assessed. The process was documented and maintained and all remediation activities must be approved by management.	No deviations noted.
14	Key SynqUp stakeholders evaluate risks and threats during a risk assessment meeting, takes place on an annual basis. The meeting minutes are documented within the SynqUp internal tool.	Inspected the risk assessment meeting invitations and minutes and determined that risks and threats were evaluated by key SynqUp stakeholders during an annual meeting. The meeting minutes were documented within the SynqUp internal tool.	No deviations noted.

CC3.4 / COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
15	SynqUp assesses, on an annual basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the SynqUp's objectives.	Inspected the vendors' risk assessments mapping and determined that SynqUp assessed, on an annual basis, the risks that vendors and business partners represent to the achievement of SynqUp's objectives.	No deviations noted.
30	SynqUp performs a review of the SOC 2 report of the datacenter on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at SynqUp to address the CUECs.	Inspected the AWS SOC2 reports review documentation and determined that SynqUp performed a review of the SOC2 reports of AWS on an annual basis. Deviations were investigated. The review included identifying and documenting the controls in place at SynqUp to address the CUECs.	No deviations noted.
46	SynqUp has implemented a Disaster Recovery Plan and a Business Continuity Plan. The plans are reviewed annually.	Inspected the disaster recovery plan and determined that SynqUp had implemented a Disaster Recovery Plan and a Business Continuity Plan. The plans were reviewed annually.	No deviations noted.
50	Audit trail are produced automatically after every access to AWS, machines and to clients confidential information within the SynqUp production and Application. The logs are review on a monthly basis. Logs are retained for 6 months.	Inspected the audit trail logs and determined that audit trails were produced automatically after every access to AWS, machines and to clients confidential information within the SynqUp production and Application. Inspected a sample of a logs review documentation and determined that SynqUp reviewed the logs on a monthly basis. Logs were retained for 6 months. Inspected a sample notification sent to relevant stakeholder and determined that alerts were generated for further investigation.	No deviations noted.
51	New vendors, business partners and subcontractors are required to sign a standard NDA agreement outlining the confidentiality and the intellectual property clauses.	Inspected a sample of confidentiality agreement and determined that business partners were required to sign an agreement containing a confidentiality clause.	No deviations noted.

Monitoring Activities

CC4.1 / COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
14	Key SynqUp stakeholders evaluate risks and threats during a risk assessment meeting, takes place on an annual basis. The meeting minutes are documented within the SynqUp internal tool.	Inspected the risk assessment meeting invitations and minutes and determined that risks and threats were evaluated by key SynqUp stakeholders during an annual meeting. The meeting minutes were documented within the SynqUp internal tool.	No deviations noted.
16	SynqUp uses a suite of monitoring tools to monitor its production environment. Alerts are sent to relevant stakeholders based on pre-defined rules.	Inspected the SynqUp's monitoring tool dashboards, configurations, and thresholds and determined that monitoring tools were in place in order to monitor its production environment. Alerts were sent to relevant stakeholders based on pre-defined rules.	No deviations noted.

CC4.2 / COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	There is a Management to the company that meets on a monthly basis. The Management meeting has a fix agenda with (1) financial aspects details, (2) HR, (3) Pipeline of clients, (4) SynqUp issues review, (5) the product discussion with new features. Meeting minutes are retained.	Inspected the management meeting minutes and invitations for a sample of months and determined that the Management of SynqUp met on a monthly basis to discuss on-going issues and updates. Meeting had a fixed agenda.	No deviations noted.
16	SynqUp uses a suite of monitoring tools to monitor its production environment. Alerts are sent to relevant stakeholders based on pre-defined rules.	Inspected the SynqUp's monitoring tool dashboards, configurations, and thresholds and determined that monitoring tools were in place in order to monitor its production environment. Alerts were sent to relevant stakeholders based on pre-defined rules.	No deviations noted.

Control Activities

CC5.1 / COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3	Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and available to SynqUp's employees within the SynqUp internal portal.	Inspected SynqUp's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the SynqUp management on an annual basis. Inspected SynqUp's internal portal and determined that policies and procedures were available to SynqUp employees within the internal portal.	No deviations noted.
13	A comprehensive risk assessment that identifies and evaluates changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives is performed periodically. As part of this process, threats to system security are identified, evaluated and the risk from these threats is formally assessed. The process is documented and maintained and all remediation activities must be approved by management.	Inspected the risk assessment documentation and determined that a comprehensive risk assessment that identified and evaluated changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives was performed annually . As part of this process, threats to system security were identified, evaluated and the risk from these threats was formally assessed. The process was documented and maintained and all remediation activities must be approved by management.	No deviations noted.

