SOC 2 Type II Report

For the period April 1, 2024 to May 31, 2025

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

Table of contents

Section I – SysAid Technologies Ltd.'s Management Assertion

June 17, 2025

We have prepared the accompanying "Description of the SysAid Platform relevant to Security, Availability and Confidentiality throughout the period April 01, 2024 to May 31, 2025" (Description) of SysAid Technologies 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 SysAid 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, Availability and Confidentiality 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: SysAid Technologies Ltd. uses Amazon Web Services ('AWS') to provide infrastructure management services. The Description indicates that complementary controls at AWS that are suitably designed and operating effectively are necessary, along with controls at SysAid Technologies Ltd. to achieve the service commitments and system requirements. The Description presents SysAid Technologies Ltd.'s controls and the types of complementary subservice organization controls assumed in the design of SysAid Technologies Ltd.'s controls. The Description does not disclose the actual controls at the carved-out AWS.

Complementary user entity controls: The Description also indicates complementary user entity controls that are suitably designed and operating effectively are necessary along with SysAid Technologies Ltd.'s controls to achieve the service commitments and system requirements. The Description presents SysAid Technologies Ltd.'s controls and the complementary user entity controls assumed in the design of SysAid Technologies Ltd.'s controls.

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 April 01, 2024 to May 31, 2025 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed throughout the period April 01, 2024 to May 31, 2025 to provide reasonable assurance that SysAid Technologies 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 SysAid Technologies Ltd.'s controls throughout that period.

c. The SysAid Technologies Ltd. controls stated in the Description operated effectively throughout the period April 01, 2024 to May 31, 2025 to provide reasonable assurance that SysAid Technologies Ltd.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary user entity controls and the complementary carved-out subservice organization controls assumed in the design of SysAid Technologies Ltd.'s controls operated effectively throughout that period.

Alex Raif, Chief Information Security Officer,
SysAid Technologies Ltd.

Shape the future
with confidence

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 Management of SysAid Technologies Ltd.

Scope

We have examined SysAid Technologies Ltd.’s accompanying description titled "Description of the SysAid Platform relevant to Security, Availability and Confidentiality throughout the period April 01, 2024 to May 31, 2025" (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 April 01, 2024 to May 31, 2025 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (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: SysAid Technologies Ltd. uses AWS (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 SysAid Technologies Ltd., to provide reasonable assurance that SysAid Technologies Ltd.’s service commitments and system requirements are achieved based on the applicable trust services criteria. The description presents SysAid Technologies 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 AWS. The Description does not disclose the actual controls at AWS. Our examination did not include the services provided by AWS and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period April 01, 2024 to May 31, 2025.

Complementary user entity controls: The Description indicates that SysAid Technologies 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 SysAid Technologies 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.

SysAid Technologies Ltd.’s responsibilities

SysAid Technologies 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. SysAid Technologies Ltd. has provided the accompanying assertion titled, SysAid Technologies 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. SysAid Technologies 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.

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 April 01, 2024 to May 31, 2025. 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 SysAid Technologies 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.

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 SysAid Platform system that was designed and implemented throughout the period April 01, 2024 to May 31, 2025 in accordance with the Description Criteria.
b. the controls stated in the Description were suitably designed throughout the period April 01, 2024 to May 31, 2025, to provide reasonable assurance that SysAid Technologies 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 SysAid Technologies Ltd.'s controls throughout that period.
c. the controls stated in the Description operated effectively throughout the period April 01, 2024 to May 31, 2025 to provide reasonable assurance that SysAid Technologies 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 SysAid Technologies 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 SysAid Technologies Ltd., user entities of SysAid Technologies Ltd.'s SysAid Platform system during some or all of the period April 01, 2024 to May 31, 2025 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.

Kost Forer Gabbay and Kasierer

Kost Forer Gabbay and Kasierer
A member firm of Ernst & Young Global

June 17, 2025
Tel-Aviv, Israel

Section III - Description of the SysAid Platform relevant to Security, Availability, and Confidentiality for the period April 1, 2024 to May 31, 2025

Company Overview and Background

Founded in 2002 and headquartered in Airport City, Israel, SysAid Provides services of IT Service Management software. SysAid's customers range from small businesses to Fortune 500 enterprises across 140 countries.

Purpose and Scope of the Report

The scope of this report is limited to the controls supporting SysAid Platform and products and does not extend to other available software products and services or the controls at third third-party service providers.

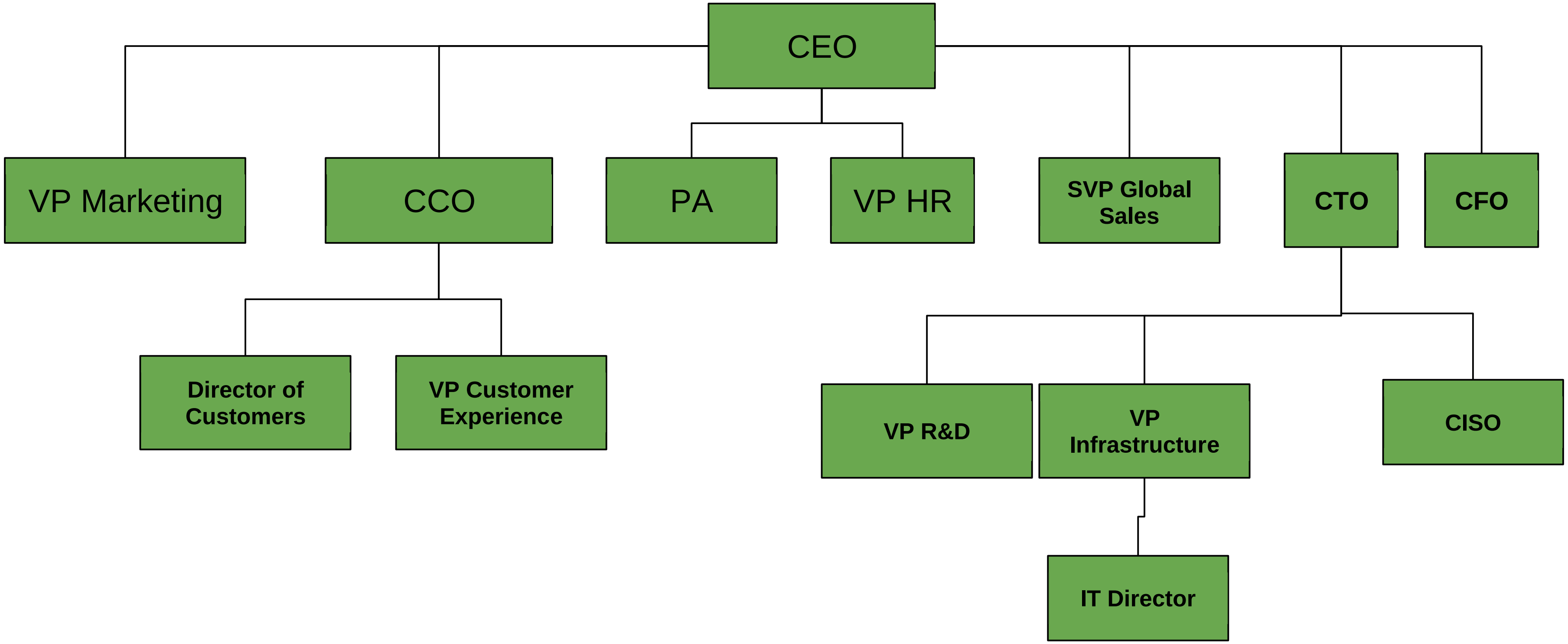
Note: Parenthetical references have been included in the following narrative as a cross-reference to the applicable control procedures included in the Description of Criteria, Controls, Tests and Results of Tests section of this report

Products and Services

SysAid is a service automation company that provides service management software mainly for IT teams to control all aspects of service management. From ticket sorting through workflows that eliminate the need for manual repetitive tasks, and empowerment of users to resolve common issues.

Organizational Structure

SysAid's organizational structure provides the overall framework for planning, directing and controlling operations. An organizational chart is documented and approved by management that clearly defines management authorities and reporting hierarchy (3). It utilizes an approach whereby personnel and business functions are segregated into departments according to job responsibilities, lines of reporting and communications, and allows employees to focus on the specific business issues impacting their customers. Below is a description of key SysAid departments:



People

The following groups of employees are used to support the company services:

- Under the CCO -SysAid customer care department - provide support requested and needed by SysAid customers including Tiers 1,2 and 3, professional services and implementations.
- SysAid R&D - Provides the research and development of SysAid Product.
- Under VP infrastructure and devops - Devops department providing cloud operations and maintenance , and also Director of IT providing IT support and maintain all SysAid IT infrastructure.

Chief information security officer of SysAid is under the CTO - Leading all Cyber Security operations.

Description of the Control Environment, Risk Assessment and Mitigation, Control Activities, Information and Communication and Monitoring

A company's internal control is a process – affected by the entity's boards of directors, management, and other personnel – designed to enable the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations. The following section is a description of the five components of internal control for SysAid.

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its employees. It reflects the overall attitude, awareness, and actions of management, the Board of Directors, and others concerning the importance of controls and the emphasis given to controls in the entity's policies, procedures, methods and organizational structure. SysAid's executive management recognizes its responsibility for directing and controlling operations and for establishing, communicating and monitoring control policies and procedures. Policy and procedures documents for significant processes that address system requirements and relevant updates are available on the company's internal channels.

Authority and Responsibility

Lines of authority and responsibility are clearly established throughout the organization and are communicated through SysAid's:

(1) Management operating style
(2) Organizational structure
(3) Employee job descriptions and
(4) Organizational policies and procedures.

