linford&co llp

Ledidi

TYPE II SOC 2

REPORT ON CONTROLS RELEVANT TO SECURITY

MAY 1, 2025 TO APRIL 30, 2026

Ledidi AS

Report on Ledidi's Description of Its Ledidi Services and Its Controls Relevant to Security

Table of Contents

Table of Contents (continued)

1550 wewatta st., 2nd floor
denver, co 80202
tel: + (720) 330 7201
email: info@linfordco.com

Section I – Independent Service Auditor's Report

To the Board of Directors of Ledidi AS:

Scope

We have examined Ledidi AS' (Ledidi or the Company) accompanying description of its Ledidi services titled, "Ledidi's Description of Its Ledidi Services" throughout the period May 1, 2025 to April 30, 2026 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance—2022)*, in AICPA *Description Criteria* (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period May 1, 2025 to April 30, 2026 to provide reasonable assurance that Ledidi's service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022),* in AICPA *Trust Services Criteria*.

Ledidi uses Amazon Web Services, Inc. (AWS), a subservice organization, to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Ledidi, to achieve Ledidi's service commitments and system requirements based on the applicable trust services criteria. The description presents Ledidi's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Ledidi's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Ledidi, to achieve Ledidi's service commitments and system requirements based on the applicable trust services criteria. The description presents Ledidi's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Ledidi's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Ledidi 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 Ledidi's service commitments and system requirements were achieved. Ledidi has provided the accompanying assertion titled "Assertion of Ledidi Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Ledidi is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation

of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

- ✓ Obtaining an understanding of the system and service organization's service commitments and system requirements.
- ✓ Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- ✓ Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- ✓ Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- ✓ Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- ✓ Evaluating the overall presentation of the description.

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

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

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in Section IV of this report titled, *Independent Service Auditor's Description of Tests of Controls and Results*.

Opinion

In our opinion, in all material respects:

a. The description presents Ledidi's services that were designed and implemented throughout the period May 1, 2025 to April 30, 2026 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period May 1, 2025 to April 30, 2026 to provide reasonable assurance that Ledidi'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 Ledidi's controls throughout that period.
c. The controls stated in the description operated effectively throughout the period May 1, 2025 to April 30, 2026 to provide reasonable assurance that Ledidi's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Ledidi's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Ledidi, user entities of Ledidi's services during some or all of the period May 1, 2025 to April 30, 2026, business partners of Ledidi subject to risks arising from interactions with the services, practitioners providing services to such user entities and business partners, prospective user entities and business partners, 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, business partners, subservice organizations, and 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 may affect the user entity's ability to effectively use the service organization's services.
- ✓ The applicable trust services criteria.
- ✓ The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

linford&co llp

May 1, 2026
Denver, Colorado

Section II – Assertion of Ledidi Management

May 1, 2026

We have prepared the accompanying description of Ledidi AS' (Ledidi or the Company) services titled, "Ledidi's Description of Its Ledidi Services" throughout the period May 1, 2025 to April 30, 2026 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance—2022)* in AICPA *Description Criteria* (description criteria). The description is intended to provide report users with information about the Ledidi services that may be useful when assessing the risks arising from interactions with Ledidi's system, particularly information about system controls that Ledidi 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 set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022),* in AICPA *Trust Services Criteria*.

Ledidi uses Amazon Web Services, Inc. (AWS), a subservice organization, to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Ledidi, to achieve Ledidi's service commitments and system requirements based on the applicable trust services criteria. The description presents Ledidi's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Ledidi's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Ledidi, to achieve Ledidi's service commitments and system requirements based on the applicable trust services criteria. The description presents Ledidi's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Ledidi's controls.

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

a. The description presents Ledidi's services that were designed and implemented throughout the period May 1, 2025 to April 30, 2026 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period May 1, 2025 to April 30, 2026 to provide reasonable assurance that Ledidi'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 Ledidi's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period May 1, 2025 to April 30, 2026 to provide reasonable assurance that Ledidi's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Ledidi's controls operated effectively throughout that period.

Danckert Mellbye
Chief Operating Officer

Section III – Ledidi's Description of Its Ledidi Services

Overview of Operations

Overview of Ledidi

Ledidi AS ("Ledidi" or the "Company") is a Norwegian health technology company headquartered in Oslo, Norway, with a UK subsidiary, Ledidi UK Ltd (company registration 14216477; ICO registration ZB521530).

Ledidi develops and operates a cloud-based platform for health and life sciences research and registries. The platform enables users to design studies, capture and collect structured research data, perform statistical analysis and data visualisation, and collaborate securely across institutions and jurisdictions.

Ledidi's customers are primarily medical, clinical and life sciences professionals, academic medical centres, hospitals, contract research organisations, and pharmaceutical and biotechnology companies, who use the platform for research, registries and clinical studies.

System Description

The Ledidi services in scope of this report are delivered by the Ledidi platform, a secure, multi-tenant research environment that supports the full research data lifecycle — from study design and data capture, through structured data management, statistical analysis and data visualisation, to controlled collaboration and project output.

The platform is designed to allow customers to process research data that may include electronic Protected Health Information (ePHI) subject to HIPAA, as well as personal data subject to the EU and UK General Data Protection Regulation, in a single environment governed by a common set of administrative, physical and technical safeguards.

Ledidi also offers a Trials module, designed to meet GxP requirements (FDA 21 CFR Part 11 and GAMP 5).

Components of the System Used to Provide the Services

The system used by Ledidi to deliver the Ledidi services is comprised of a combination of components that include the products and the data processed, but also extends to the underlying infrastructure, subservice organization's services supporting the platform, the Company's employees and contractors, as well as the policies and procedures followed to maintain the security of the Ledidi services and client data. The following is a summary of the components that comprise the system. Specific processes and controls relevant to the HIPAA requirements are described in the remainder of this section of the report.

Infrastructure
Ledidi's system is a Software-as-a-Service (SaaS) cloud-based system. The primary components of the system are built on top of AWS.

Subservice Organization: AWS is the principal subservice organisation used by Ledidi. AWS hosts Ledidi's production IT environment and provides managed infrastructure services including compute, primary and secondary data storage, encrypted backup, network isolation and key management.

AWS is certified under the EU-US Data Privacy Framework and the CISPE Code of Conduct (an EU cloud code approved under GDPR Article 40) and undergoes an annual SOC 2 Type II examination. Ledidi obtains and reviews the AWS SOC 2 report annually to confirm that the controls relevant to Ledidi's hosting environment are designed and operating effectively, and to identify and address any complementary user entity controls (CUECs) listed in that report. A Transfer Impact Assessment for AWS was completed in January 2026.

Ledidi uses Amazon RDS for PostgreSQL as the production database for customer research data. All data at rest is encrypted using AWS-managed keys, and data in transit is protected by TLS 1.2 or higher. Customer data is logically partitioned at the application and database layer to prevent unauthorised access across tenants.

Administrative access by Ledidi personnel to the production environment is restricted under the principle of least privilege and protected by complex passwords and multi-factor authentication; access is logged and reviewed (see Logical and Physical Access).

Software
The Ledidi services are developed and maintained by Ledidi personnel. The software engineering team enhances and maintains the Ledidi services to provide the current services and future enhancements to its user entities. Access to the Ledidi services is governed by the principle of least privilege. User entities are, in general, responsible for identifying the access needs for their users and for the security of those devices used to access the Ledidi services. Complementary user entity controls are noted within this description (Section III) to highlight control activities that Ledidi believes should be considered and/or present at each user entity of its Ledidi services.