CC5.2 / COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3	Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and available to SynqUp's employees within the SynqUp internal portal.	Inspected SynqUp's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the SynqUp management on an annual basis.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected SynqUp's internal portal and determined that policies and procedures were available to SynqUp employees within the internal portal.	
13	A comprehensive risk assessment that identifies and evaluates changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives is performed periodically. As part of this process, threats to system security are identified, evaluated and the risk from these threats is formally assessed. The process is documented and maintained and all remediation activities must be approved by management.	Inspected the risk assessment documentation and determined that a comprehensive risk assessment that identified and evaluated changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives was performed annually . As part of this process, threats to system security were identified, evaluated and the risk from these threats was formally assessed. The process was documented and maintained and all remediation activities must be approved by management.	No deviations noted.

CC5.3 / COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3	Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and available to SynqUp's employees within the SynqUp internal portal.	Inspected SynqUp's set of policies and procedures and determined that policies and procedures were documented, reviewed and approved by the SynqUp management on an annual basis. Inspected SynqUp's internal portal and determined that policies and procedures were available to SynqUp employees within the internal portal.	No deviations noted.

Logical and Physical Access Controls

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
19	Access to system resources is protected through a combination of firewalls, VPN, native operating	Inspected the architecture diagram and determined that access to system resources was protected through a	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	system security, database management system security, application controls and intrusion detection monitoring software.	combination of firewalls, VPNs, native operating system security, database management system security, application controls and intrusion detection monitoring software.	
20	Users are identified through the use of a user ID/ password combination using Google Workspace. Strong password configuration settings, where applicable, are enabled on the domain, application and database including: (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of attempts to enter a password before the user ID is suspended, and (4) password complexity.	Inspected the Gsuite and AWS password policies configuration and determined that strong password configuration settings were enabled on the domain, application and database. These settings included: (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of tempts to enter a password before the user ID was suspended, and (4) password complexity.	No deviations noted.
22	The console access to the AWS is restricted to authorized personnel and is performed using a two-factors authentication method.	Inspected the list of users with access to AWS and determined that the console access to AWS was restricted to authorized personnel. Inspected the AWS access configuration and determined that the console access to AWS was performed using a two-factor authentication method.	No deviations noted.
23	Developers have not access to the production environment.	Inspected the list of user with access to the production environment and their permissions and determined that developers had not access to the production environment.	No deviations noted.
25	Administrative access to the change management tool is restricted to authorized personnel using a two-factor authentication method.	Inspected the list of users with administrative access to change management tool and determined that administrative access to the change management tool was restricted to authorized personnel. Inspected the change management tool access configuration and determined that the access to the	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		tool was performed using a two-factor authentication method.	
26	Access to the source control tool is restricted to authorized users and is performed using two-factor authentication.	Inspected the list of users with access to source control tool and determined that access to the source control tool was restricted to authorized personnel. Inspected the source control tool access configuration and determined that the access to the tool was performed using a two-factor authentication method.	No deviations noted.
27	The access to the backup and database storage is restricted to authorized individuals.	Inspected the list of users with access to backup and database storage and determined that access to the backup and database storage was restricted to authorized individuals.	No deviations noted.
28	Strict firewall rules are configured to protect network access and allow access to approved services. Access to the firewall management tool is restricted to authorized personnel.	Inspected the firewall configuration and determined that strict firewall rules were configured to protect network access and allow access to approved services. Inspected the list of users with access to the firewall management tool and determined that access was restricted to authorized personnel.	No deviations noted.
72	Single sign-on (SSO) is used for identity and access management that enables users to securely authenticate with multiple applications and websites by logging with one set of credentials.	Inspected the SSO configuration and determined that it allowed users to securely authenticate to multiple applications and websites by logging in with one set of credentials. Inspected the SSO list of users and determined that a single sign-on (SSO) was used for identification and access to the management environment. Inspected the SynqUp's application configuration and determined that a trusted third party verified the users.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
47	Sensitive information and PII encrypted within the SynqUp application database according to the SynqUp security policy.	Inspected the database configuration and determined that sensitive information and PII were encrypted within the SynqUp application database according to the SynqUp security policy.	No deviations noted.
48	Encryption between SynqUp customers and the SynqUp application is enabled using a minimum HTTPS TLS 1.2 authenticated tunnel.	Inspected the TLS certificate and determined that interactions between customers and the SynqUp platform were performed by using an encrypted channel based on an authenticated TLS connection.	No deviations noted.
49	SynqUp database disks and backups are encrypted within the Cloud. The encryption is executed by AWS. SynqUp end-point disks that have access to the sensitive environment are encrypted as well.	Inspected the backup and database configurations and determined that SynqUp database disks and backups were encrypted within the cloud. The encryption was executed by AWS. Inspected the device configurations and determined that SynqUp's end-point disks that had access to the sensitive environment were encrypted as well.	No deviations noted.
50	Audit trail are produced automatically after every access to AWS, machines and to clients confidential information within the SynqUp production and Application. The logs are review on a monthly basis. Logs are retained for 6 months.	Inspected the audit trail logs and determined that audit trails were produced automatically after every access to AWS, machines and to clients confidential information within the SynqUp production and Application. Inspected a sample of a logs review documentation and determined that SynqUp reviewed the logs on a monthly basis. Logs were retained for 6 months. Inspected a sample notification sent to relevant stakeholder and determined that alerts were generated for further investigation.	No deviations noted.

CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
6	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different SynqUp policies and work procedures.	Inspected the onboarding checklist template and determined that new employees went through an onboarding process during which, among others, were communicated their responsibilities and the different SynqUp policies and work procedures.	No deviations noted.
24	Permissions with the different environments (servers, database, and application) are reviewed and approved on an annual basis.	Inspected the user access review documentation and determined that permissions with the different environments (servers, database and application) were reviewed, approved and documented by the SynqUp management on an annual basis.	No deviations noted.
31	Terminated employees who had access to the production environment have their permissions removed in a timely manner.	Inspected the offboarding checklist template and determined that terminated employees went through an off-boarding process and if they had access to the production environment had their permissions removed and company equipment returned in a timely manner.	No deviations noted.

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
24	Permissions with the different environments (servers, database, and application) are reviewed and approved on an annual basis.	Inspected the user access review documentation and determined that permissions with the different environments (servers, database and application) were reviewed, approved and documented by the SynqUp management on an annual basis.	No deviations noted.
31	Terminated employees who had access to the production environment have their permissions removed in a timely manner.	Inspected the offboarding checklist template and determined that terminated employees went through an off-boarding process and if they had access to the production environment had their permissions removed and company equipment returned in a timely manner.	No deviations noted.

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
30	SynqUp performs a review of the SOC 2 report of the datacenter on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at SynqUp to address the CUECs.	Inspected the AWS SOC2 reports review documentation and determined that SynqUp performed a review of the SOC2 reports of AWS on an annual basis. Deviations were investigated. The review included identifying and documenting the controls in place at SynqUp to address the CUECs.	No deviations noted.

CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
30	SynqUp performs a review of the SOC 2 report of the datacenter on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at SynqUp to address the CUECs.	Inspected the AWS SOC2 reports review documentation and determined that SynqUp performed a review of the SOC2 reports of AWS on an annual basis. Deviations were investigated. The review included identifying and documenting the controls in place at SynqUp to address the CUECs.	No deviations noted.

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
9	A security policy is documented by SynqUp management, reviewed and approved on an annual basis by the CTO. The security policy is available to SynqUp employees and reviewed annually within the shared folders.	Inspected SynqUp's security policy and determined that a security policy was documented, reviewed and approved by SynqUp management on an annual basis by the CTO. The security policy was available to SynqUp employees and reviewed annually within the shared folders.	No deviations noted.
19	Access to system resources is protected through a combination of firewalls, VPN, native operating system security, database management system security, application controls and intrusion detection monitoring software.	Inspected the architecture diagram and determined that access to system resources was protected through a combination of firewalls, VPNs, native operating system security, database management system security,	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		application controls and intrusion detection monitoring software.	
28	Strict firewall rules are configured to protect network access and allow access to approved services. Access to the firewall management tool is restricted to authorized personnel.	Inspected the firewall configuration and determined that strict firewall rules were configured to protect network access and allow access to approved services. Inspected the list of users with access to the firewall management tool and determined that access was restricted to authorized personnel.	No deviations noted.
50	Audit trail are produced automatically after every access to AWS, machines and to clients confidential information within the SynqUp production and Application. The logs are review on a monthly basis. Logs are retained for 6 months.	Inspected the audit trail logs and determined that audit trails were produced automatically after every access to AWS, machines and to clients confidential information within the SynqUp production and Application. Inspected a sample of a logs review documentation and determined that SynqUp reviewed the logs on a monthly basis. Logs were retained for 6 months. Inspected a sample notification sent to relevant stakeholder and determined that alerts were generated for further investigation.	No deviations noted.

CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
9	A security policy is documented by SynqUp management, reviewed and approved on an annual basis by the CTO. The security policy is available to SynqUp employees and reviewed annually within the shared folders.	Inspected SynqUp's security policy and determined that a security policy was documented, reviewed and approved by SynqUp management on an annual basis by the CTO. The security policy was available to SynqUp employees and reviewed annually within the shared folders.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
22	The console access to the AWS is restricted to authorized personnel and is performed using a two-factors authentication method.	Inspected the list of users with access to AWS and determined that the console access to AWS was restricted to authorized personnel. Inspected the AWS access configuration and determined that the console access to AWS was performed using a two-factor authentication method.	No deviations noted.
23	Developers have not access to the production environment.	Inspected the list of user with access to the production environment and their permissions and determined that developers had not access to the production environment.	No deviations noted.
25	Administrative access to the change management tool is restricted to authorized personnel using a two-factor authentication method.	Inspected the list of users with administrative access to change management tool and determined that administrative access to the change management tool was restricted to authorized personnel. Inspected the change management tool access configuration and determined that the access to the tool was performed using a two-factor authentication method.	No deviations noted.
26	Access to the source control tool is restricted to authorized users and is performed using two-factor authentication.	Inspected the list of users with access to source control tool and determined that access to the source control tool was restricted to authorized personnel. Inspected the source control tool access configuration and determined that the access to the tool was performed using a two-factor authentication method.	No deviations noted.
27	The access to the backup and database storage is restricted to authorized individuals.	Inspected the list of users with access to backup and database storage and determined that access to the backup and database storage was restricted to authorized individuals.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
28	Strict firewall rules are configured to protect network access and allow access to approved services. Access to the firewall management tool is restricted to authorized personnel.	Inspected the firewall configuration and determined that strict firewall rules were configured to protect network access and allow access to approved services. Inspected the list of users with access to the firewall management tool and determined that access was restricted to authorized personnel.	No deviations noted.
47	Sensitive information and PII encrypted within the SynqUp application database according to the SynqUp security policy.	Inspected the database configuration and determined that sensitive information and PII were encrypted within the SynqUp application database according to the SynqUp security policy.	No deviations noted.
49	SynqUp database disks and backups are encrypted within the Cloud. The encryption is executed by AWS. SynqUp end-point disks that have access to the sensitive environment are encrypted as well.	Inspected the backup and database configurations and determined that SynqUp database disks and backups were encrypted within the cloud. The encryption was executed by AWS. Inspected the device configurations and determined that SynqUp's end-point disks that had access to the sensitive environment were encrypted as well.	No deviations noted.

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
32	External penetration test is performed on an annual basis. High issues are investigated and taken care of as part of the SDLC process or by any necessary means.	Inspected the penetration test report and determined that an external penetration test was performed on an annual basis. High issues were investigated and addressed of as part of the SDLC process or by any necessary means.	No deviations noted.
34	An antivirus/malware solution is installed on employees' laptops that have access to the sensitive environment. An antivirus/malware solution is installed in order to detect and prevent infection of unauthorized or malicious software. All employees'	Inspected the list of the endpoint devices and determined that antivirus software was installed on workstations, laptops, and servers supporting such software. SynqUp used a centralized management tool in order to receive alerts of the antivirus status.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	laptops should be assessed and documented as part of the company's risk assessment.		
35	Patch management is in process for the company's laptops and servers. Security settings are hardened and cannot be changed by users. Alerts and remediation are triggered automatically when deficiencies are discovered.	Inspected the device configuration and determined that patch management was in process for the company's laptops and servers. Security settings were hardened and cannot be changed by users. Alerts and remediation were triggered automatically when deficiencies were discovered.	No deviations noted.

System Operations

CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
16	SynqUp uses a suite of monitoring tools to monitor its production environment. Alerts are sent to relevant stakeholders based on pre-defined rules.	Inspected the SynqUp's monitoring tool dashboards, configurations, and thresholds and determined that monitoring tools were in place in order to monitor its production environment. Alerts were sent to relevant stakeholders based on pre-defined rules.	No deviations noted.
32	External penetration test is performed on an annual basis. High issues are investigated and taken care of as part of the SDLC process or by any necessary means.	Inspected the penetration test report and determined that an external penetration test was performed on an annual basis. High issues were investigated and addressed of as part of the SDLC process or by any necessary means.	No deviations noted.
33	Vulnerability scans are performed in the infrastructure in order to detect potential security breaches.	Inspected a sample of vulnerability scan test results and determined that vulnerability scans were performed in order to detect potential security breaches. Vulnerabilities were tracked until resolution.	No deviations noted.
41	Vulnerability scans are performed on all the code, using a dedicated tool in order to identify issues within the application.	Inspected a sample of vulnerability scan test results and determined that vulnerability scans were performed on all the code, using a dedicated tool in order to identify issues within the application.	No deviations noted.

CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
16	SynqUp uses a suite of monitoring tools to monitor its production environment. Alerts are sent to relevant stakeholders based on pre-defined rules.	Inspected the SynqUp's monitoring tool dashboards, configurations, and thresholds and determined that monitoring tools were in place in order to monitor its production environment. Alerts were sent to relevant stakeholders based on pre-defined rules.	No deviations noted.
32	External penetration test is performed on an annual basis. High issues are investigated and taken care of as part of the SDLC process or by any necessary means.	Inspected the penetration test report and determined that an external penetration test was performed on an annual basis. High issues were investigated and addressed of as part of the SDLC process or by any necessary means.	No deviations noted.
33	Vulnerability scans are performed in the infrastructure in order to detect potential security breaches.	Inspected a sample of vulnerability scan test results and determined that vulnerability scans were performed in order to detect potential security breaches. Vulnerabilities were tracked until resolution.	No deviations noted.
34	An antivirus/malware solution is installed on employees' laptops that have access to the sensitive environment. An antivirus/malware solution is installed in order to detect and prevent infection of unauthorized or malicious software. All employees' laptops should be assessed and documented as part of the company's risk assessment.	Inspected the list of the endpoint devices and determined that antivirus software was installed on workstations, laptops, and servers supporting such software. SynqUp used a centralized management tool in order to receive alerts of the antivirus status.	No deviations noted.
41	Vulnerability scans are performed on all the code, using a dedicated tool in order to identify issues within the application.	Inspected a sample of vulnerability scan test results and determined that vulnerability scans were performed on all the code, using a dedicated tool in order to identify issues within the application.	No deviations noted.

CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
16	SynqUp uses a suite of monitoring tools to monitor its production environment. Alerts are sent to relevant stakeholders based on pre-defined rules.	Inspected the SynqUp's monitoring tool dashboards, configurations, and thresholds and determined that monitoring tools were in place in order to monitor its production environment. Alerts were sent to relevant stakeholders based on pre-defined rules.	No deviations noted.
17	The company has developed an Incident Management Process in order to respond to Security Incidents and Personal Data Breaches in accordance with applicable laws and regulations.	Inspected the incident management policy and determined that the company had developed an Incident Management Process in order to respond to Security Incidents and Personal Data Breaches in accordance with applicable laws and regulations.	No deviations noted.
33	Vulnerability scans are performed in the infrastructure in order to detect potential security breaches.	Inspected a sample of vulnerability scan test results and determined that vulnerability scans were performed in order to detect potential security breaches. Vulnerabilities were tracked until resolution.	No deviations noted.
41	Vulnerability scans are performed on all the code, using a dedicated tool in order to identify issues within the application.	Inspected a sample of vulnerability scan test results and determined that vulnerability scans were performed on all the code, using a dedicated tool in order to identify issues within the application.	No deviations noted.

CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
17	The company has developed an Incident Management Process in order to respond to Security Incidents and Personal Data Breaches in accordance with applicable laws and regulations.	Inspected the incident management policy and determined that the company had developed an Incident Management Process in order to respond to Security Incidents and Personal Data Breaches in accordance with applicable laws and regulations.	No deviations noted.

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
17	The company has developed an Incident Management Process in order to respond to Security Incidents and Personal Data Breaches in accordance with applicable laws and regulations.	Inspected the incident management policy and determined that the company had developed an Incident Management Process in order to respond to Security Incidents and Personal Data Breaches in accordance with applicable laws and regulations.	No deviations noted.
35	Patch management is in process for the company's laptops and servers. Security settings are hardened and cannot be changed by users. Alerts and remediation are triggered automatically when deficiencies are discovered.	Inspected the device configuration and determined that patch management was in process for the company's laptops and servers. Security settings were hardened and cannot be changed by users. Alerts and remediation were triggered automatically when deficiencies were discovered.	No deviations noted.
46	SynqUp has implemented a Disaster Recovery Plan and a Business Continuity Plan. The plans are reviewed annually.	Inspected the disaster recovery plan and determined that SynqUp had implemented a Disaster Recovery Plan and a Business Continuity Plan. The plans were reviewed annually.	No deviations noted.

Change Management

CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	There is a Management to the company that meets on a monthly basis. The Management meeting has a fix agenda with (1) financial aspects details, (2) HR, (3) Pipeline of clients, (4) SynqUp issues review, (5) the product discussion with new features. Meeting minutes are retained.	Inspected the management meeting minutes and invitations for a sample of months and determined that the Management of SynqUp met on a monthly basis to discuss on-going issues and updates. Meeting had a fixed agenda.	No deviations noted.
36	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the management team within the Change Management application. Change Management tickets are	For a sample of changes, inspected the change management tickets and determined that design, acquisition, implementation, configuration, modification, and management of infrastructure and software were documented and approved within the	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	prioritized and labeled based on development phase and urgency.	change management application. Change management tickets were prioritized and labeled based on development phase and urgency.	
37	Changes in the change management tool are connected to the source control tool in order to link the request to the code change.	For a sample of changes, inspected the change management tickets and determined that changes in the change management tool were connected to the source control tool in order to link the request to the code change.	No deviations noted.
38	Sprint Planning meetings take place at least on a bi weekly basis, where tasks and planning are discussed and prioritized. Meeting minutes are retained.	Inspected a sample of sprint planning meeting minutes and invitations and determined that sprint meeting took place at least on a bi weekly basis, where tasks and planning were discussed and prioritized. Meeting minutes were retained.	No deviations noted.
39	Code changes are reviewed (on front-end changes) along with the pull request performed by authorized personnel. The code review is documented on the version control System. Code review is mandatory in order to continue in the SDLC process and deploy a version to the production environment.	For a sample of changes, inspected the code review documentation and determined that code changes were reviewed along with the pull request performed by the authorized personnel. The code review was documented on the version control System. Inspected the code review configuration and determined that the code review was mandatory in order to continue in the SDLC process and deploy a version to the production environment.	No deviations noted.
42	Manual tests are performed on each version and documented before deployment in order to identify issues within the application. A successful test status is required to continue in the SDLC process.	For a sample of changes, inspected the tests documentation and determined that manual tests were performed on each version and documented before deployment in order to identify issues within the application. Inspected the test configuration and determined that a successful test status was required to continue in the SDLC process.	No deviations noted.