Board of Directors – The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda to review (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features (1). The independent directors are divided into two groups: (1) Industry experts; (2) Investor representatives. The Board of Directors is actively engaged in the governance of the Company and its strategic direction. The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations. It has sufficient members who are independent from management and objective in evaluations and decision making. Part of the Board's mission is to define, maintain and periodically evaluate the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action. The Board's responsibilities include but are not limited to (1) monitoring the actual performance of the Company through its financial results; (2) monitoring the Company's compliance with legal and regulatory requirements; (3) analysis of the budget vs actual results; (4) guiding the Company in the way it funds its operation; (5) approving arrangements with executive officers relating to their employment relationships with the Company, including, without limitation, employment agreements, severance agreements, change in control agreements and restrictive covenants and (6) approving equity-based compensation plans in which directors, officers or employees may participate. The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control. The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the standards of conduct.

Management Philosophy and Operating Style – The management of the company meets on a weekly basis to discuss on-going issues and updates (2). The Management Team, chaired by the Chief Executive Officer (“CEO”), has been delegated by the Board the responsibility to manage SysAid and its daily business. In its role, the Management Team assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. Management and the Board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives. The Management Team designs policies and communications so that personnel understand SysAid's objectives, know how their individual actions interrelate and contribute to those objectives and recognize how and for what they will be held accountable. Contractors and vendor employees are considered during the processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner. Communication exists between management and the Board of directors so that both have information needed to fulfill their roles. Management and the Board of directors' delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of SysAid.

Integrity and Ethical values – Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of key processes. Integrity and ethical behavior are the products of SysAid's ethical and behavioral standards, how they are communicated and how they are monitored and enforced in its business activities. They include management’s actions to remove or reduce inappropriate incentives or extraneous pressures, and opportunities that might prompt personnel to engage in dishonest, illegal or unethical acts. They also include the communication of the organization’s values and behavioral standards to personnel through policy statements and from the executives. Processes are in place to evaluate the performance of individuals and teams against SysAid's expected standards of conduct. The Board of Directors and Management Team recognize their responsibility to foster a strong ethical environment within SysAid to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct. Deviations from the SysAid’s expected standards of conduct are identified and remedied in a timely and consistent manner. The Management Team and the Board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence. Rewards or disciplinary action are exercised when appropriate.

Human Resources Policy and Practices – Human resource policies and practices relate to hiring, orienting, training, evaluating, promoting and compensating personnel. The competence and integrity of SysAid's personnel are essential elements of its control environment. Policies and practices reflect expectations of competence necessary to support the achievement of the company’s objectives. The organization’s ability to recruit and retain highly trained, competent and responsible personnel is dependent to a great extent on its human resource policies and practices. Teams are expected to adhere to the SysAid's policies that define how services should be delivered and products need to be developed. These are located on SysAid network and can be accessed by relevant SysAid team members while communicated by emails on an as-needed basis. SysAid establishes performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the company, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives. The rewards and incentives are aligned with the fulfillment of internal control responsibilities in the achievement of objectives. Teams are expected to evaluate and adjust pressures associated with the achievement of objectives.

Commitment to Competence – The board of directors and the Management Team evaluate competence across SysAid and in outsourced service providers in relation to established policies and practices. Competence at SysAid is designed to (1) identify and hire competent personnel, (2) provide employees with the training and information they need to perform their jobs, (3) evaluate the performance of employees to determine their ability to perform job assignments, and (4) through the performance evaluation process, identify opportunities for growth and job performance improvement. The technical competency of potential and existing personnel, contractors, and vendor employees is considered by SysAid when determining whether to employ and retain the individuals. New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different SysAid policies and work procedures (8). The purpose of these sessions is to provide them with the necessary knowledge about the firm and general work procedures. SysAid considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals. Job descriptions are documented and maintained within the SysAid website and on external tools. Candidates go through screening and appropriate reference checks (7).

Additionally, SysAid's Team Leaders are responsible for training plans for their newcomers. SysAid provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives. It is the manager’s role to decide what training a particular employee requires as they relate to specific job requirements. Personnel responsible for the design, development, implementation, and operation of systems affecting security, availability, confidentiality, undergo training on an annual basis (11). Employees go through a feedback process on at least an annual basis. The feedback reports are retained within the employee personal record (14). Main review topics are Job perception, performance feedback, and manager-employee open discussion. Currently this review is not based on quantitative objectives. The review is written and submitted in native language (per site). Salary increases depend on promotion as well as evaluation discussions.

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. SysAid’s operating and functional units are required to implement control activities that help achieve business objectives associated with :

(1) The reliability of financial reporting ,
(2) The effectiveness and efficiency of operations and
(3) Compliance with applicable laws and regulations .

The controls activities are designed to address specific risks associated with SysAid operations and are reviewed as part of the risk assessment process. SysAid has developed formal policies and procedures covering various operational matters to document the requirements for performance of many control activities. Controls are in place to put the policies into actions in a timely manner. Competent personnel with sufficient authority perform the control activities with diligence and continuing focus. Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.

Risk Assessment

Risk identification: The process of identifying, assessing and managing risks is a critical component of SysAid's internal control system. The purpose of SysAid's risk assessment process is to identify, assess and manage risks that affect the organization’s ability to achieve its objectives. Risk analysis embodies identification of key business processes in which potential exposures of some consequence exist. Exposures defined by SysAid, considers both internal and external influences that may harm the entity's ability to provide reliable services. It includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets. It also includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, business partners, customers, and others with access to SysAid's information systems. Risks and threats are evaluated by key SysAid stakeholders during an annual meeting. Action items are documented within minutes of the meeting. (16).

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. 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 (17). Ongoing monitoring and risks assessment procedures are built into the normal recurring activities of SysAid and include regular management and supervisory activities. Identified risks are analyzed through a process that includes estimating the potential significance of the risk. The assessment includes how the risk should be managed and whether to accept, avoid, reduce, or share the risk. Risks and threats are evaluated by key SysAid stakeholders during a quarterly risk assessment. Minutes of risk assessment meetings and actions items are documented into emails. The Management Team considers the significance of the identified risks by determining the criticality and impact of the risks.

Risk Mitigation: Once the severity and likelihood of a potential risk has been assessed, management considers how the risk should be mitigated. The mitigation process involves making inferences based on assumptions about the risk and carrying out a cost-benefit analysis. Necessary actions are taken to reduce the level of severity or the likelihood of the risk occurring, and the control activities necessary to mitigate the risk are identified. SysAid selects and develops control activities that contribute to the mitigation of risks to the achievement of the company's objectives to acceptable levels. The risk mitigation process is integrated with the company's risk assessment. Moreover, SysAid assesses on an annual basis, the risks that vendors and business partners represent to the achievement of the company's objectives (19).

Risk responses that address and mitigate risks are carried out. The Management Team considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities. The relevant business processes are thoroughly controlled using a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls. Financial impacts of the risks are also taken into consideration during the process. SysAid assesses the risks associated with their vendors and business partners on a periodic basis. Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the Company's objectives during response, mitigation, and recovery efforts (18). Additionally, SysAid has implemented a vendor management policy which details the vendor termination process. The policy is reviewed and approved annually (20).

Information and Communication

Information and communication are an integral component of SysAid's internal control system. It is the process of identifying, capturing and exchanging information in the form and timeframe necessary to conduct, manage and control the organization's operations. Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to SysAid's employees within the SysAid internal portal (5). At SysAid, information is identified, captured, processed and reported by various information systems, as well as through conversations with clients, vendors, regulators and employees. A description of the SysAid system and its boundaries is documented and communicated to the relevant SysAid employees and to external users through SysAid's website (4). New features are communicated to employees by release notes emails (13). Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties. Every two weeks management meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls and other strategic initiatives. Senior executives who lead the meetings use information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. Employees receive communications about their responsibilities and have the information necessary to carry out those responsibilities. General updates to organization-wide security policies and procedures are usually communicated to the appropriate SysAid personnel via email messages and shared with appropriate audiences through the use of the company's internal documentation platform. Additionally, new features are communicated to customers, if relevant, through the website or directly through the account manager (12).

Monitoring

Management uses automated reports created through various applications and processes to monitor the efficiency of certain processes and the effectiveness of certain key controls. Metrics produced from these systems are used to identify the strengths and achievements as well as the weaknesses, inefficiencies or potential performance issues with respect to a particular process. Managers are given the responsibility to inform the individuals who report to them about these items at the appropriate time. Analysis of root cause is performed through various tools and meetings, and corrective measures are communicated to relevant groups through emails, meetings, and a project portal tool in order to prevent future occurrences.

Logical and Physical Access

An information security policy is documented, reviewed and approved by SysAid management on an annual basis. The security policy is available to SysAid employees within the SysAid portal (6). SysAid has established an organization-wide information security policy designed to protect information at a level commensurate with its value. The policy dictates security controls for media where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission. A security policy is documented by SysAid management, reviewed and approved on an annual basis.

Physical Access and Visitors

SysAid recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures and controls have been implemented to help prevent unauthorized access to data, assets and restricted areas. Physical access to the offices is restricted to authorized personnel using a personal identification card according to the physical access policy (33). These access cards are issued to SysAid's employees by the administrative manager. Visitors to the SysAid office are accompanied while on premises (34). Permissions to issue cards and grant access are restricted to the administrative manager and the authorized designees.

Access Control, User and Permissions Management

SysAid builds its production environment system architecture using the AWS services. Users are identified through the use of a user ID/password combination using an SSO tool. Strong password configuration settings, where applicable, are enabled including: (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 is suspended, and (4) password complexity (25). Firewall detailed configuration is defined and performed by the SysAid Operations team. In addition, the global management of the SysAid infrastructure is performed by SysAid using a dedicated AWS workspace. This interface allows SysAid to, among others, (1) add, modify and manage servers, (2) create security policies as they relate to these servers, (3) configure a few network and firewall parameters, (4) manage the databases and (5) manage the AWS users. Firewalls separate the internal network from the internet. Firewall settings have been configured to allow only authorized traffic, as defined in SysAid's Security Policy.