People
Ledidi's staff is organised into functional areas — Engineering, Product, Customer Success, Quality and Compliance, and Commercial — reporting to the executive team and the Board of Ledidi AS. Designated roles include a Data Protection Officer, an Information Security Officer, and a Clinical Safety Officer (CSaO). Responsibilities, authorities and segregation of duties are defined in the Ledidi Quality Assurance and Internal ControI System (LICS) and all personnel complete annual security and data protection training.

Data

Sensitive customer data, including ePHI processed on behalf of HIPAA-regulated customers, is stored within the Ledidi platform's production databases hosted by AWS. Ledidi has implemented administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of customer data.

Access to data subject to HIPAA is restricted to authorised personnel with a documented business need, governed by role-based access control and least privilege. Customer data is logically partitioned at the application and database layer to prevent cross-tenant access. Data is encrypted at rest using AES-256 and in transit using Transport Layer Security (TLS) 1.2 or higher. The effectiveness of these safeguards is validated through annual third-party penetration testing (Mnemonic, most recently Q3 2025) and continuous monitoring.

Policies and Procedures

Ledidi's policies and procedures are maintained within the Ledidi LICS, the Company's integrated information security and quality management framework. LICS governs the development, operation, maintenance, support and security of the Ledidi services, and is certified to ISO 27001:2022 by Kiwa.

All policies and procedures are version-controlled, reviewed at least annually, approved by the relevant policy owner, and made available to personnel via an internal company site. Personnel are required to acknowledge applicable policies on hire and on material change.

Principal Service Commitments and System Requirements

Ledidi designs its processes and procedures to meet objectives for itsservices. Those objectives are based on the service commitments that Ledidi makes to user entities and the compliance requirements that Ledidi has established for their services.

Security commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security and confidentiality principles within the fundamental design of the Ledidi services are implemented to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Controlled access to the production environment and the supporting infrastructure.
- Segregation of client data.
- Monitoring of system performance metrics and critical application services.

Ledidi establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Ledidi’s system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around

how the service is designed and developed, how the system is operated, how the internal networks are managed, and how personnel are onboarded and trained.

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

Note: Parenthetical references have been included in the following narratives as a cross reference to the applicable control activities included in Section IV of this report.

A company's entity-level controls reflect the overall attitude, awareness, and actions of management and others concerning the importance of controls and the emphasis given to controls in the company's policies, procedures, methods, and organizational structure. Entity-level controls are not specific to any individual transaction but apply to the company as a whole. These types of controls are necessary to facilitate the proper functioning of activity-level controls supporting the Ledidi services. Throughout this section, a description is presented of the five components of internal control (control environment, risk assessment, information and communication, monitoring, and control activities) as they relate to the services Ledidi provides to its clients.

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. The security criteria and the controls designed, implemented, and operated to meet them such that the system is protected against unauthorized access (both physical and logical). Entity-level controls and specific control activities supporting the applicable trust services criteria are provided in the descriptions of this section of the report, and in *Section IV – Independent Service Auditor's Description of Tests of Controls and Results.*

Control Environment

A board of directors, consisting of internal and external individuals, exercises oversight of Ledidi's strategic direction, operational performance, and internal control **(1.1)**. In addition, Ledidi has an executive management team that guides the Company and sets the tone at the top of the organization that is followed by all employees. The tone is demonstrated through their directives, actions, and behavior, and highlights the importance of integrity and ethical values to support the functioning of the system of internal control. The executive management team meets on a weekly basis **(1.2)**.

To help employees understand expectations, executive management has established Ledidi's LICS. Ledidi's LICS applies to all full-time, part-time, and contractor staff and includes the following sections: goals and annual plan, security, code of conduct, disciplinary process, and reporting violations **(1.3)**.

Continuous Independent Compliance and Security Monitoring: Ledidi has established an internal compliance function and supporting tools which monitor the Ledidi control environment and alerts management when internal control and security issues arise **(1.4)**.

Organizational Structure: Management has established structures, reporting lines, and appropriate authorities in the pursuit of Ledidi's business objectives. The structures, reporting lines, and authority are communicated through management's operational style, the organizational structure, policies and procedures, and employee job descriptions. Ledidi's organizational structure defines authorities across the Company to facilitate information flow and establish responsibilities **(1.5)**. To increase the operational effectiveness of employees within this structure, every position has a job description so that individuals understand their responsibilities **(1.6)**. The role of HIPAA Security Officer has been assigned and communicated throughout the organization. The HIPAA Security Officer is responsible for the security of Ledidi's systems **(1.7)**.

Hiring: When a position is open at Ledidi, a job description and listing will be posted on Ledidi's website, as well as on other job forums. Additionally, Ledidi sources candidates via referrals. Resumes of applicants are received and reviewed by the hiring manager. The interview process is tailored to match the position being hired for and is a several-stage process. Applicants for full-time employment at Ledidi are required to complete a successful reference check as part of the terms of their employment **(1.8)**. As part of the hiring process, applicants are required to sign an employee contract that contains a confidentiality agreement **(1.9)**. An onboarding checklist is completed to monitor completion of employment documentation and acknowledgment of Ledidi's LICS and assigned policies **(1.10)**.

New Hire Training: New hires are required to complete Ledidi security awareness training and HIPAA training and sign the Health, Environment, & Security (HES) Declaration at the start of their position **(1.11)**.

Performance and Feedback: Ledidi evaluates competence across the entity in relation to established policies and practices and acts, as necessary, to address shortcomings. Employee performance and feedback reviews are performed at least annually **(1.12)**. Ledidi believes feedback is forward-looking and is information that someone can use to grow and develop. Performance assessments, however, look to the past to discover how an individual performed over the last six months. Feedback is provided on an ongoing basis and formally on a biannual basis. As part of the terms of the employment agreement with individuals, Ledidi maintains the right to discipline or terminate individuals based on a pattern of poor job performance.

Information and Communication

Internal Control Monitoring: Ledidi uses a variety of methods to monitor production systems and internal controls to support the functioning of internal controls. The methods include a compliance function for monitoring internal controls relevant to security compliance, as well as application and infrastructure monitoring tools and penetration testing.

Internal Communication: Ledidi maintains policies to communicate security and privacy responsibilities to Ledidi personnel **(2.1)**. The policies include objectives and responsibilities for internal control necessary to support the functioning of internal control. Policies are reviewed at least annually and updated, as necessary. Ledidi uses an internal communication tool to distribute policies and periodic security reminders

to employees including responsibilities related to security **(2.2)**. In addition, the policies are available for all employees to reference as needed.

Annual Security Awareness Training: To assist with Ledidi's commitments to security and HIPAA compliance, Ledidi management provides annual security awareness training and HIPAA training for all employees that covers information security, data protection, and confidentiality of client information **(2.3)**.

Service Offering and Service Agreement: Ledidi has created a high-level overview of the Ledidi system used to describe the services provided to the clients that Ledidi serves **(2.4)**. Ledidi and its clients' responsibilities and commitments regarding the acceptable use of the Ledidi system and Protected Health Information (PHI), as applicable, are included within the Ledidi Enterprise Agreement and Terms of Service, which clients must agree to before using the Ledidi software **(2.5)**. For any service provider handling PHI on behalf of Ledidi, a BAA (Business Associate Addendum) is also required to be executed **(2.6)**.

Complementary User Entity Controls: *User entities are responsible for executing any required contractual obligations per their regional regulations and/or requirements.*

Incident Reporting: Ledidi has provided methods to clients and employees to report failures, incidents, concerns, or other complaints related to the services or systems provided by Ledidi in the event there are problems **(2.7)**. Ledidi personnel may contact their supervisor or the Compliance Officer to report important matters requiring attention. Ledidi has established an incident procedure to define the process for handling incidents and roles and responsibilities for the personnel responding to the incidents.