Risk Mitigation

CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
14	Key SynqUp stakeholders evaluate risks and threats during a risk assessment meeting, takes place on an annual basis. The meeting minutes are documented within the SynqUp internal tool.	Inspected the risk assessment meeting invitations and minutes and determined that risks and threats were evaluated by key SynqUp stakeholders during an annual meeting. The meeting minutes were documented within the SynqUp internal tool.	No deviations noted.
51	New vendors, business partners and subcontractors are required to sign a standard NDA agreement outlining the confidentiality and the intellectual property clauses.	Inspected a sample of confidentiality agreement and determined that business partners were required to sign an agreement containing a confidentiality clause.	No deviations noted.

CC9.2: The entity assesses and manages risks associated with vendors and business partners.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	There is a Management to the company that meets on a monthly basis. The Management meeting has a fix agenda with (1) financial aspects details, (2) HR, (3) Pipeline of clients, (4) SynqUp issues review, (5) the product discussion with new features. Meeting minutes are retained.	Inspected the management meeting minutes and invitations for a sample of months and determined that the Management of SynqUp met on a monthly basis to discuss on-going issues and updates. Meeting had a fixed agenda.	No deviations noted.
13	A comprehensive risk assessment that identifies and evaluates changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives is performed periodically. As part of this process, threats to system security are identified, evaluated and the risk from these threats is formally assessed. The process is documented and maintained and all remediation activities must be approved by management.	Inspected the risk assessment documentation and determined that a comprehensive risk assessment that identified and evaluated changes to business objectives, commitments and requirements, internal operations and external factors that threaten the achievement of business objectives was performed annually . As part of this process, threats to system security were identified, evaluated and the risk from these threats was formally assessed. The process was documented and maintained and all remediation activities must be approved by management.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
14	Key SynqUp stakeholders evaluate risks and threats during a risk assessment meeting, takes place on an annual basis. The meeting minutes are documented within the SynqUp internal tool.	Inspected the risk assessment meeting invitations and minutes and determined that risks and threats were evaluated by key SynqUp stakeholders during an annual meeting. The meeting minutes were documented within the SynqUp internal tool.	No deviations noted.
15	SynqUp assesses, on an annual basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the SynqUp's objectives.	Inspected the vendors' risk assessments mapping and determined that SynqUp assessed, on an annual basis, the risks that vendors and business partners represent to the achievement of SynqUp's objectives.	No deviations noted.
30	SynqUp performs a review of the SOC 2 report of the datacenter on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at SynqUp to address the CUECs.	Inspected the AWS SOC2 reports review documentation and determined that SynqUp performed a review of the SOC2 reports of AWS on an annual basis. Deviations were investigated. The review included identifying and documenting the controls in place at SynqUp to address the CUECs.	No deviations noted.