SysAid manages and delivers its services using a variety of systems and environments. As previously described, information security controls and procedures are implemented throughout these systems, to help prevent unauthorized access to data. Several controls are in place to ensure that access management is properly done:

- Access to system resources is protected through a combination of firewalls, VPNs, native operating system security, database management system security, application controls and intrusion detection monitoring software (29).
- 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 (36).
- Access to the source control tool is performed using MFA and is restricted to authorized personnel (30).

- Developers do not have access to the production and database environments. Specific developers can be granted access for specific projects. These accesses are logged and reviewed (28).

Authorized access to the AWS' hosting environment is performed directly from the SysAid office or using VPN to SysAid office then to servers' farm by using SAML authentication and two factors authentication. The database servers reside within the production environment. The access to the production environment servers is restricted to authorized personnel (refer to section 'Production Environment Logical Access).

Recertification of Access Permissions

SysAid has implemented a recertification process to help ensure that only authorized personnel have access to the production interface, servers, environments and databases. Employees whose job functions have changed and therefore no longer require access to a group of user permissions will have their access disabled or modified as needed. Permissions to the different environments (production, databases and applications) are reviewed, approved and documented by the SysAid management on a bi - yearly basis (32).

Revocation Process

Terminated employees complete a termination clearance process on their last day at SysAid while the termination notification is documented and accessible within the SysAid Internal IT management ticket system. This process includes revocation of access permissions to the systems and premises, as well as the return of the property, data and equipment. Terminated employees who had access to the production environment have their permissions removed and company equipment returned in a timely manner (27).

Production Environment Logical Access

The production environment is separated into Virtual Private Cloud (VPC) which are assigned to customers. Access to the customer environment web application interface is performed using personal production username and password for relevant users. Admin access to the AWS servers is performed using a VPN between SysAid's offices and the AWS Data Centers, which is uniquely identified at the AWS datacenter. This access still requires a specific production username and password, which is available to each relevant user. The access to the production server is performed using SSH key and is restricted to authorized personnel (26).

Employees are provided with the minimal access rights required to carry out their duties. New users accessing SysAid system are granted access upon notification from the HR department. A detailed ticket is opened in the IT management ticketing system using a new hire template. This template includes all user detailed permissions. New employees are granted access to the different environments by a ticketing system process and subject to manager approval (31).

Remote Access

SysAid's internal networks are protected using commercial firewalls configured and administered by the IT department. In addition, SysAid's production environment servers are protected by the AWS tools and controls configured by SysAid. SysAid employees are granted remote access to the internal production network environment based on the need-to-work principle. Traffic entering SysAid's production network is monitored and screened by a firewall and monitoring tools implemented by AWS and configured by SysAid. Remote users are automatically disconnected from the production servers after a pre-defined period of inactivity and need to login again in order to re-establish connection to the network.

Software Development Lifecycle (SDLC) Overview

The software development lifecycle consists of the following stages:

- Product/Engineering Requirements Definition
- Detailed Design
- Coding

- Unit Testing
- Integration Testing
- System Testing
- SAST scanning
- Beta Release
- General Availability (GA) Release

There is a documented change management policy. The policy is reviewed and approved on an annual basis (42). Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved within the change management application. Change management tickets are prioritized and labeled based on development phase and urgency (43). Each change goes through a life cycle. Tickets in the change management tool are connected to the source control tool in order to link the request to the code change (44). Product requirements are constantly being collected from customers and from market research by SysAid's Product Managers. These requirements combined with additional engineering improvement requirements are discussed by VP R&D managers and Product Manager and are converted to a Product Requirements Document (PRD) that contains more specific description of required features and changes.

The R&D Managers review the PRD and provide a high-level effort estimation for every feature. The product managers work with the R&D managers to create a prioritized features list based on the effort estimation and required timeline of the release. The Release Manager collects the features list, validates the total effort vs teams foreseen progress and creates a release plan specifying integration dates, Feature Freeze and Code Freeze dates as well as the release date of 1st release candidate to PS.

R&D Engineers are engaged with ongoing enhancements of the product functionality. Each engineer implements Unit Testing to every new coded software module in accordance with Unit Tests guidelines document. SysAid performs unit testing using a dedicated tool. R&D engineer's check-in their respective code to a common source control system that provides extensive version tracking functionality and other software building abilities. All changes which are added to the Source Control contain information linking them to the relevant features and bugs. Code changes are reviewed along with the pull request performed by the team leader. The code review is documented on the source control tool. Code review is mandatory in order to continue in the SDLC process and deploy a version to the production environment (45). Unit Tests are maintained according to product changes and enhanced based on bugs that were detected in previous product versions. Check-in of code triggers Unit testing process and if passed successfully, a new build is created, and automated tests are executed on it. Automation tests are performed using a dedicated tool on a regular basis in order to identify issues within the application (47). A successful test status is required to continue in the SDLC process (48).

Software Testing and QA Process: SysAid Quality Assurance (QA) is constantly involved from early development stages. Based on the PRD, QA creates internal test plans. Test plans are reviewed by Product Managers and by R&D Team Leader responsible for the feature design. Each build goes through an automated pass/fail sanity testing process during which it is determined if it is acceptable to commence a full QA cycle. A full QA cycle (Stabilization) includes regression and progression tests according to test plan documents. During this stage bugs are reported in TFS. Manual tests are performed by the QA team. Each bug is assigned to an R&D Engineer for resolving with severity and a target version. Bugs that were targeted to the current version are fixed and verified as closed or are reopened. During Code Freeze, only Show Stopper bugs are fixed by the engineers.

Software Release: The official release of a version from SysAid development should qualify by the Release Exit Criteria. It is mandatory that all automation tests pass and that scans are free of Critical and High findings. SysAid secured development process also includes a yearly pen testing of which findings are fixed in the following release. The released version is verified by the Professional Services (PS) prior to releasing to Beta customers. Show stopper bugs are reported and fixed in a new Release Candidate. A Beta version is released to selected customers. Customers who receive Beta version are notified in advance and express their wish to actively participate in this stage. The Beta version is used in standard operational environments of these customers. Bugs or functional requests that are made by customers are reported in TFS and marked with customer tag. Faults reported during this stage are analyzed by R&D and if defined as showstoppers, they will be fixed for the General Availability (GA) release. Requests for functional enhancements are going to Product Managers backlog for future Releases. A General Availability (GA) version is released as a complete installation package including Built-in help, Administration Guide and Release Notes documents. A "release exit" checklist is filled by SysAid before releasing a version to production. The permission to approve merge requests and to deploy required MFA and is restricted to authorized personnel (46).

Monitoring the Change Management Processes

A change management meeting is performed every week, to assess the risks identified and review changes required to the production environment. Action items are updated within as part of the process and change is approved only after review and assessment. In addition, metric reports are regularly issued to the Management Team in order to provide them with key indicators regarding the change management process.

Infrastructure Change Management Overview

SysAid regularly makes changes within its production environment in response to the evolving client and market needs. These changes include adding/removing/changing the configuration policies of the existing servers or performing routine maintenance activities, software updates, and other infrastructure-related changes accordingly to available possibilities provides by the third-party vendors. Infrastructure changes are documented within the Change Management process. The request is reviewed and approved by the Director of IT and Information Security.

Emergency changes are performed and updated as part of hot fixes, which follow the same process as described above though the timeframe may be shortened, and approvals may be provided after the change was already performed.

Description of the Production Environment

The processes described below are executed within SysAid's production environment, hosted by Amazon Web Services in various regions.

The scope of this examination included SysAid platform and cloud hosted services located on AWS regions. The in-scope infrastructure consists of multiple applications operating system platforms and databases as shown in the below table:

Primary infrastructure			
Production Application	Business Function Description	Operating System Platform	Physical Location
HA proxy load balancer	Control All requests reaching the system and balance them between the relevant services; provide additional capabilities like managing clients' SSL certificates, redirect URL's, block or throttle certain requests and so on.	Amazon Linux 2	AWS - N. Virginia, Oregon, Ireland, Frankfurt, Canada, Sydney
Web servers for admins and end users	Fulfillment of requests entering the system. These are application servers, auto scaled per load on the environment. They do not contain client's data, can be killed and scaled at any moment.	Amazon Linux 2	AWS - N. Virginia, Oregon, Ireland, Frankfurt, Canada, Sydney

Agent traffic	Services that fulfill “non-human” requests coming from SysAid RDS and agents. Also auto scaled.	Amazon Linux 2	AWS - N. Virginia, Oregon, Ireland, Frankfurt, Canada, Sydney
SysAid agent	SysAid agent installed on end machines within customer networks	Run by customers on multiple operating systems (Windows, Linux, MacOS)	Run by customers on multiple locations
SysAid RDS	SysAid remote discovery system is the service that bridges between SysAid cloud and customer network performing operations on behalf of SysAid within the customer network.	Run by customers on windows machines.	Run by customers on multiple locations
SysAid Backoffice (scheduler)	Service Responsible for background scheduled tasks, such as email integrations, escalation rules, timers, scheduled reports, scheduled tasks and so on	Amazon Linux 2	AWS - N. Virginia, Oregon, Ireland, Frankfurt, Canada, Sydney
SysAid DB	The primary DB used to store all operational data	SaaS Service (AWS Aurora MySQL 5.7)	AWS - N. Virginia, Oregon, Ireland, Frankfurt, Canada, Sydney
SysAid storage (NFS/EFS/S3)	The frameworks used to store both customer files like attachments, configuration files, like reports, logo and icons.	Amazon Linux 2	AWS - N. Virginia, Oregon, Ireland, Frankfurt, Canada, Sydney

SysAid cloud application is hosted on AWS and utilizes many additional AWS services that are included in platform architecture. Examples for the Main services which are in use are: AWS EC2, EBS, SQS, ElastiCache, ElasticSearch, API GW and more.