Risk Assessment

Ledidi Risk Assessment and Management Program: Ledidi's risk assessment procedure describes the processes Ledidi has in place to identify new business and technical risks and how to achieve the desired level of risk **(3.1)**. The procedure document designates responsibility for risk management at Ledidi and outlines the process for identifying and addressing risks to the confidentiality, integrity, and security of client data that Ledidi accesses, stores, and transmits. The policy is made available to all employees through the Company's policy repository **(3.2)**. Key business and operational risks are closely monitored, particularly those related to the security of Ledidi's production environment, as these are especially critical risks that have the potential to affect the services provided to clients. Ledidi also mitigates business risks by adhering to industry practices to reduce risks related to the system.

Principles: Ledidi specifies risk management objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. Ledidi's primary duty is to maintain the security of critical systems and customer data. The duty to maintain a secure and available infrastructure requires Ledidi to identify and manage risks.

Risk Management Oversight: Overall, the execution, development, and implementation of risk assessments and remediation programs is the joint responsibility of Ledidi's Chief Operating Officer, Chief Technology Officer, Chief Product Officer, and the Compliance Officer. All departments and employees are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Annually, the risks identified are formally documented in a risk assessment matrix **(3.3)**. Each risk is assessed and given a risk rating. Risk owners work with the Compliance Officer in the development of a risk treatment plan per risk assessment performed and the risk assessment is reviewed by Ledidi management **(3.4)**.

Supplier Risk Management: Ledidi relies on suppliers to perform a variety of services, some of which are critical for operations. Ledidi aims to manage its relationship with suppliers and minimize the risk associated with engaging third parties to perform services. The supplier management procedures provide a framework for managing the life cycle of supplier relationships **(3.5)**. Risk assessments for suppliers are covered under Ledidi's supplier management program, which includes a risk assessment targeted at a particular suppliers' security and controls.

Fraud Risk: Ledidi has considered the potential for fraud when assessing risks to the achievement of objectives **(3.6)**.

Change Identification and Risk Assessment: Ledidi's risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates **(3.7)**.

Monitoring Activities

Application Logging and Monitoring: Ledidi uses monitoring tools to monitor application health and the monitoring tool alerts system administrators when the application is not operating within defined boundaries **(4.1)**. Ledidi uses various third-party tools for monitoring. When alerts from the tools are received, they are followed up on until they are resolved.

Infrastructure Logging and Monitoring: Ledidi logs authentication, availability, and error events and uses tools for infrastructure monitoring **(4.2)**. Every authentication event to the application and infrastructure records a log event that may be used later for forensic purposes to research security incidents. Clients of Ledidi may also enter service tickets regarding potential issues they are experiencing. The client-submitted tickets are addressed by Ledidi personnel **(4.3)**.

Vulnerability Management: Ledidi has implemented steps within the change management process to test for security vulnerabilities that could impact operations of the Ledidi services offering **(4.4)**. Should errors or vulnerabilities be identified during the testing, the change would be held until resolved.

Penetration Testing: Ledidi bi-annually has a third-party application penetration test performed and issues identified during the test are remediated, as needed **(4.5)**.

Control Activities

Control activities are the specific functions performed by Ledidi management and employees to address the individual risks associated with the achievement of the Company's objectives. Properly functioning control activities support company operations and can be objectively viewed and independently tested. Control activities can take the form of automated and/or manual controls and function in a combination of systems and business processes.

Ledidi's appointed Compliance Officer, Data Protection Officer, and HIPAA Security Officer oversee the compliance program for the Company. Part of this oversight includes the establishment of policies and procedures to manage and direct company activity and to allow for periodic assessments of adherence to the policies and procedures **(5.1)**. In addition to developing policies and procedures, Ledidi's management also segregates responsibilities and duties across the organization to mitigate risks to the services provided to its clients and to the Ledidi platform **(5.2)**.

Ledidi has established a compliance program for management and monitoring of key practices and control points with key components of compliance, HIPAA, and security **(5.3)**. The compliance program includes monitoring of key activity and tracking of activity through a non-conformity register **(5.4)**. Meetings are held to review identified company activities, current status, and remediation activities **(5.5)**. Results of these compliance activities are presented at company management meetings **(5.6)**. Action is taken to address concerns as considered necessary as well as updates and additions made to the compliance program.

Logical and Physical Access

Ledidi System Access and Authorization Control Policy: Ledidi employees and contractors have limited access to Ledidi systems and applications. Access is provisioned on a minimum-necessary (least-privilege) basis. Ledidi's system access procedures document the requirements for registering and authorizing employees and contractors prior to being issued system credentials and granted the ability to access the system **(6.1)**.

Employee Access to Ledidi Systems: Access to Ledidi systems and third-party accounts owned by Ledidi are only granted on a need-to-use basis, as defined by the responsibilities of the position held and the duties of the position. Access control and management is divided into multiple phases of the account life cycle, which include creation, privilege management, account audit, revocation – role changes and termination, authentication, guest access, disciplinary action, and responsibility.

Authorization – Role Based Access Control: Ledidi employees and contractors are granted access to Ledidi systems according to their role and/or team **(6.2)**. The executive team and team managers are jointly responsible for maintaining a list of roles and associated access scope for team members. The COO is the owner of the onboarding process, and the Compliance Officer is responsible for adherence to the procedure.

User Provisioning and Deprovisioning: Ledidi has implemented role-based security to limit and control access within Ledidi's production environment. Access is provisioned by the security officer based on notification received from the CEO authorizing such access **(6.3)**. Access approval is based on the role and responsibilities of the user, and a policy of least privilege. The individual requesting access cannot approve their own access. In addition, Ledidi employees and contractors must accept the Company's acceptable use policy upon being hired **(6.4)**. When an employee or contractor is terminated, the Security team revokes production access upon termination **(6.5)**.

Complementary User Entity Controls: *User entities are responsible for provisioning and deprovisioning user access to authorized individuals according to the principle of least privilege.*

Account Audit: On a semi-annual basis, the system owners conduct a user appropriateness review of access to Ledidi resources to validate internal user access is commensurate with job responsibilities **(6.6)**. This review is performed as part of the overall company risk assessment activities.

Complementary User Entity Controls: *User entities are responsible for periodically reviewing user access and access permissions to determine whether access is limited to appropriate personnel.*

Complementary User Entity Controls: *User entities are responsible for configuring strong password complexity requirements when using their own authentication method into the Ledidi environment.*

Complementary User Entity Controls: *User entities are responsible for configuring multifactor authentication when using their own authentication method into the Ledidi environment.*

Administrator and Remote Access: Administrator-level access privileges to the production environment are restricted to only those individuals who require such access to perform their respective job functions **(6.7)**. Access is limited to certain individuals who require the ability to add, delete, and modify users' access to the production system.

Passwords: Ledidi has developed a password policy to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change. Password parameters to production systems enforce standards for minimum length and complexity **(6.8)**. Remote access to the production infrastructure is limited to authorized individuals and communications are encrypted **(6.9)**.

Access to Client Data: Client data is stored within Ledidi's production database instance. Access to client data within the Ledidi production database by Ledidi employees is restricted to authorized users **(6.10)**. In addition, client users have access to their data only and no other clients' data **(6.11)**.