Confidentiality

C1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	SynqUp Board of Directors (BOD) meets on a quarterly basis and has a fixed agenda. Meeting minutes are retained. The board establishes oversight responsibilities, applies relevant expertise and operates independently from management.	Inspected the board meeting minutes and invitations for a sample of quarters and determined that the board met at least on a quarterly basis and had a fixed agenda.	No deviations noted.
2	There is a Management to the company that meets on a monthly basis. The Management meeting has a fix agenda with (1) financial aspects details, (2) HR, (3) Pipeline of clients, (4) SynqUp issues review, (5) the product discussion with new features. Meeting minutes are retained.	Inspected the management meeting minutes and invitations for a sample of months and determined that the Management of SynqUp met on a monthly basis to discuss on-going issues and updates. Meeting had a fixed agenda.	No deviations noted.
12	Security awareness training is performed on an annual basis by SynqUp management.	Inspected the security awareness training documentation and determined that SynqUp employees	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		went through security awareness training on an annual basis.	
19	Access to system resources is protected through a combination of firewalls, VPN, native operating system security, database management system security, application controls and intrusion detection monitoring software.	Inspected the architecture diagram and determined that access to system resources was protected through a combination of firewalls, VPNs, native operating system security, database management system security, application controls and intrusion detection monitoring software.	No deviations noted.
20	Users are identified through the use of a user ID/ password combination using Google Workspace. Strong password configuration settings, where applicable, are enabled on the domain, application and database including: (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of attempts to enter a password before the user ID is suspended, and (4) password complexity.	Inspected the Gsuite and AWS password policies configuration and determined that strong password configuration settings were enabled on the domain, application and database. These settings included: (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of tempts to enter a password before the user ID was suspended, and (4) password complexity.	No deviations noted.
28	Strict firewall rules are configured to protect network access and allow access to approved services. Access to the firewall management tool is restricted to authorized personnel.	Inspected the firewall configuration and determined that strict firewall rules were configured to protect network access and allow access to approved services. Inspected the list of users with access to the firewall management tool and determined that access was restricted to authorized personnel.	No deviations noted.
47	Sensitive information and PII encrypted within the SynqUp application database according to the SynqUp security policy.	Inspected the database configuration and determined that sensitive information and PII were encrypted within the SynqUp application database according to the SynqUp security policy.	No deviations noted.
49	SynqUp database disks and backups are encrypted within the Cloud. The encryption is executed by AWS. SynqUp end-point disks that have access to the sensitive environment are encrypted as well.	Inspected the backup and database configurations and determined that SynqUp database disks and backups were encrypted within the cloud. The encryption was executed by AWS.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the device configurations and determined that SynqUp's end-point disks that had access to the sensitive environment were encrypted as well.	
50	Audit trail are produced automatically after every access to AWS, machines and to clients confidential information within the SynqUp production and Application. The logs are review on a monthly basis. Logs are retained for 6 months.	Inspected the audit trail logs and determined that audit trails were produced automatically after every access to AWS, machines and to clients confidential information within the SynqUp production and Application. Inspected a sample of a logs review documentation and determined that SynqUp reviewed the logs on a monthly basis. Logs were retained for 6 months. Inspected a sample notification sent to relevant stakeholder and determined that alerts were generated for further investigation.	No deviations noted.
51	New vendors, business partners and subcontractors are required to sign a standard NDA agreement outlining the confidentiality and the intellectual property clauses.	Inspected a sample of confidentiality agreement and determined that business partners were required to sign an agreement containing a confidentiality clause.	No deviations noted.

C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
31	Terminated employees who had access to the production environment have their permissions removed in a timely manner.	Inspected the offboarding checklist template and determined that terminated employees went through an off-boarding process and if they had access to the production environment had their permissions removed and company equipment returned in a timely manner.	No deviations noted.

Privacy

P1.0: Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy

P1.1: The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
54	The SynqUp privacy policy is available on its website and fully discloses the type of information the company may collect from the SynqUp application and website, as well as how SynqUp may use this information.	Inspected SynqUp's website and privacy policy and determined that SynqUp's privacy policy was available on its website and fully disclosed the type of information the company may collect from the SynqUp service, as well as how SynqUp may use this information.	No deviations noted.
55	The SynqUp privacy policy is reviewed and updated by management on at least an annual basis.	Inspected the SynqUp's privacy policy and data protection policy and determined that the privacy policy was reviewed and updated by management on at least an annual basis.	No deviations noted.

P2.0: Privacy Criteria Related to Choice and Consent

P2.1: The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
54	The SynqUp privacy policy is available on its website and fully discloses the type of information the company may collect from the SynqUp application and website, as well as how SynqUp may use this information.	Inspected SynqUp's website and privacy policy and determined that SynqUp's privacy policy was available on its website and fully disclosed the type of information the company may collect from the SynqUp service, as well as how SynqUp may use this information.	No deviations noted.
56	SynqUp customers sign on contracts that address how their personal information will be securely handled.	Inspected customer contracts and determined that customer contracts addressed how customer personal information was handled.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
57	Personal information is collected consistent with the SynqUp's objectives related to privacy.	Inspected the SynqUp's privacy policies, customer contracts, and company website and determined that personal information was collected consistent with SynqUp's objectives related to privacy.	No deviations noted.

P3.0: Privacy Criteria Related to Collection

P3.1: Personal information is collected consistent with the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
57	Personal information is collected consistent with the SynqUp's objectives related to privacy.	Inspected the SynqUp's privacy policies, customer contracts, and company website and determined that personal information was collected consistent with SynqUp's objectives related to privacy.	No deviations noted.

P3.2: For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
54	The SynqUp privacy policy is available on its website and fully discloses the type of information the company may collect from the SynqUp application and website, as well as how SynqUp may use this information.	Inspected SynqUp's website and privacy policy and determined that SynqUp's privacy policy was available on its website and fully disclosed the type of information the company may collect from the SynqUp service, as well as how SynqUp may use this information.	No deviations noted.

P4.0: Privacy Criteria Related to Use, Retention, and Disposal

P4.1: The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
54	The SynqUp privacy policy is available on its website and fully discloses the type of information the company may collect from the SynqUp application and website, as well as how SynqUp may use this information.	Inspected SynqUp's website and privacy policy and determined that SynqUp's privacy policy was available on its website and fully disclosed the type of information the company may collect from the SynqUp service, as well as how SynqUp may use this information.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
58	Access to personal information in databases is restricted to authorized SynqUp personnel including help desk personnel.	Inspected the password policies, user access lists, and the user access reviews and determined that the access to personal information in databases was restricted to authorized SynqUp personnel.	No deviations noted.