Infrastructure and information systems

The following table presents a summary of the in-scope infrastructure and information systems:

Primary infrastructure			
Production Application	Business Function Description	Operating System Platform	Physical Location
FortiGate	FW and VPN	FortiGate E200	Israel Office
Active directory	SysAid Employees and Objects such as computers and servers	Win server 2019	2 - Israel Office 1 - AWS
vSphere	Corporate Servers + Automation servers	Vcenter 6.7	Israel Office

Backup server	Backup the corporate servers	Windows server 2019 Veeam 11	Israel Office
BB +Users Switches	Network	Dell Juniper	Israel Office
Storage	Datacenter and File server	HP NImble	Israel Office
Google workspace	Emails and Drives	Google workspace	Google
Office 365	Office	Office pro plus	Microsoft
Zoom	Zoom meetings		Zoom
Anti-Virus	servers AV	Symantec	SysAid Office
EDR	Computers and DC	Sentinel one	SysAid Office

SysAid's infrastructure runs on top of AWS's Infrastructure as a Service (IaaS) and utilizes various services such as: (1) EC2, (2) S3, (3) RDS (4), Redshift, (5) EMR, (6) CloudFront, which is the AWS's CDN, and more. These services are designed to make web-scale computing easier for SysAid.

AWS's web service interface (AWS Console) allows SysAid to obtain and configure capacity. It provides SysAid with control of computing resources and runs on AWS's computing environment. EC2 reduces the time required to obtain and boot new server instances to minutes, allowing to quickly scale capacity, both up and down, as computing requirements change. The use of EC2 allows to:

- Select a pre-configured template to get up and running immediately or create a per-need AMI containing SysAid -configured applications, libraries, data, and associated configuration settings.
- Configure security and network access on the Ec2 instance.
- Choose which instance type(s), then start, terminate, and monitor as many instances as needed, using the web service APIs.
- Determine whether to run in multiple locations, utilize static IP endpoints, or attach persistent block storage to instances.

The production environment is completely separated from the corporate environment and follows strict access and data processing procedures and processes. The environment is managed by a selected few Security personnel who use 2FA to connect using a dedicated AWS workspace.

All SysAid users who connect to the customers' VPCs for support purposes should login via a named workspace. All authentication is performed with a SAML provider. Customers' data is encrypted at test and in transfer. Access of SysAid personnel as well as customers is further restricted by IP filtering.

Note: Controls performed by the data center service providers are not included in the scope of this report.

Network Infrastructure

Robust network infrastructure is essential for reliable and secure real-time data communication between the SysAid cloud service components. To provide sufficient capacity, the SysAid network infrastructure relies on platforms provided by Amazon Web Services (AWS). To ensure appropriate network security levels, SysAid security standards and practices are backed by a multi-layered approach that incorporates practices for preventing security breaches, ensuring confidentiality, integrity and availability. SysAid's security model encompasses the following components:

- Application layer security, including:
  - Various authentication schemas such as multi-factor authentication (MFA), unique ID and complex password policy
  - Logical security
  - Penetration testing
  - IP address source restriction
  - Customer's data encryption at-rest and in transit
- Network and infrastructure security, including:
  - Network architecture
  - Risk management
  - AWS data centers
  - Cloud operation security (change management, monitoring and log analysis)

Web, Application and Service Supporting Infrastructure Environment

SysAid utilizes AWS's clustered infrastructure design to provide redundancy and high availability. In addition, the infrastructure is configured in a way that enables auto scaling capabilities. This allows supporting high performance during demand spikes to the services.

Production Monitoring

SysAid uses a suite of monitoring tools in order to monitor its service. The production environment, including the servers and application, is monitored by the Operation Team (24). SysAid's production network encompasses numerous components including web services, application and data server types, database, monitoring tools, and redundant network equipment provided as part of the AWS services. In addition, in order to improve service availability to clients and to support the operations of the SysAid environments, SysAid maintains a dedicated Security department. The Security department is responsible for the ongoing work on the production environment as well as investigating escalated issues. The production environment, including the servers and application, is monitored 24/7/365 by the NOC and Security team. Key SysAid staff members are notified of events related to the security, availability or confidentiality of service to clients.

Security and Architecture

SysAid provides a secure, reliable and resilient Software-as-a-Service platform that has been designed from the ground up based on industry best practices. The below addresses the network and hardware infrastructure, software and information security elements that SysAid delivers as part of this platform, database management system security, application controls and intrusion detection monitoring software.

Data Center Security

SysAid performs a review of the SOC 2 report of its third-party infrastructure provider on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at SysAid to address the CUECs (35). SysAid relies on Amazon Web Services global infrastructure, including the facilities, network, hardware, and operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of basic computing resources and storage. This infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards: ISO 27001:2013, ISO 27017, ISO 27018, AICPA SOC 2and PCI-DSS and more. The environmental protection managed by the vendors policies are:

- Redundancy - The data centers are designed to anticipate and tolerate failure while maintaining service levels with core applications deployed to multiple regions.
- Fire Detection and Suppression – Automatic fire detection and suppression equipment has been installed to reduce risk.

- Redundant Power – the data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and Uninterruptable Power Supply (UPS) units provide back-up power in the event of an electrical failure. Data centers use generators to provide back-up power for the entire facility.
- Climate and Temperature Controls – maintain a constant operating temperature and humidity level for all hardware.
- Physical access - AWS recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures and controls have been implemented to help prevent unauthorized access to data, assets and restricted areas.

Infrastructure Security

SysAid performs a review of the SOC 2 report of its third-party infrastructure provider on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at SysAid to address the CUECs (35). SysAid relies on Amazon Web Services global infrastructure, including the facilities, network, hardware, and operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of basic computing resources and storage. This infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards: ISO 27001:2013, ISO 27017, ISO 27018, AICPA SOC 2and PCI-DSS and more. The environmental protection managed by the vendors policies are:

- Redundancy - The data centers are designed to anticipate and tolerate failure while maintaining service levels with core applications deployed to multiple regions.
- Fire Detection and Suppression – Automatic fire detection and suppression equipment has been installed to reduce risk.
- Redundant Power – the data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and Uninterruptable Power Supply (UPS) units provide back-up power in the event of an electrical failure. Data centers use generators to provide back-up power for the entire facility.
- Climate and Temperature Controls – maintain a constant operating temperature and humidity level for all hardware.
- Physical access - AWS recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures and controls have been implemented to help prevent unauthorized access to data, assets and restricted areas.

Application Security

Penetration Testing - The penetration tests include, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. In addition, security scans are performed on a semi-annual basis. The penetration tests and security scans are performed by a reputable third-party vendor. An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved (38).

Vulnerabilities Management - *W*eb application architecture and implementation follow OWASP guidelines. The application is regularly tested for common vulnerabilities (such as CSRF, XSS, SQL Injection). Vulnerability scans are performed in order to detect potential security breaches. Vulnerabilities are tracked until resolution. Reports are created and sent to the security team (37).

Segregation of Customer Data - SysAid employs a login system and authorization mechanism based on industry best practices. During each user request, a validation process is performed through encrypted identifiers to ensure that only authorized users gain access to the specific data. The process is validated by third-party security consultants on a yearly basis.

Operational Security

Configuration and Patch Management – SysAid employs a centrally managed configuration management system, including infrastructure-as-code systems through which predefined configurations are enforced on its servers, as well as the desired patch levels of the various software components.

Security Incident Response Management - Whenever a security incident of a physical or electronic nature is suspected or confirmed, SysAid's engineers are instructed to follow appropriate procedures. Customers and legal authorities will be notified as recurred by Privacy regulations.

Antivirus - Anti-virus definition updates are performed and monitored on a regular basis by the IT and Operations teams. The employees' laptops are encrypted with the use of a 256-bit AES encryption. Antivirus software is installed on workstations, laptops, and servers supporting such software. SysAid uses a centralized management tool in order to receive alerts of the antivirus status (39).

Unified Endpoint Management - SysAid uses a dedicate tool that implemented an Agent in advance on the company's endpoint in order to monitor and control the updates, data, content, configuration and encryption of the asset. The company Security Policy is enforced using a dedicate tool.

Human Resource Security

Security Awareness Training – SysAid's employees undergo an information security awareness training upon joining the company, as well as periodically in conformance to SysAid's information security policy. The training ensures that each group of employees receive security training according to its technical knowledge and its needs. Employees go through annual security awareness training based on the SysAid security policy (10).

Secure Coding Standards and Training - *SysAid's* R&D team is regularly trained in secure coding practices such as CERT Oracle Secure Coding Standard for Java and the OWASP top 10. Furthermore, it is involved with analyzing penetration test results and defining the 'lessons learned'.

Data Encryption

Data in transit - all traffic between the customer and the SysAid platform is encrypted through TLS with only the most secure algorithms enabled. Encryption between SysAid customers and the Application as well as between SysAid sites is enabled using an authenticated TLS tunnel. Connections to the SysAid network and databases are obtained through a secured IPSEC tunnel, only accessible from within the production network. Clients' sessions and interactions are encrypted using 256bit SSL V3/TLS HTTPS. Customer passwords are encrypted within the database (53). Interactions between customers and the SysAid platform are performed by using an encrypted channel based on an authenticated SSL connection (54). Internet traffic is encrypted using high class level certificates based on the PKI infrastructure. SysAid uses encryption to supplement other measures used to protect data-at-rest when such protections are deemed appropriate based on assessed risk. Processes are in place to protect encryption keys during generation, storage, use, and destruction.