Encryption of Client Data: Ledidi understands the sensitivity of its clients' data and has therefore implemented security controls to protect the confidentiality of the data. Client data within Ledidi's production databases is encrypted **(6.12)**.

Infrastructure Authentication: Multifactor authentication is required for access to the production environment **(6.13)**.

Workstation Use and Security: The Company's policies and procedures provide guidance to its personnel concerning the physical safeguarding of workstations with access to the IT environment **(6.14)**. The guidance applies to devices such as a Windows or MacBook laptop, tablet, or other electronic devices (e.g., fixed workstation, portable workstation/laptop computer, tablet computer, smartphone, etc.) and to locations such as office, home, public place, etc. The guidance also includes access to physical and logical information and data subject to HIPAA requirements. User workstations are required to be encrypted, maintain current patching and operating systems, have antimalware software installed, and configured to automatically lock after five minutes of inactivity **(6.15)**. Ledidi manages server infrastructure through a combination of AWS managed services and automated life cycle management. The workloads run on AWS ECS Fargate and AWS Lambda, which are fully managed, serverless platforms. AWS manages the patching and OS maintenance.

Physical Access to Facilities and Information: Ledidi is headquartered in Oslo, Norway, and has a physical office located in the Oslo Science Park. Oslo Science Park manages access to the facility and the Ledidi office via keycard access. Only authorized Ledidi personnel have a keycard to the Ledidi office **(6.16)**. A personal pin code, in addition to the keycard, is required to enter the facility after business hours. All infrastructure, including that which contains client data and/or electronic PHI (ePHI), is housed entirely within subservice provider AWS' environment. Physical and environmental security of the Ledidi production environment are the responsibility of AWS and are covered by their SOC 2 report **(6.17)**. The majority of Ledidi's workforce works remotely. Physical security controls are deemed not applicable for Ledidi as client data and/or ePHI is housed entirely within AWS.

Ledidi's acceptable use policy, which all new hires must review and acknowledge, provides the requirements for handling documents, physical media, and storage devices along with the information classification and handling scheme **(6.18)**. The policy describes the handling of physical documents, including storing such documents in locked cabinets/drawers when not needed or outside of work hours. The policy also states that documents containing health and personal data shall not be printed. Ledidi operates on a clear desk, clear screen policy.

Virtual Private Cloud: Virtual private cloud (VPC) rules are configured to block unauthorized traffic into the network **(6.19)**. Access to modify VPC rules is restricted to authorized individuals **(6.20)**.

Transmission Encryption: All data transfers between users and the Ledidi system are secured using TLS and industry standard encryption **(6.21)**.

Removable Media: Ledidi has taken measures to restrict the usage of removable media to help mitigate both the risk of data loss as well as the risk of malware being introduced onto Ledidi systems. The use of portable devices or removable media is governed by the acceptable use policy **(6.22)**.

Hardware and Data Disposal: Ledidi's acceptable use policy describes the configuration requirements for Ledidi managed and BYOD (bring your own device) devices and the deletion and cleansing or destruction of devices when no longer used for Ledidi purposes **(6.23)**. Ledidi's data retention and deletion procedure defines specific requirements for the retention and disposal of the different types of data Ledidi may possess including PHI **(6.24)**. The data retention is broken into type of data and purpose of such data. This includes employee information, company information, business agreements and supporting documentation, customer content, and data that has been prepared and shared with a data subject.

System Operations

Incident Response Program: Ledidi has a documented incident procedure which establishes the procedures to be undertaken in response to information security incidents **(7.1)**. The incident procedure has been communicated to appropriate personnel and includes the following:

- Definition of an event
- Roles and responsibilities
- Steps to analyze, document, and remediate the identified incident
- Incident severity identification and classification
- Communications protocols
- A retrospective analysis to determine the root cause and implement incident response enhancements

The incident procedure is updated annually, and more frequently based upon incident outcomes and lessons learned, as appropriate **(7.2)**.

Incident Monitoring and Recordkeeping: Ledidi maintains a record of security incidents **(7.3)**. The incident records include a description of the incident and relevant facts (e.g., information that was disclosed), mitigations, risk assessment, and outcomes.

Notification in the Case of Breach: Ledidi's policies and procedures related to breach notification are consistent with the HIPAA Breach Notification Rule. In the event of a breach, Ledidi is required to notify each client affected by the breach **(7.4)**. Business associate agreements with service providers and contractors obligates such organizations to report breaches, if any, to Ledidi in a timely manner **(7.5)**. The data processing agreements Ledidi holds with data controllers requires Ledidi to notify the data controller of any potential personal data breaches **(7.6)**.

Complementary User Entity Controls: *User entities are responsible for assessing whether significant harm occurred in a breach and bear the burden of demonstrating through recordkeeping that all required notifications were made, if warranted, within timing constraints and without unreasonable delay.*

Workstation Antivirus and Patching: The Company's policies and procedures provide guidance to its personnel concerning the physical safeguarding of workstations with access to the IT environment and

information relevant to HIPAA requirements for both company managed and BYOD devices **(7.7)**. The guidance applies to devices such as Windows or MacBook laptops, tablets, or other electronic devices (e.g., fixed workstation, portable workstation/laptop computer, tablet computer, smartphone, etc.) and to locations such as office, home, public place, etc. The guidance also includes access to physical and logical information and data subject to HIPAA requirements. User workstations are required to maintain current patching and operating systems and have antimalware software installed **(7.8)**.

Monitoring of Servers: Ledidi subscribes to AWS' automatic server maintenance and patching service where AWS provides notice to its subscribers of maintenance actions needing to be performed. AWS will automatically perform the described maintenance activity after a defined period of time.

Backups: Ledidi has documented a backup policy that describes how often service and client data are backed up **(7.9)**. All original customer data on Ledidi's infrastructure must be backed up. Database backups are automatically performed hourly and daily, depending upon the data **(7.10)**. Backups are stored within AWS. A backup of the Ledidi database is restored at least annually so that restore operations are executed smoothly, if needed **(7.11)**.

Disaster Recovery Policy: Ledidi has created a business continuity plan to define the organization's procedures to recover IT infrastructure and IT services in the case of an outage or other disruptive incident **(7.12)**.

The following goals have been established for the plan:

1. **High availability:** Provide for the capability and processes so that a business has access to applications regardless of local failures.
2. **Continuous operations:** Safeguard the ability to keep things running during a disruption, as well as during planned outages such as scheduled backups or planned maintenance.
3. **Disaster recovery:** Establish a way to recover a data center at a different site if a disaster destroys the primary site or otherwise renders it inoperable.

Detailed steps and contacts are defined in the plan to provide direction regarding steps to take in the case of a disaster. Ledidi performs a test of the business continuity plan on an annual basis **(7.13).** Various scenarios are tested to determine Ledidi's ability to address each scenario.

Change Management

An effective system development and maintenance process is critical to the availability and integrity of Ledidi's system. The Ledidi platform is a proprietary and in-house developed system where custom changes are often necessary to enhance system functionality. Ledidi follows a defined development operating procedure for making changes to the system used to support the services provided to its clients **(8.1)**. Ledidi's development operating procedure describes how changes to the Ledidi system are proposed, reviewed, deployed, and managed. The change management procedure covers all changes made to the Ledidi software, regardless of their size, scope, or potential impact.