P4.2: The entity retains personal information consistent with the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
59	SynqUp retains personal information consistent with the entity's objectives related to privacy.	Inspected the SynqUp's data retention and disposal policy, privacy policies, and customer contracts and determined that personal information was retained for no longer than necessary to fulfill the entity's objectives related to privacy.	No deviations noted.

P4.3: The entity securely disposes of personal information to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
60	SynqUp securely disposes of personal information to meet the entity's objectives related to privacy.	Inspected the SynqUp's data retention and disposal policy, privacy policies, and customer contracts and determined that SynqUp securely disposed of personal information to meet the entity's objectives related to privacy.	No deviations noted.

P5.0: Privacy Criteria Related to Access

P5.1: The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
61	SynqUp grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are	Inspected the SynqUp's privacy policy, data protection policy, and data subject communications and determined that SynqUp granted identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provided physical or electronic copies of that	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	information to data subjects to meet the entity's objectives related to privacy.	

P5.2: The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
62	SynqUp corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	Inspected the SynqUp's privacy policy, data protection policy, and data subject communications and data subject requests, and determined that SynqUp corrected or amended personal information based on information provided by data subjects and communicated such information to third parties, as committed or required, to meet the entity's objectives related to privacy.	No deviations noted.

P6.0: Privacy Criteria Related to Disclosure and Notification

P6.1: The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
63	SynqUp discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	Inspected the SynqUp's privacy policy and website and determined that SynqUp disclosed personal information to third parties with the explicit consent of data subjects, and such consent was obtained prior to the disclosure to meet the entity's objectives related to privacy.	No deviations noted.

P6.2: The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
64	SynqUp creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	Inspected the list of sub-processors and determined that SynqUp had practices in place for maintaining and documenting records of authorized disclosures of personal information to meet the entity's objectives related to privacy.	No deviations noted.

P6.3: The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
65	SynqUp creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.	Inspected SynqUp's data incident response policy and determined that in the event of an unauthorized disclosure (including a personal data breach) the company effectively documented the incident.	No deviations noted.

P6.4: The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
66	SynqUp obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	Inspected SynqUp's data processing agreements with vendors and list of sub-processors and determined that SynqUp obtained privacy commitments from vendors and other third parties who had access to the company's personal information. SynqUp assessed those parties' compliance on a periodic and as-needed basis and took corrective action, if necessary.	No deviations noted.

P6.5: The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
67	SynqUp obtains commitments from vendors and other third parties with access to personal	Inspected SynqUp's data processing agreements with vendors and determined that SynqUp obtained	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.	commitments from vendors and other third parties to notify the company in the event of actual or suspected unauthorized disclosures of information.	

P6.6: The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
54	The SynqUp privacy policy is available on its website and fully discloses the type of information the company may collect from the SynqUp application and website, as well as how SynqUp may use this information.	Inspected SynqUp's website and privacy policy and determined that SynqUp's privacy policy was available on its website and fully disclosed the type of information the company may collect from the SynqUp service, as well as how SynqUp may use this information.	No deviations noted.
67	SynqUp obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.	Inspected SynqUp's data processing agreements with vendors and determined that SynqUp obtained commitments from vendors and other third parties to notify the company in the event of actual or suspected unauthorized disclosures of information.	No deviations noted.

P6.7: The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
68	SynqUp provides notification of data breaches and incidents to the affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	Inspected SynqUp's data incident response policy and policies and determined that SynqUp had processes in place to provide notice of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	No deviations noted.
69	SynqUp provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	Inspected the SynqUp's privacy policy and website and determined that data subjects were provided with an accounting of personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the company's objectives related to privacy.	No deviations noted.

P7.0: Privacy Criteria Related to Quality

P7.1: The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
56	SynqUp customers sign on contracts that address how their personal information will be securely handled.	Inspected customer contracts and determined that customer contracts addressed how customer personal information was handled.	No deviations noted.
70	SynqUp collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	Inspected SynqUp's privacy policies and procedures and determined that SynqUp had processes in place for maintaining accurate and complete personal information for the purposes for which it was being used.	No deviations noted.

P8.0: Privacy Criteria Related to Monitoring and Enforcement

P8.1: The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
56	SynqUp customers sign on contracts that address how their personal information will be securely handled.	Inspected customer contracts and determined that customer contracts addressed how customer personal information was handled.	No deviations noted.
71	SynqUp implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	Inspected the SynqUp's privacy policy, data protection policy, and data subject communications and determined that the company had implemented a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy.	No deviations noted.

****