Data at rest - Encrypted based on AWS's data at rest encryption policies which adhere to the following: Several layers of encryption to protect customer data at rest in Amazon Web Services products. Data stored in AWS is encrypted at the storage level using AES256 Customer content stored at rest is encrypted, without any action required from the customer, using one or more encryption mechanisms. Data for storage is split into chunks, and each chunk is encrypted with a unique data encryption key. These data encryption keys are stored with the data, encrypted with ("wrapped" by) key encryption keys that are exclusively stored and used inside Amazon's central Key Management Service. Amazon's Key Management Service is redundant and globally distributed. A common cryptographic library is used to implement encryption consistently across almost all Google Cloud Platform products. Because this common library is widely accessible, only a small team of cryptographers needs to properly implement and maintain this tightly controlled and reviewed code.

Support

SysAid's customer support procedures are designed to handle and resolve issues and requests in a timely manner. This includes issues that are internally identified, or issues submitted by clients. SysAid provides its clients with three types of support. SysAid customers choose either the Standard support level, Premium support level or Customized support level (as per customer request). All three types are available 24/7/365 via support mail, support hotline and customer support portal. Support metrics are generated from the CRM application which include Key Performance Indicators (KPI). The KPIs are sent to relevant stakeholders (15). Service interruptions and maintenance notifications are sent by email to customers and employees (21).

Ticketing and Management

SysAid opens a ticket when an issue is raised by a client or when an issue is proactively identified. SysAid uses a third-party CRM application to manage, classify and ticket the client support-related issues. Tickets are classified by the level of urgency and assigned to the appropriate support tier for resolution. Response time to customer issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract (22).

Incident Management Process

A help-desk application is available to SysAid employees in order to report breaches in system security, availability, and confidentiality. New employees are trained in the use of this application at the beginning of their employment. SysAid has a security incident response management policy. Incidents trigger tickets and are tracked to resolution (40). The process is initiated when a new ticket is submitted in the helpdesk application or through emails. The company has a procedure and process in place to raise and manage Information Security Incidents. Incidents are classified according to the level of urgency and importance. Incidents can be submitted into the system following a customer-identified issue, through both manual and automated proactive checks, or automatically through an email request. The application has pre-defined steps that are assigned to a pre-defined group of employees. The completion of each step is recorded in the application. When an incident is submitted, an email is sent to the IT and Information Security Director. Resources are allocated in order to investigate the incident and resolve the issue. The Information Security Manager is responsible for escalating critical incidents and perform Lesson Learned reviews. By procedure and according to a strict SLA, Incident notifications are sent to customers in the case that their data has been impacted. Root cause analysis is performed following security incidents (41).

Escalation Process

SysAid's goal is to resolve issues in an efficient manner. The issue is tracked and updated in the support ticketing system. The escalation process is defined and documented by Customer Support. Tickets are escalated as deemed necessary to Security, R&D or Technical Services teams. Service interruptions are communicated to clients using e-mail based on the escalation procedures and Service Level Agreement (SLA) notification thresholds. In addition, to maintain visibility on current support issues and potential problem trends, support metrics (including Key Performance Indicators) are generated from the support application and sent to Company's stakeholders on a regular basis.

Availability Procedures

SysAid database is backed up according to the backup policy. The logs are backed up on a daily basis (49). SysAid's production environment is fully managed as part of the AWS services and monitored by SYSAID Operation team using the tools provided by AWS as well as internal tools. The application level is fully managed by the SysAid Security team. SysAid has implemented the operations management controls described below to manage and execute production operations.

Database Backup

SysAid’s databases are hosted at AWS. and fully on a weekly and monthly basis. The backup system automatically generates a backup log. In case of failure, a notification is sent to the operation team. The company hold replica to each data center for high-availability standards in case of a disaster. SysAid databases are replicated in several availability zones (50).

Restoration

Backup data captured as part of the daily, weekly and monthly backup procedures is restored automatically into a separate environment in order to determine the integrity of data and potential data recovery issues. A log of the restoring process is sent to the Director of Operations for review. A restore process is performed and documented on an annual basis (51).

Data center availability procedures

AWS provides SysAid with a secured location implementing security measures to protect against environmental risks or disaster.

Disaster Recovery Plan (DRP)

SysAid has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of disaster. The DRP is tested on an annual basis (52). SysAid has developed a Business Continuity Plan to enable the company to continue to provide critical services in case of a disaster. SysAid maintains a backup server's infrastructure at a separate location within the AWS environments. The backup server's infrastructure has been designed to provide clients with business-critical services until the disaster has been resolved and the primary system is fully restored. The alternative processing environment is wholly managed by appropriate SYSAID personnel, as is the case with the primary production environment.

Monitoring Usage

The management team is updated on an annual basis on security, confidentiality and availability non-compliance issues that may come up and address them as needed. Such issues are documented as part of a support process and if necessary, notifications are sent to the Security team or the Information Security Manager. Change reports, vulnerability reports from production and monitoring tools as well as support metrics are reviewed and discussed in relation to organization's system security, availability and confidentiality policies. In addition, environmental, regulatory and technological changes are monitored. Their effects are assessed, and their policies are updated accordingly. A summarized protocol is made available to relevant managers and team members. Actions performed on the production environment, including OS, DB and application are monitored, logged and reviewed. Alerts are triggered upon the identification of an anomaly (23).

Confidentiality Procedures

Customer confidentiality is key factor in SysAid. As such, SysAid has implemented security measures to ensure the confidentiality of its customer’s sensitive personal information. The security measures aim to prevent unauthorized access, disclosure, alteration or destruction of sensitive personal information. Upon customer request at the end of a contract agreement, SysAid will dispose of customer confidential information (56). In this context, SysAid has adopted the ISO 27018 standard. In addition, connections to the SysAid network and databases are obtained through a secured IPSEC tunnel, only accessible from within the production network. Business partners are required to sign an agreement containing a confidentiality clause (55). Moreover, new employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses (9).

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 the virtual and physical servers, software, firewalls and physical 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.

Complementary User Entity Controls (CUECs)

In designing its system, SysAid allows for certain complementary controls to be implemented by user organizations to meet certain criteria applicable to security, availability, confidentiality, and privacy. A customer organization’s overall internal control structure should be in operation and evaluated in conjunction with SysAid’s controls presented in this section of the report.

The Kost Forer Gabbay and Kasierer (KFGK) examination was limited to the design of the controls in place at SysAid as they relate to SysAid’s customers. Accordingly, the examination did not extend to any controls beyond those listed in this report or those in place at customer organizations. The Complementary User Entity Controls section describes controls that have to be placed in operation at customers to complement SysAid’s controls. It is each interested party’s responsibility to evaluate the user entity control considerations presented in this section in relation to the internal controls that are in place at customer organizations in order to obtain a complete understanding of the total internal control structure surrounding the SysAid hosted services and application and to assess risk control. The portions of the internal control provided by the customer organizations are to be evaluated together with SysAid. If effective internal customer organization controls are not in place, SysAid’s controls may not be adequate to compensate for such weaknesses. Furthermore, this list is only a partial list of controls that customer organizations should have in place in order to complement the controls of SysAid.

SysAid Technologies' Customers’ Responsibilities

- Implementing sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with SysAid Technologies.
- 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 SysAid Technologies' services.
- Maintaining authorized, secure, timely, and complete transactions for user organizations relating to SysAid Technologies' services.
- Protecting data that is sent to SysAid Technologies by using appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.
- Implementing controls requiring additional approval procedures for critical transactions relating to SysAid Technologies' services.
- Reporting to SysAid Technologies in a timely manner any material changes to their overall control environment that may adversely affect services being performed by SysAid Technologies.

- Notifying SysAid Technologies in a timely manner of any changes to personnel directly involved with services performed by SysAid Technologies. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by SysAid Technologies.
- Adhering to the terms and conditions stated within their contracts with SysAid Technologies.
- Developing, and if necessary, implementing a business continuity and disaster recovery plan (DRP) that will aid in the continuation of services provided by SysAid Technologies.

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 SysAid, Kost Forer Gabbay & Kasierer (KFGK) considered aspects of SysAid’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 Control

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 SysAid. The testing performed by KFGK and the results of the tests are the responsibility of the service auditor. Refer to the Trust Services criteria mapping section for the mapping of these controls to the Trust Services criteria.