A request for a change can come internally from management or Ledidi personnel or externally from clients. A project management tool is used to prioritize, assign the task to team members, and track which changes are authorized for development **(8.2)**. Once assigned, an engineer develops the change and then oversees any needed testing or peer reviews. Engineering uses a software development platform to manage and record activities related to the change management process **(8.3)**. The tool enforces version control and is used to document control points within the change management process. Engineers work on the changes in the development environment. Ledidi maintains separate development, test, and production environments internally **(8.4)**. Part of the change management process involves automated code testing, which includes code security vulnerability checks. Automated testing is run for each change taking place with any errors needing to be remediated prior to moving the change to the next stage of the cycle **(8.5)**.

Once a change is ready for deployment to production, the assigned engineer submits the change's pull request for review, testing, and approval to release the change to production **(8.6)**. Branch protection rules have been configured to require review and approval of the change in order to be released to production **(8.7)**. The quality assurance team has multiple recurring weekly checkpoints to review open items, bug lists, and approve changes for release **(8.8)**.

Authorization to Implement Changes: Ledidi restricts the ability to implement changes into the production environment to only those individuals who require the ability to implement changes as part of their job function **(8.9)**.

Communication of Changes: Changes and enhancements impacting the functionality of the Ledidi software are communicated internally to employees and externally to system users as necessary **(8.10)**.

Risk Mitigation

New Suppliers: Ledidi has a supplier management procedure document that is followed for onboarding new suppliers **(9.1)**. Any suppliers that are key to Ledidi services are required to be reviewed to validate conformance of established information security requirements. An inventory of suppliers is maintained that includes the services provided and general compliance information **(9.2)**.

Supplier Risk Assessments: Ledidi understands that risks exist when engaging in business relationships and as a result, considers those risks that could potentially affect Ledidi's ability to meet its internal and external business objectives. See the preceding *Risk Assessment* section for additional information on Ledidi's risk assessment process.

Subservice Providers Monitoring: Ledidi uses a number of suppliers to assist with Ledidi's business needs including security and infrastructure through the services these suppliers provide. Ledidi completes an annual review of key suppliers that includes obtaining and reviewing the supplier's SOC examination **(9.3)**. Ledidi documents the results of the review and includes the review of the complementary subservice organization controls included in the supplier SOC reports **(9.4)**.

Complementary Subservice Organization Controls (CSOC)

Ledidi's controls related to the Ledidi services cover only a portion of the overall system of internal control for each user entity of Ledidi. It is not feasible for the applicable trust services criteria related to the Ledidi services to be achieved solely by Ledidi. Therefore, each user entity's internal controls must be evaluated in conjunction with Ledidi's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations, described as follows:

	AWS Complementary Subservice Organization Controls	**Related Control Criteria**
1.	The subservice organization is responsible for providing the physical security controls protecting the production servers from unauthorized access.	CC6.4-CC6.5
2.	The subservice organization is responsible for providing the environmental controls protecting the production servers.	CC7.2-CC7.5
3.	The subservice organization is responsible for maintaining the availability of the hosted environments 24/7/365.	CC7.2-CC7.5
4.	The subservice organization is responsible for managing and resolving incidents and problems reported by Ledidi in a timely manner.	CC7.2-CC7.5

(The remainder of this page is left blank intentionally.)

Complementary User Entity Controls (CUEC)

Ledidi's controls related to its Ledidi services cover only a portion of the overall system of internal control for each user entity of Ledidi. It is not feasible for the applicable trust services criteria related to the Ledidi services to be achieved solely by Ledidi. Therefore, each user entity's internal controls should be evaluated in conjunction with Ledidi's controls, and the related tests and results described in Section IV of this report, taking into account the related complementary user entity controls identified under each control area, where applicable.

This section highlights additional control activities that Ledidi believes should be considered and/or present at each user entity. Each user entity must evaluate its own system of internal control to determine if the following controls are in place. User auditors should consider whether the following controls have been placed in operation at user organizations:

	Complementary User Entity Controls	**Related Control Criteria**
1.	User entities are responsible for executing any required contractual obligations per their regional regulations and/or requirements.	CC2.3
2.	User entities are responsible for provisioning and deprovisioning user access to authorized individuals according to the principle of least privilege.	CC6.2-CC6.3
3.	User entities are responsible for periodically reviewing user access and access permissions to determine whether access is limited to appropriate personnel.	CC6.3
4.	User entities are responsible for configuring strong password complexity requirements when using their own authentication method into the Ledidi environment.	CC6.6
5.	User entities are responsible for configuring multifactor authentication when using their own authentication method into the Ledidi environment.	CC6.6
6.	User entities are responsible for assessing whether significant harm occurred in a breach and bear the burden of demonstrating through recordkeeping that all required notifications were made, if warranted, within timing constraints and without unreasonable delay.	CC7.2-CC7.4

(The remainder of this page is left blank intentionally.)

Section IV – Independent Service Auditor's Description of Tests of Controls and Results

Purpose and Objective of the Independent Auditor's Examination

This report on controls placed in operation and tests of the suitability of the design and operating effectiveness is intended to provide users of the report with information sufficient to obtain an understanding of those aspects of Ledidi's controls that may be relevant to user entities' internal controls. This report, when coupled with an understanding of the internal controls in place at each user entity, is intended to assist in the assessment of the total internal control surrounding Ledidi's services.

Our examination was limited to those controls performed by Ledidi. It is each user entity's responsibility to evaluate this information in relation to the internal controls in place at each user entity to obtain an overall understanding of the internal controls and assess control risk. The portion of controls provided by each user entity and Ledidi must be evaluated together. If effective control activities are not in place at the user entity, Ledidi's controls may not compensate for such weaknesses.

Our examination included inquiries of appropriate management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and tests of controls surrounding Ledidi's services. Our tests of controls were performed for the period of May 1, 2025 to April 30, 2026 and were applied to those controls relating to the applicable trust services criteria.

The description of controls is the responsibility of Ledidi's management. Our responsibility is to express an opinion that the controls are suitably designed and operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the applicable trust services criteria, specified by the AICPA, were achieved for the period of May 1, 2025 to April 30, 2026.

Any exceptions noted by Linford & Company LLP regarding the suitability of the design or operating effectiveness of the controls identified related to the applicable control criteria or the level of compliance with the controls are presented in this section under the caption, "Results of Testing." Concerns identified herein are not necessarily weaknesses in the total system of internal control at Ledidi as this determination can only be made after consideration of controls in place at each client. Complementary user entity controls that should be exercised by clients in order to complement the controls of Ledidi to attain the stated criteria are presented in Section III when considered applicable.

Overview of the Internal Control Environment

Entity-Level Controls

Our examination considered the control environment and included inquiry of appropriate management and staff, inspection of documents and records, and observation of activities and operations. Our examination of the tests of design and operational effectiveness was for the period of May 1, 2025 to April 30, 2026 and was applied to those controls relating to the applicable trust services criteria.

The control environment represents the collective effect of various elements in establishing, enhancing, or mitigating the effectiveness of specified controls. In addition to our review of the controls placed into operation, our procedures included tests of the relevant elements of Ledidi's control environment, including Ledidi's organizational structure and management control methods.

Our evaluation of the control environment included the following procedures, to the extent necessary:

- ✓ *Inspected* Ledidi's organizational structure and noted the segregation of functional responsibilities, personnel policies, and other policies and procedures.
- ✓ *Inquired* through discussion with management personnel responsible for developing, monitoring, and enforcing controls.
- ✓ *Observed* personnel in the performance of their assigned duties.

No exceptions were noted in entity-level testing.

* * * * *

The results of these procedures were considered in planning the nature, timing, and extent of evaluation procedures around the suitability of the design and operating effectiveness of controls.