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
7	Job descriptions are documented and maintained within the SysAid website and on external tools. Candidates go through screening and appropriate reference checks.	Inspected SysAid's website and determined that job descriptions were documented and maintained within the company website. Inspected the reference checks for a sample of new employees and determined that candidates went through screening and appropriate reference checks.	No deviations noted.
9	New employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses.	Inspected the signed employment agreement for a sample of new employees and determined the agreement included confidentiality and intellectual properly clauses.	No deviations noted.
55	Business partners are required to sign an agreement containing a confidentiality clause.	Inspected examples of signed business partner agreements and determined that the agreements contained a confidentiality clause.	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	The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda to review (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	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	The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda to review (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The management of the company meets on a weekly basis to discuss on-going issues and updates.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a weekly basis and that meeting minutes were retained.	No deviations noted.
3	An organizational chart is documented and approved by management that clearly defines management authorities and reporting hierarchy.	Inspected SysAid's organizational chart and determined that the chart was documented and management authorities and reporting hierarchy were clearly defined.	No deviations noted.
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to SysAid's employees within the SysAid internal portal.	Inspected the policies and determined that they were documented, reviewed, and approved by management on an annual basis. Inspected the internal portal and determined that policies were available to employees.	No deviations noted.
6	An information security policy is documented, reviewed and approved by SysAid management on an annual basis. The security policy is available to SysAid employees within the SysAid portal.	Inspected SysAid's information security policy and determined that it was documented, reviewed, and approved by management on an annual basis. Inspected the internal portal and determined that the policy was available to employees.	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
7	Job descriptions are documented and maintained within the SysAid website and on external tools. Candidates go through screening and appropriate reference checks.	Inspected SysAid's website and determined that job descriptions were documented and maintained within the company website. Inspected the reference checks for a sample of new employees and determined that candidates went through screening and appropriate reference checks.	No deviations noted.
8	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different SysAid policies and work procedures.	Inspected the onboarding checklists for a sample of new employees and determined that new employees went through an onboarding process during which, among others, their responsibilities and the different SysAid policies were communicated.	No deviations noted.
10	Employees go through annual security awareness training based on the SysAid security policy.	Inspected the security awareness training materials and the certificate of completion for a sample of employees and determined that employees went through awareness training on an annual basis.	No deviations noted.
11	Personnel responsible for the design, development, implementation, and operation of systems affecting security, availability, confidentiality, undergo training on an annual basis.	Inspected SysAid's training program and the certificate of completion for a sample of R&D employees and determined that training was performed on an ad hoc basis by R&D personnel.	No deviations noted.
14	Employees go through a feedback process on at least an annual basis. The feedback reports are retained within the employee personal record.	Inspected the employees' feedback reports for a sample of employees and determined there was a documented annual employee feedback process in place.	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	An organizational chart is documented and approved by management that clearly defines management authorities and reporting hierarchy.	Inspected SysAid's organizational chart and determined that the chart was documented and management	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		authorities and reporting hierarchy were clearly defined.	
8	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different SysAid policies and work procedures.	Inspected the onboarding checklists for a sample of new employees and determined that new employees went through an onboarding process during which, among others, their responsibilities and the different SysAid policies were communicated.	No deviations noted.
9	New employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses.	Inspected the signed employment agreement for a sample of new employees and determined the agreement included confidentiality and intellectual properly clauses.	No deviations noted.
11	Personnel responsible for the design, development, implementation, and operation of systems affecting security, availability, confidentiality, undergo training on an annual basis.	Inspected SysAid's training program and the certificate of completion for a sample of R&D employees and determined that training was performed on an ad hoc basis by R&D personnel.	No deviations noted.
14	Employees go through a feedback process on at least an annual basis. The feedback reports are retained within the employee personal record.	Inspected the employees' feedback reports for a sample of employees and determined there was a documented annual employee feedback process in place.	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
15	Support metrics are generated from the CRM application which include Key Performance Indicators (KPI). The KPIs are sent to relevant stakeholders.	Inspected the CRM tool dashboards and determined that the support metrics were available. Inspected a sample of reports and determined that KPI reports were sent to relevant stakeholders.	No deviations noted.
16	Risks and threats are evaluated by key SysAid stakeholders during an annual meeting. Action items are documented within minutes of the meeting.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key SysAid stakeholders during an annual risk	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		assessment. Minutes of risk assessment meetings and actions items were documented.	

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
4	A description of the SysAid system and its boundaries is documented and communicated to the relevant SysAid employees and to external users through SysAid's website.	Inspected SysAid's website and determined that a description of the SysAid system and its boundaries was documented and available to employees. Inspected SysAid's website and determined that a description of the SysAid system and its boundaries was documented and available to external users.	No deviations noted.
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to SysAid's employees within the SysAid internal portal.	Inspected the policies and determined that they were documented, reviewed, and approved by management on an annual basis. Inspected the internal portal and determined that policies were available to employees.	No deviations noted.
6	An information security policy is documented, reviewed and approved by SysAid management on an annual basis. The security policy is available to SysAid employees within the SysAid portal.	Inspected SysAid's information security policy and determined that it was documented, reviewed, and approved by management on an annual basis. Inspected the internal portal and determined that the policy was available to employees.	No deviations noted.
8	New employees go through an onboarding process during which, among others, are communicated their responsibilities and the different SysAid policies and work procedures.	Inspected the onboarding checklists for a sample of new employees and determined that new employees went through an onboarding process during which, among others, their responsibilities and the different SysAid policies were communicated.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
10	Employees go through annual security awareness training based on the SysAid security policy.	Inspected the security awareness training materials and the certificate of completion for a sample of employees and determined that employees went through awareness training on an annual basis.	No deviations noted.
14	Employees go through a feedback process on at least an annual basis. The feedback reports are retained within the employee personal record.	Inspected the employees' feedback reports for a sample of employees and determined there was a documented annual employee feedback process in place.	No deviations noted.
15	Support metrics are generated from the CRM application which include Key Performance Indicators (KPI). The KPIs are sent to relevant stakeholders.	Inspected the CRM tool dashboards and determined that the support metrics were available. Inspected a sample of reports and determined that KPI reports were sent to relevant stakeholders.	No deviations noted.
22	Response time to customer issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.	Inspected SysAid's SLA agreement and an extraction of customer support tickets and determined that response time to customer issues was according to the company's SLA.	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
4	A description of the SysAid system and its boundaries is documented and communicated to the relevant SysAid employees and to external users through SysAid's website.	Inspected SysAid's website and determined that a description of the SysAid system and its boundaries was documented and available to employees. Inspected SysAid's website and determined that a description of the SysAid system and its boundaries was documented and available to external users.	No deviations noted.
12	New features are communicated to customers, if relevant, through emails, the website or directly through the account manager.	Inspected a sample of release notes and determined that new features were communicated to customers through emails, the website or directly through the account manager.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
21	Service interruptions and maintenance notifications are sent by email to customers and employees.	Inspected SysAid's status page and determined that the uptime report was available to customers.	No deviations noted.
22	Response time to customer issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.	Inspected SysAid's SLA agreement and an extraction of customer support tickets and determined that response time to customer issues was according to the company's SLA.	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
16	Risks and threats are evaluated by key SysAid stakeholders during an annual meeting. Action items are documented within minutes of the meeting.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key SysAid stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were documented.	No deviations noted.
17	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. 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 it was performed and documented annually.	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	The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda to review (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The management of the company meets on a weekly basis to discuss on-going issues and updates.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a weekly basis and that meeting minutes were retained.	No deviations noted.
16	Risks and threats are evaluated by key SysAid stakeholders during an annual meeting. Action items are documented within minutes of the meeting.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key SysAid stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were documented.	No deviations noted.
17	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. 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 it was performed and documented annually.	No deviations noted.