Controls Specified by Ledidi, Testing Procedures, and Results of Tests

The following tables include a description of the control activities, testing procedures performed, and results of tests. Ledidi management specified the control activities and the AICPA specified the related control criteria in *Section V – Trust Services Criteria*.

Control Activities Relevant to the Security Criteria

Control Environment

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
1.1	A board of directors, consisting of internal and external individuals, exercises oversight of Ledidi's strategic direction, operational performance, and internal control.	*Inspected* the board of directors listing and meeting minutes and noted that the board of directors included both internal and external members. *Inspected* a sample of board meeting minutes and noted that the board met at least quarterly to discuss items related to Ledidi.	No exceptions noted. No exceptions noted.
1.2	The executive management team meets on a weekly basis.	For a sample of management meetings, *inspected* the meeting invitations and minutes and noted that the meetings occurred weekly and included members of executive management.	No exceptions noted.
1.3	Ledidi's LICS applies to all full-time, part-time, and contractor staff and includes the following sections: goals and annual plan, security, code of conduct, disciplinary process, and reporting violations.	*Inspected* Ledidi's code of conduct and noted that it included expected employee and contractor behaviors as noted within the control.	No exceptions noted.

Control Environment (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
1.4	Ledidi has established an internal compliance function and supporting tools which monitor the Ledidi control environment and alerts management when internal control and security issues arise.	*Inspected* an audit report and noted that an audit was performed on Ledidi's internal control environment. *Inspected* the internal monitoring tools and noted that management used the tools to alert when security issues arose.	No exceptions noted. No exceptions noted.
1.5	Ledidi's organizational structure defines authorities across the Company to facilitate information flow and establish responsibilities.	*Inspected* Ledidi's organizational structure and noted that it defined responsibilities and lines of authority throughout the organization.	No exceptions noted.
1.6	To increase the operational effectiveness of employees within this structure, every position has a job description so that individuals understand their responsibilities.	For a sample of job titles, *inspected* the documented job descriptions for the positions and noted that they reflected the employee's responsibilities.	No exceptions noted.
1.7	The HIPAA Security Officer is responsible for the security of Ledidi's systems.	*Inspected* the HIPAA Security Officer's job description and noted that the role of Security Officer had been assigned and was responsible for the security of Ledidi's systems.	No exceptions noted.
1.8	Applicants for full-time employment at Ledidi are required to complete a successful reference check as part of the terms of their employment.	For a sample of individuals hired during the period, *inspected* the onboarding checklists and noted that a reference check was completed for each new hire.	No exceptions noted.

Control Environment (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
1.9	As part of the hiring process, applicants are required to sign an employee contract that contains a confidentiality agreement.	For a sample of individuals hired during the period, *observed* the offer letter and confidentiality agreements and noted that both documents were signed by the new hires prior to the individuals' start dates.	No exceptions noted.
1.10	An onboarding checklist is completed to monitor completion of employment documentation and acknowledgment of Ledidi's LICS and assigned policies.	For a sample of individuals hired during the period, *inspected* the policy acknowledgements and noted that each new hire acknowledged the required policies and procedures as part of onboarding.	No exceptions noted.
1.11	New hires are required to complete Ledidi security awareness training and HIPAA training and sign the HES Declaration at the start of their position.	For a sample of individuals hired during the period, *inspected* training logs and noted that the new hires completed security awareness and HIPAA training as part of onboarding.	No exceptions noted.
1.12	Employee performance and feedback reviews are performed at least annually.	For a sample of employees, *inspected* performance review documentation and noted that a performance review was performed within the past year for each individual.	No exceptions noted.

Information and Communication

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
2.1	Ledidi maintains policies to communicate security and privacy responsibilities to Ledidi personnel.	*Inspected* the Ledidi internal privacy and acceptable use policy and noted that Ledidi communicated security and privacy responsibilities to Ledidi personnel.	No exceptions noted.
2.2	Ledidi uses an internal communication tool to distribute policies and periodic security reminders to employees including responsibilities related to security.	*Inspected* Ledidi's internal communication tool and noted that it was used to distribute policies. *Inspected* security communication to employees and noted that security reminders were conducted.	No exceptions noted. No exceptions noted.
2.3	Ledidi management provides annual security awareness training and HIPAA training for all employees that covers information security, data protection, and confidentiality of client information.	*Inspected* training materials and noted that Ledidi provided security awareness training, privacy, and HIPAA training on an annual basis covering information security, data protection, and confidentiality. *Inspected* the security awareness training and HIPAA training records for a sample of employees and noted that the employee completed the trainings within the past year.	No exceptions noted. No exceptions noted.

Information and Communication (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
2.4	Ledidi has created a high-level overview of the Ledidi system used to describe the services provided to the clients that Ledidi serves.	*Inspected* the Ledidi product and IT-architecture information on the Ledidi website and noted that a high-level overview of the Ledidi system was available to clients that Ledidi serves.	No exceptions noted.
2.5	Ledidi and its clients' responsibilities and commitments regarding the acceptable use of the Ledidi system and PHI, as applicable, are included within the Ledidi Enterprise Agreement and Terms of Service, which clients must agree to before using the Ledidi software.	*Inspected* the Ledidi Enterprise Agreement and Terms of Service and noted that they included Ledidi's clients' responsibilities and commitments regarding the acceptable use of the Ledidi system and PHI.	No exceptions noted.
2.6	For any service provider handling PHI on behalf of Ledidi, a BAA is also required to be executed.	For the only service provider handling PHI, *inspected* the BAA and noted that it provided the terms for the business associate and covered entity regarding the handling of PHI of the covered entity by the business associate.	No exceptions noted.
2.7	Ledidi has provided methods to clients and employees to report failures, incidents, concerns, or other complaints related to the services or systems provided by Ledidi in the event there are problems.	*Inspected* the Ledidi services and noted that methods were provided to clients to report issues and other concerns to the Company. *Inspected* internal policies and noted that employees were provided with information on how to report failures, incidents, concerns, or other complaints.	No exceptions noted. No exceptions noted.

Risk Assessment

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
3.1	Ledidi's risk assessment procedure describes the processes Ledidi has in place to identify new business and technical risks and how to achieve the desired level of risk.	*Inspected* the risk assessment procedure and noted that Ledidi had a process in place to identify and mitigate new business and technical risks.	No exceptions noted.
3.2	The policy is made available to all employees through the Company's policy repository.	*Inspected* the policy repository on the internal compliance portal and noted that Ledidi's risk assessment procedure was available to employees on the compliance management portal.	No exceptions noted.
3.3	Annually, the risks identified are formally documented in a risk assessment matrix.	*Inspected* the risk assessment matrix and noted that the risk assessment documented identified risk scenarios.	No exceptions noted.
3.4	Risk owners work with the Compliance Officer in the development of a risk treatment plan per risk assessment performed and the risk assessment is reviewed by Ledidi management.	*Inspected* the risk assessment matrix and noted that the risk identification and treatment plan were the joint responsibility of the Compliance Officer and department heads for the respective areas covered.	No exceptions noted.
3.5	The supplier management procedures provide a framework for managing the life cycle of supplier relationships.	*Inspected* the supplier management policy and noted that it provided guidance for managing the life cycle of supplier relationships.	No exceptions noted.

Risk Assessment (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
3.6	Ledidi has considered the potential for fraud when assessing risks to the achievement of objectives.	Through *inquiries* of Ledidi management, determined that the potential for fraud was addressed through internal processes implemented within the organization.	No exceptions noted.
3.7	Ledidi's risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.	Through *inquiries* of Ledidi management, noted that Ledidi considered changes to the regulatory, economic, and physical environment in which the entity operates.	No exceptions noted.