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	The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda to review (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The management of the company meets on a weekly basis to discuss on-going issues and updates.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a weekly basis and that meeting minutes were retained.	No deviations noted.
16	Risks and threats are evaluated by key SysAid stakeholders during an annual meeting. Action items are documented within minutes of the meeting.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key SysAid stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were documented.	No deviations noted.
17	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. 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 it was performed and documented annually.	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
1	The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda to review (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The management of the company meets on a weekly basis to discuss on-going issues and updates.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a weekly basis and that meeting minutes were retained.	No deviations noted.
37	Vulnerability scans are performed in order to detect potential security breaches. Vulnerabilities are tracked until resolution. Reports are created and sent to the security team.	Inspected the vulnerability scanning tool configuration and determined that vulnerability scans were configured to run on a weekly basis using an external tool on the production environment. Inspected the vulnerability scan report and determined that reports were sent to the security team on an annual basis. Inspected an example of a vulnerability ticket and determined that vulnerabilities were tracked until resolution.	No deviations noted.
38	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.	Inspected the penetration test report and determined that it was performed on an annual basis. Inspected the penetration test report and determined that critical and high issues were investigated and resolved.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
52	SysAid has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of disaster. The DRP is tested on an annual basis.	Inspected the Disaster Recovery Plan and determined that the policy was reviewed and approved on an annual basis. Inspected the Disaster Recovery test and determined that the DRP was tested on an annual basis.	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
19	SysAid assesses on an annual basis, the risks that vendors and business partners represent to the achievement of the company's objectives.	Inspected the vendor assessment and determined that vendors were assessed annually for the risk they may represent to the achievement of the company's objectives.	No deviations noted.
23	Actions performed on the production environment, including OS, DB and application are monitored, logged and reviewed. Alerts are triggered upon the identification of an anomaly.	Inspected the monitoring logs and determined that actions performed in the production and database environments were logged and reviewed. Inspected examples of alerts rules configuration and determined that alerts were triggered upon the identification of an anomaly.	No deviations noted.
24	SysAid uses a suite of monitoring tools in order to monitor its service. The production environment, including the servers and application, is monitored by the Operation Team.	Inspected SysAid’s monitoring dashboards and configuration and determined that SysAid used a suite of monitoring tools to monitor its service. Inspected SysAid’s monitoring configuration and examples of alerts and determined that alerts were sent to relevant stakeholders by an internal communication tool 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
1	The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda to review (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The management of the company meets on a weekly basis to discuss on-going issues and updates.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a weekly basis and that meeting minutes were retained.	No deviations noted.
24	SysAid uses a suite of monitoring tools in order to monitor its service. The production environment, including the servers and application, is monitored by the Operation Team.	Inspected SysAid’s monitoring dashboards and configuration and determined that SysAid used a suite of monitoring tools to monitor its service. Inspected SysAid’s monitoring configuration and examples of alerts and determined that alerts were sent to relevant stakeholders by an internal communication tool 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
16	Risks and threats are evaluated by key SysAid stakeholders during an annual meeting. Action items are documented within minutes of the meeting.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key SysAid stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were documented.	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
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to SysAid's employees within the SysAid internal portal.	Inspected the policies and determined that they were documented, reviewed, and approved by management on an annual basis. Inspected the internal portal and determined that policies were available to employees.	No deviations noted.
10	Employees go through annual security awareness training based on the SysAid security policy.	Inspected the security awareness training materials and the certificate of completion for a sample of employees and determined that employees went through awareness training on an annual basis.	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	An organizational chart is documented and approved by management that clearly defines management authorities and reporting hierarchy.	Inspected SysAid's organizational chart and determined that the chart was documented and management authorities and reporting hierarchy were clearly defined.	No deviations noted.
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to SysAid's employees within the SysAid internal portal.	Inspected the policies and determined that they were documented, reviewed, and approved by management on an annual basis. Inspected the internal portal and determined that policies were available to employees.	No deviations noted.
6	An information security policy is documented, reviewed and approved by SysAid management on an annual basis. The security policy is available to SysAid employees within the SysAid portal.	Inspected SysAid's information security policy and determined that it was documented, reviewed, and approved by management on an annual basis. Inspected the internal portal and determined that the policy was available to employees.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
20	SysAid has implemented a vendor management policy which details the vendor termination process. The policy is reviewed and approved annually.	Inspected the vendor management policy and determined that it was documented, reviewed, and approved annually. Inspected the vendor management policy and determined that SysAid detailed the vendor termination process.	No deviations noted.
22	Response time to customer issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.	Inspected SysAid's SLA agreement and an extraction of customer support tickets and determined that response time to customer issues was according to the company's SLA.	No deviations noted.
42	There is a documented change management policy. The policy is reviewed and approved on an annual basis.	Inspected the change management policy and determined that it was reviewed and approved on an annual basis.	No deviations noted.
52	SysAid has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of disaster. The DRP is tested on an annual basis.	Inspected the Disaster Recovery Plan and determined that the policy was reviewed and approved on an annual basis. Inspected the Disaster Recovery test and determined that the DRP was tested on an annual basis.	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
25	Users are identified through the use of a user ID/password combination using an SSO tool. Strong password configuration settings, where applicable, are enabled including: (1) forced password change at defined intervals, (2) a minimum password length,	Inspected the Single Sign-On password configuration settings and determined that strong password configuration settings, where applicable, were enabled on the SSO and native tools, including: (1) forced password change at defined intervals; (2) a minimum	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	(3) a limit on the number of attempts to enter a password before the user ID is suspended, and (4) password complexity.	password length; (3) a limit on the number of attempts to enter a password before the user ID was suspended; and (4) password complexity.	
26	The access to the production server is performed using SSH key and is restricted to authorized personnel.	Inspected the list of users with access to the production server by SSH key and determined it was restricted to authorized personnel. Inspected the SSH configuration and determined that it was restricted to authorized personnel.	No deviations noted.
28	Developers do not have access to the production and database environments. Specific developers can be granted access for specific projects. These accesses are logged and reviewed.	Inspected the list of users with access permissions to the production and database environment and determined that developers did not have access to the production and database. Inspected the log configuration and determined that accesses were logged and reviewed.	No deviations noted.
30	Access to the source control tool is performed using MFA and is restricted to authorized personnel.	Inspected the list of users with access to the source control tool and determined it was restricted to authorized personnel. Inspected the list of users with access to the source control tool and determined that MFA was enabled.	No deviations noted.
36	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 configuration settings and determined that 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 it was restricted to authorized personnel.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
46	The permission to approve merge requests and to deploy is restricted to authorized personnel.	Inspected the list of users with permission to approve merge requests and deploy and determined that it was restricted to authorized personnel.	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
27	Terminated employees who had access to the production environment have their permissions removed and company equipment returned in a timely manner.	Inspected the offboarding checklist for a sample of terminated employees and determined that permissions were revoked in a timely manner and assets were returned.	No deviations noted.
31	New employees are granted access to the different environments by a ticketing system process and subject to manager approval.	Inspected access granting tickets for a sample of new employees and determined that the access provisioning was initiated during onboarding, limited to role-specific access, and approved by authorized personnel.	No deviations noted.
32	Permissions to the different environments (production, databases and applications) are reviewed, approved and documented by the SysAid management on a bi - yearly basis.	Inspected the user access review documentation and determined that accesses and permissions for the different environments were reviewed and approved by the management on a bi - yearly basis.	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
27	Terminated employees who had access to the production environment have their permissions removed and company equipment returned in a timely manner.	Inspected the offboarding checklist for a sample of terminated employees and determined that permissions were revoked in a timely manner and assets were returned.	No deviations noted.
31	New employees are granted access to the different environments by a ticketing system process and subject to manager approval.	Inspected access granting tickets for a sample of new employees and determined that the access provisioning	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		was initiated during onboarding, limited to role-specific access, and approved by authorized personnel.	
32	Permissions to the different environments (production, databases and applications) are reviewed, approved and documented by the SysAid management on a bi - yearly basis.	Inspected the user access review documentation and determined that accesses and permissions for the different environments were reviewed and approved by the management on a bi - yearly basis.	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
33	Physical access to the offices is restricted to authorized personnel using a personal identification card according to the physical access policy.	Inspected the physical access policy and determined that physical access was restricted to authorized personnel using personal identification cards.	No deviations noted.
34	Visitors to the SysAid office are accompanied while on premises.	Performed a walkthrough of SysAid's office and inspected the physical access policy and determined that visitors were accompanied while on premises.	No deviations noted.
35	SysAid performs a review of the SOC 2 report of its third party infrastructure provider on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at SysAid to address the CUECs.	Inspected the review of the data center SOC 2 report performed by SysAid and determined that the review was performed annually and included an investigation of deviations and identifying and documenting the controls in place at SysAid 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
35	SysAid performs a review of the SOC 2 report of its third party infrastructure provider on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at SysAid to address the CUECs.	Inspected the review of the data center SOC 2 report performed by SysAid and determined that the review was performed annually and included an investigation of deviations and identifying and documenting the controls in place at SysAid 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
29	Access to system resources is protected through a combination of firewalls, VPNs, native operating system security, database management system security, application controls and intrusion detection monitoring software.	Inspected the system architecture diagram and determined that access was protected through a combination of firewalls, VPNs, native operating system security, database management system security and application controls and intrusion detection monitoring software.	No deviations noted.
54	Interactions between customers and the SysAid platform are performed by using an encrypted channel based on an authenticated SSL connection.	Inspected the encryption configuration and determined that the encryption between SysAid customers and the SysAid application was enabled using an authenticated SSL tunnel.	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
29	Access to system resources is protected through a combination of firewalls, VPNs, native operating system security, database management system security, application controls and intrusion detection monitoring software.	Inspected the system architecture diagram and determined that access was protected through a combination of firewalls, VPNs, native operating system security, database management system security and application controls and intrusion detection monitoring software.	No deviations noted.
54	Interactions between customers and the SysAid platform are performed by using an encrypted channel based on an authenticated SSL connection.	Inspected the encryption configuration and determined that the encryption between SysAid customers and the SysAid application was enabled using an authenticated SSL tunnel.	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
37	Vulnerability scans are performed in order to detect potential security breaches. Vulnerabilities are	Inspected the vulnerability scanning tool configuration and determined that vulnerability scans were	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	tracked until resolution. Reports are created and sent to the security team.	configured to run on a weekly basis using an external tool on the production environment. Inspected the vulnerability scan report and determined that reports were sent to the security team on an annual basis. Inspected an example of a vulnerability ticket and determined that vulnerabilities were tracked until resolution.	
38	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.	Inspected the penetration test report and determined that it was performed on an annual basis. Inspected the penetration test report and determined that critical and high issues were investigated and resolved.	No deviations noted.
39	Antivirus software is installed on workstations, laptops, and servers supporting such software. SysAid uses a centralized management tool in order to receive alerts of the antivirus status.	Inspected the unified endpoint management tool configuration and dashboard and determined that an antivirus solution was installed on employees laptops.	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
37	Vulnerability scans are performed in order to detect potential security breaches. Vulnerabilities are tracked until resolution. Reports are created and sent to the security team.	Inspected the vulnerability scanning tool configuration and determined that vulnerability scans were configured to run on a weekly basis using an external tool on the production environment.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected the vulnerability scan report and determined that reports were sent to the security team on an annual basis. Inspected an example of a vulnerability ticket and determined that vulnerabilities were tracked until resolution.	
38	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.	Inspected the penetration test report and determined that it was performed on an annual basis. Inspected the penetration test report and determined that critical and high issues were investigated and resolved.	No deviations noted.
39	Antivirus software is installed on workstations, laptops, and servers supporting such software. SysAid uses a centralized management tool in order to receive alerts of the antivirus status.	Inspected the unified endpoint management tool configuration and dashboard and determined that an antivirus solution was installed on employees laptops.	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
22	Response time to customer issues is defined in the SLA agreement. The agreement is communicated to the customers as part of the contract.	Inspected SysAid's SLA agreement and an extraction of customer support tickets and determined that response time to customer issues was according to the company's SLA.	No deviations noted.
24	SysAid uses a suite of monitoring tools in order to monitor its service. The production environment, including the servers and application, is monitored by the Operation Team.	Inspected SysAid’s monitoring dashboards and configuration and determined that SysAid used a suite of monitoring tools to monitor its service.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected SysAid's monitoring configuration and examples of alerts and determined that alerts were sent to relevant stakeholders by an internal communication tool based on pre-defined rules.	
38	An external penetration test is performed on an annual basis. Critical and high issues are investigated and resolved.	Inspected the penetration test report and determined that it was performed on an annual basis. Inspected the penetration test report and determined that critical and high issues were investigated and resolved.	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
24	SysAid uses a suite of monitoring tools in order to monitor its service. The production environment, including the servers and application, is monitored by the Operation Team.	Inspected SysAid's monitoring dashboards and configuration and determined that SysAid used a suite of monitoring tools to monitor its service. Inspected SysAid's monitoring configuration and examples of alerts and determined that alerts were sent to relevant stakeholders by an internal communication tool based on pre-defined rules.	No deviations noted.
37	Vulnerability scans are performed in order to detect potential security breaches. Vulnerabilities are tracked until resolution. Reports are created and sent to the security team.	Inspected the vulnerability scanning tool configuration and determined that vulnerability scans were configured to run on a weekly basis using an external tool on the production environment. Inspected the vulnerability scan report and determined that reports were sent to the security team on an annual basis.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		Inspected an example of a vulnerability ticket and determined that vulnerabilities were tracked until resolution.	
40	SysAid has a security incident response management policy. Incidents trigger tickets and are tracked to resolution.	Inspected the incident response policy and determined that it defined the steps to be taken upon identification of a security incident. During the audit period, no security events occurred.	No deviations noted.
41	Root cause analysis is performed following security incidents.	Inspected the incident management policy and determined it included guidelines on how to perform a root cause analysis.	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
37	Vulnerability scans are performed in order to detect potential security breaches. Vulnerabilities are tracked until resolution. Reports are created and sent to the security team.	Inspected the vulnerability scanning tool configuration and determined that vulnerability scans were configured to run on a weekly basis using an external tool on the production environment. Inspected the vulnerability scan report and determined that reports were sent to the security team on an annual basis. Inspected an example of a vulnerability ticket and determined that vulnerabilities were tracked until resolution.	No deviations noted.
40	SysAid has a security incident response management policy. Incidents trigger tickets and are tracked to resolution.	Inspected the incident response policy and determined that it defined the steps to be taken upon identification of a security incident. During the audit period, no security events occurred.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
41	Root cause analysis is performed following security incidents.	Inspected the incident management policy and determined it included guidelines on how to perform a root cause analysis.	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
21	Service interruptions and maintenance notifications are sent by email to customers and employees.	Inspected SysAid's status page and determined that the uptime report was available to customers.	No deviations noted.
37	Vulnerability scans are performed in order to detect potential security breaches. Vulnerabilities are tracked until resolution. Reports are created and sent to the security team.	Inspected the vulnerability scanning tool configuration and determined that vulnerability scans were configured to run on a weekly basis using an external tool on the production environment. Inspected the vulnerability scan report and determined that reports were sent to the security team on an annual basis. Inspected an example of a vulnerability ticket and determined that vulnerabilities were tracked until resolution.	No deviations noted.
40	SysAid has a security incident response management policy. Incidents trigger tickets and are tracked to resolution.	Inspected the incident response policy and determined that it defined the steps to be taken upon identification of a security incident. During the audit period, no security events occurred.	No deviations noted.
41	Root cause analysis is performed following security incidents.	Inspected the incident management policy and determined it included guidelines on how to perform a root cause analysis.	No deviations noted.
52	SysAid has developed a Disaster Recovery Plan in order to continue to provide critical services in the	Inspected the Disaster Recovery Plan and determined that the policy was reviewed and approved on an annual basis.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	event of disaster. The DRP is tested on an annual basis.	Inspected the Disaster Recovery test and determined that the DRP was tested on an annual basis.	
51	A restore process is performed and documented on an annual basis.	Inspected the restoration test results and determined that the restore process was performed successfully and documented on an annual basis.	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
42	There is a documented change management policy. The policy is reviewed and approved on an annual basis.	Inspected the change management policy and determined that it was reviewed and approved on an annual basis.	No deviations noted.
43	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved within the change management application. Change management tickets are prioritized and labeled based on development phase and urgency.	Inspected the change management tickets for a sample of software and infrastructure changes that were merged to production and determined that changes were documented, prioritized, and labeled based on the development phase and urgency. Inspected the change management tickets for a sample of software and infrastructure changes that were merged to production and determined that tickets contained a documented description of the required change.	No deviations noted.
44	Tickets in the change management tool are connected to the source control tool in order to link the request to the code change.	Inspected the pull requests for a sample of software and infrastructure changes that were merged to production and determined that the code changes in the source control tool were linked to the change requirements documented in the change management tool.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
45	Code changes are reviewed along with the pull request performed by the team leader. The code review is documented on the source control tool. Code review is mandatory in order to continue in the SDLC process and deploy a version to the production environment.	Inspected the pull requests for a sample of software and infrastructure changes that were merged to production and determined that code reviews were conducted as part of the change management approval process. Inspected the source control tool configuration and determined that code review was mandatory to continue in the SDLC process.	No deviations noted.
47	Automation tests are performed using a dedicated tool on a regular basis in order to identify issues within the application.	Inspected a sample of software and infrastructure changes that were merged to production and determined that changes underwent automated testing.	No deviations noted.
48	A successful test status is required to continue in the SDLC process.	Inspected the source control tool's configuration and determined that a successful test status was mandatory in order to continue with 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
9	New employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses.	Inspected the signed employment agreement for a sample of new employees and determined the agreement included confidentiality and intellectual properly clauses.	No deviations noted.
16	Risks and threats are evaluated by key SysAid stakeholders during an annual meeting. Action items are documented within minutes of the meeting.	Inspected a sample of meeting minutes and invitations and determined that risks and threats were evaluated by key SysAid stakeholders during an annual risk assessment. Minutes of risk assessment meetings and actions items were documented.	No deviations noted.
18	Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to,	Inspected the risk assessment documentation and determined that a mitigation plan was associated with each identified risk.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the Company's objectives during response, mitigation, and recovery efforts.		

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	The management of the company meets on a weekly basis to discuss on-going issues and updates.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a weekly basis and that meeting minutes were retained.	No deviations noted.
19	SysAid assesses on an annual basis, the risks that vendors and business partners represent to the achievement of the company's objectives.	Inspected the vendor assessment and determined that vendors were assessed annually for the risk they may represent to the achievement of the company's objectives.	No deviations noted.
20	SysAid has implemented a vendor management policy which details the vendor termination process. The policy is reviewed and approved annually.	Inspected the vendor management policy and determined that it was documented, reviewed, and approved annually. Inspected the vendor management policy and determined that SysAid detailed the vendor termination process.	No deviations noted.
33	Physical access to the offices is restricted to authorized personnel using a personal identification card according to the physical access policy.	Inspected the physical access policy and determined that physical access was restricted to authorized personnel using personal identification cards.	No deviations noted.
34	Visitors to the SysAid office are accompanied while on premises.	Performed a walkthrough of SysAid's office and inspected the physical access policy and determined that visitors were accompanied while on premises.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
35	SysAid performs a review of the SOC 2 report of its third party infrastructure provider on an annual basis. Deviations are investigated. The review includes identifying and documenting the controls in place at SysAid to address the CUECs.	Inspected the review of the data center SOC 2 report performed by SysAid and determined that the review was performed annually and included an investigation of deviations and identifying and documenting the controls in place at SysAid to address the CUECs.	No deviations noted.
55	Business partners are required to sign an agreement containing a confidentiality clause.	Inspected examples of signed business partner agreements and determined that the agreements contained a confidentiality clause.	No deviations noted.

Availability

A1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
24	SysAid uses a suite of monitoring tools in order to monitor its service. The production environment, including the servers and application, is monitored by the Operation Team.	Inspected SysAid’s monitoring dashboards and configuration and determined that SysAid used a suite of monitoring tools to monitor its service. Inspected SysAid’s monitoring configuration and examples of alerts and determined that alerts were sent to relevant stakeholders by an internal communication tool based on pre-defined rules.	No deviations noted.
50	SysAid databases are replicated in several availability zones.	Inspected the SysAid database's configuration and determined that it was replicated in several availability zones.	No deviations noted.

A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
21	Service interruptions and maintenance notifications are sent by email to customers and employees.	Inspected SysAid's status page and determined that the uptime report was available to customers.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
49	SysAid database is backed up according to the backup policy. The logs are backed up on a daily basis.	Inspected the database backup configuration and determined that the SysAid application database was backed up on a daily basis.	No deviations noted.

A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
52	SysAid has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of disaster. The DRP is tested on an annual basis.	Inspected the Disaster Recovery Plan and determined that the policy was reviewed and approved on an annual basis. Inspected the Disaster Recovery test and determined that the DRP was tested on an annual basis.	No deviations noted.
51	A restore process is performed and documented on an annual basis.	Inspected the restoration test results and determined that the restore process was performed successfully and documented on an annual basis.	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	The Board of Directors meets on a quarterly basis. The Board meeting has a fixed agenda to review (1) Financial aspects details, (2) HR, (3) Pipeline of clients, (4) Support issues review, (5) Discussion on the product and new features.	Inspected a sample of board meeting minutes and invitations and determined that the board met on a quarterly basis and that meeting minutes were retained.	No deviations noted.
2	The management of the company meets on a weekly basis to discuss on-going issues and updates.	Inspected a sample of management meeting minutes and invitations and determined that the management met on a weekly basis and that meeting minutes were retained.	No deviations noted.

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
5	Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to SysAid's employees within the SysAid internal portal.	Inspected the policies and determined that they were documented, reviewed, and approved by management on an annual basis. Inspected the internal portal and determined that policies were available to employees.	No deviations noted.
9	New employees are required to sign a standard employment agreement outlining the confidentiality and the intellectual property clauses.	Inspected the signed employment agreement for a sample of new employees and determined the agreement included confidentiality and intellectual properly clauses.	No deviations noted.
53	Customer passwords are encrypted within the database.	Inspected the external tool configuration and determined that customer passwords were encrypted according to the SysAid security policy.	No deviations noted.
55	Business partners are required to sign an agreement containing a confidentiality clause.	Inspected examples of signed business partner agreements and determined that the agreements contained 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
56	Upon customer request at the end of a contract agreement, SysAid will dispose of customer confidential information.	Inspected the service termination procedure and determined that it outlined the steps to undertake if a client requested to have their confidential information disposed of. During the audit period, no such events occurred.	No deviations noted.

****