Monitoring Activities

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
4.1	Ledidi uses monitoring tools to monitor application health and the monitoring tool alerts system administrators when the application is not operating within defined boundaries.	*Inspected* the monitoring tools and noted that Ledidi monitored application health and that the monitoring tools sent alerts when the application was not operating within defined boundaries.	No exceptions noted.
4.2	Ledidi logs authentication, availability, and error events and uses tools for infrastructure monitoring.	*Inspected* monitoring tools and noted that Ledidi monitored the infrastructure as well as logged authentication, availability, and error events.	No exceptions noted.
4.3	The client-submitted tickets are addressed by Ledidi personnel.	*Inspected* a sample ticket submitted by a client and noted that the ticket described the issue identified by the client and the steps taken by Ledidi personnel to address the issue.	No exceptions noted.
4.4	Ledidi has implemented steps within the change management process to test for security vulnerabilities that could impact operations of the Ledidi services offering.	For a sample change during the period, *inspected* the change request documentation and noted that the change was automatically tested and was successfully completed prior to the change being deployed to production.	No exceptions noted.
4.5	Ledidi annually has a third-party application penetration test performed and issues identified during the test are remediated, as needed.	*Inspected* the penetration test results and noted that the test was performed during the audit period and identified vulnerabilities were reviewed and addressed as appropriate by Ledidi's management.	No exceptions noted.

Control Activities

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
5.1	Part of this oversight includes the establishment of policies and procedures to manage and direct company activity and to allow for periodic assessments of adherence to the policies and procedures.	*Inspected* the policies and procedures and noted that they provided direction regarding performance of activities including security and privacy.	No exceptions noted.
5.2	Ledidi's management also segregates responsibilities and duties across the organization to mitigate risks to the services provided to its clients and to the Ledidi platform.	*Inspected* the Ledidi organizational chart, system configurations, and role assignments and determined that responsibilities and duties were segregated within the organization and within the Ledidi environment.	No exceptions noted.
5.3	Ledidi has established a compliance program for management and monitoring of key practices and control points with key components of compliance, HIPAA, and security.	*Inspected* the internal compliance program and noted that management maintained the program and reviewed control activities. *Inspected* compliance reporting of activity performed during the audit period and noted that it detailed the different compliance activities performed as well as outcomes of these activities.	No exceptions noted. No exceptions noted.
5.4	The compliance program includes monitoring of key activity and tracking of activity through a non-conformity register.	*Inspected* the non-conformity register and a sample report for an item listed on the non-conformity register and noted that reported items were tracked through completion.	No exceptions noted.

Control Activities (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
5.5	Meetings are held to review identified company activities, current status, and remediation activities.	*Inspected* invitations for meetings held to discuss product and development activity and noted that meetings were held regularly with relevant team members to address the topics under the responsibility of the meeting attendees.	No exceptions noted.
5.6	Results of these compliance activities are presented at company management meetings.	*Inspected* a sample management review report and noted that it detailed status of risk assessment activities including non-conformity activities.	No exceptions noted.

Logical and Physical Access

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
6.1	Ledidi's system access procedures document the requirements for registering and authorizing employees and contractors prior to being issued system credentials and granted the ability to access the system.	*Inspected* Ledidi's system access procedures and noted that the procedures specified requirements for registering and authorizing employees prior to being issued system credentials and granted the ability to access the system.	No exceptions noted.
6.2	Ledidi employees and contractors are granted access to Ledidi systems according to their role and/or team.	*Inspected* Ledidi's onboarding process document and noted that it specified that new hires were only granted access to systems according to their role and/or team. Through *inspection* of the access breakdown matrix, noted that users were assigned authorities based on their type of role and/or team.	No exceptions noted. No exceptions noted.
6.3	Access is provisioned by the security officer based on notification received from the CEO authorizing such access.	For all employees hired during the period, *inspected* the emails authorizing access and the onboarding checklists and determined that access was authorized and actions taken were documented.	No exceptions noted.
6.4	In addition, Ledidi employees and contractors must accept the Company's acceptable use policy upon being hired.	For a sample of individuals hired during the period, *inspected* policy acknowledgments within the internal compliance tool and noted that the new hires accepted the acceptable use policy.	No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
6.5	When an employee or contractor is terminated, the Security team revokes production access upon termination.	For a sample of personnel terminated during the period, *inspected* offboarding documentation and lists of system access and noted that system access was revoked within three business days of the termination dates.	No exceptions noted.
6.6	On a semi-annual basis, the system owners conduct a user appropriateness review of access to Ledidi resources to validate internal user access is commensurate with job responsibilities.	*Inspected* the management review reports and noted that the security performance reviews were conducted during the period including identification and remediation of any non-conformities.	No exceptions noted.
6.7	Administrator-level access privileges to the production environment are restricted to only those individuals who require such access to perform their respective job functions.	For all users with administrator access to the production infrastructure, *inspected* the HR organization chart and noted that access appeared appropriate to the users' job functions and the individuals were a current employee or contractor. For all users with administrator access to the production infrastructure, *inquired* of Ledidi's management and noted that access was authorized and was appropriate to the users' job functions.	No exceptions noted. No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
6.8	Password parameters to production systems enforce standards for minimum length and complexity.	*Inspected* the password policy and noted that password protection requirements were documented and defined for Ledidi production systems. *Inspected* password configurations for production systems and noted that strong password settings were enforced.	No exceptions noted. No exceptions noted.
6.9	Remote access to the production infrastructure is limited to authorized individuals and communications are encrypted.	*Inspected* the system configuration and noted that SSH using RSA and a private key was required to log directly onto a server.	No exceptions noted.
6.10	Access to client data within the Ledidi production database by Ledidi employees is restricted to authorized users.	For all users with access to client data, *inspected* the HR organization chart and noted that access appeared appropriate to each user's job functions, and the individuals were current employees or contractors. For all users with administrator access to the production infrastructure, *inquired* of Ledidi's management and noted that access was authorized and appropriate to the users' job function.	No exceptions noted. No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
6.11	In addition, client users have access to their data only and no other clients' data.	*Observed* a technical demonstration of the Ledidi services and noted that Ledidi clients may not access other clients' data.	No exceptions noted.
6.12	Client data within Ledidi's production databases is encrypted.	*Inspected* database configurations and noted that client data within Ledidi's production databases was encrypted.	No exceptions noted.
6.13	Multifactor authentication is required for access to the production environment.	*Inspected* system configurations and noted that multifactor authentication was required for access to the infrastructure.	No exceptions noted.
6.14	The Company's policies and procedures provide guidance to its personnel concerning the physical safeguarding of workstations with access to the IT environment.	*Inspected* Ledidi's acceptable use policy and noted that it specified measures to physically safeguard access to workstations.	No exceptions noted.
6.15	User workstations are required to be encrypted, maintain current patching and operating systems, have antimalware software installed, and configured to automatically lock after five minutes of inactivity.	For a sample of employees, *inspected* their workstations' configurations and determined that the workstations had encryption enabled, were on a supported operating system level, had antimalware installed, and were configured to automatically lock after five minutes of inactivity.	No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
6.16	Only authorized Ledidi personnel have a keycard to the Ledidi office.	For a sample of individuals defined in the building physical access listing, *inspected* the Ledidi personnel listing and noted that access was appropriate for the sampled individuals. For a sample of individuals terminated during the period, *inspected* the physical access listing to the Ledidi office and noted that active keycards were not issued to these individuals.	No exceptions noted. No exceptions noted.
6.17	Physical and environmental security of the Ledidi production environment are the responsibility of AWS and are covered by their SOC 2 report.	*Inspected* the annual vendor review that Ledidi completed for AWS and noted that the subservice organization had been monitored during the examination period and that Ledidi documented the review of the AWS SOC report.	No exceptions noted.
6.18	Ledidi's acceptable use policy, which all new hires must review and acknowledge, provides the requirements for handling documents, physical media, and storage devices along with the information classification and handling scheme.	*Inspected* the acceptable use policy and noted that it provided the requirements for handling documents, physical media, and storage devices along with the information classification and handling scheme.	No exceptions noted.
6.19	VPC rules are configured to block unauthorized traffic into the network.	*Inspected* the VPC rules and noted that they were configured to block unauthorized internet traffic.	No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
6.20	Access to modify VPC rules is restricted to authorized individuals.	For all users with access to modify VPC rules, *inspected* the employee listing and noted that access was commensurate with the users' job functions. For all users with access to modify VPC rules, *inquired* of Ledidi's management and determined that the users' access was authorized and appropriate.	No exceptions noted. No exceptions noted.
6.21	All data transfers between users and the Ledidi system are secured using TLS and industry standard encryption.	*Inspected* website security settings and noted that data transfers between users and the Ledidi system used TLS and industry standard encryption.	No exceptions noted.
6.22	The use of portable devices or removable media is governed by the acceptable use policy.	*Inspected* the acceptable use policy and noted that the usage of portable devices or removable media was allowed in accordance with the information classification and handling scheme, which provides the classification level of data handled by Ledidi and the level of protection to be provided for each data classification.	No exceptions noted.
6.23	Ledidi's acceptable use policy describes the configuration requirements for Ledidi managed and BYOD devices and the deletion and cleansing or destruction of devices when no longer used for Ledidi purposes.	*Inspected* the acceptable use policy and noted that it addressed the configuration requirements of Ledidi managed and BYOD devices and the deletion and cleansing or destruction of devices when no longer used for Ledidi purposes.	No exceptions noted.

Logical and Physical Access (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
6.24	Ledidi's data retention and deletion procedure defines specific requirements for the retention and disposal of the different types of data Ledidi may possess including PHI.	*Inspected* the data retention and deletion procedure and noted that client data was required to be deleted within one week of the deletion request.	No exceptions noted.

System Operations

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
7.1	Ledidi has a documented incident procedure which establishes the procedures to be undertaken in response to information security incidents.	*Inspected* the incident procedure and noted that it detailed procedures for incident response in the event of a security incident.	No exceptions noted.
7.2	The incident procedure is updated annually, and more frequently based upon incident outcomes and lessons learned, as appropriate.	*Inspected* the incident procedure and noted that it was updated and approved within the last year.	No exceptions noted.
7.3	Ledidi maintains a record of security incidents.	For a sample of security incidents during the period, *inspected* Ledidi's incident tracking documentation and noted that Ledidi maintained records of the security incidents and followed the incident through to resolution. Noted, through *inquiries* of management, that there were no incidents during the period that required usage of the incident procedure.	No exceptions noted. No exceptions noted.
7.4	In the event of a breach, Ledidi is required to notify each client affected by the breach.	*Inspected* Ledidi's incident and communication procedures and noted that they included requirements to notify affected clients. *Inquired* of management and noted that no ePHI breaches occurred during the exam period.	No exceptions noted. No exceptions noted.

System Operations (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
7.5	Business associate agreements with service providers and contractors obligates such organizations to report breaches, if any, to Ledidi in a timely manner.	*Inspected* the business associate agreement for applicable service providers and noted that they obligated the service provider to report breaches to Ledidi in a timely manner.	No exceptions noted.
7.6	The data processing agreements Ledidi holds with data controllers requires Ledidi to notify the data controller of any potential personal data breaches.	*Inspected* the data processing agreement and noted that it required Ledidi to notify the controller of a personal data breach notification affecting the controller's personal data.	No exceptions noted.
7.7	The Company's policies and procedures provide guidance to its personnel concerning the physical safeguarding of workstations with access to the IT environment and information relevant to HIPAA requirements for both company managed and BYOD devices.	*Inspected* Ledidi's acceptable use policy and noted that it specified measures to physically safeguard access to workstations.	No exceptions noted.
7.8	User workstations are required to maintain current patching and operating systems and have antimalware software installed.	For a sample of employees, *inspected* workstation configurations and determined that the workstations were on supported operating system levels and had antimalware software installed.	No exceptions noted.
7.9	Ledidi has documented a backup policy that describes how often service and client data are backed up.	*Inspected* the backup policy and noted that the frequency for backups had been documented.	No exceptions noted.

System Operations (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
7.10	Database backups are automatically performed hourly and daily, depending upon the data.	*Inspected* backup configurations and backup logs and noted that daily backups were scheduled and performed within the cloud infrastructure.	No exceptions noted.
7.11	A backup of the Ledidi database is restored at least annually so that restore operations are executed smoothly, if needed.	*Inspected* the Ledidi database and noted that the database backup was successfully restored during the audit period.	No exceptions noted.
7.12	Ledidi has created a business continuity plan to define the organization's procedures to recover IT infrastructure and IT services in the case of an outage or other disruptive incident.	*Inspected* Ledidi's business continuity plan and noted that it addressed its plan for recovering from outages or disruption of services.	No exceptions noted.
7.13	Ledidi performs a test of the business continuity plan on an annual basis.	I*nspected* business continuity exercises performed during the period and noted that the exercises tested various scenarios that could occur at Ledidi to determine Ledidi's ability to address such scenarios should they arise.	No exceptions noted.

Change Management

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
8.1	Ledidi follows a defined development operating procedure for making changes to the system used to support the services provided to its clients.	*Inspected* the documented development operating procedure and noted that Ledidi followed a defined development process for making changes to the system.	No exceptions noted.
8.2	A project management tool is used to prioritize, assign the task to team members, and track which changes are authorized for development.	*Inspected* documentation from the project management tool and noted that Ledidi used the tool to prioritize, assign tasks, and track changes to Ledidi systems.	No exceptions noted.
8.3	Engineering uses a software development platform to manage and record activities related to the change management process.	For a sample of changes during the period, *inspected* the change request documentation and noted that Ledidi used a development tool to manage and record the activities related to the change management process.	No exceptions noted.
8.4	Ledidi maintains separate development, test, and production environments internally.	*Inspected* the environments at Ledidi and noted that there were separate environments for development, testing, and production for implementing changes.	No exceptions noted.
8.5	Automated testing is run for each change taking place with any errors needing to be remediated prior to moving the change to the next stage of the cycle.	For a sample of changes during the period, *inspected* the change request documentation and noted that each change was automatically tested and successfully completed prior to the change being deployed to production.	No exceptions noted.

Change Management (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
8.6	Once a change is ready for deployment to production, the assigned engineer submits the change's pull request for review, testing, and approval to release the change to production.	For a sample of changes, *inspected* the change request documentation and noted that the changes were reviewed, approved, and tested prior to being deployed to production.	No exceptions noted.
8.7	Branch protection rules have been configured to require review and approval of the change in order to be released to production.	*Inspected* the branch protection rules and noted that the rules were configured to require a review and approval prior to merging the change into the master branch.	No exceptions noted.
8.8	The quality assurance team has multiple recurring weekly checkpoints to review open items, bug lists, and approve changes for release.	*Inspected* the recurring meeting invitations for the quality assurance team and noted that multiple milestones were scheduled weekly to review and approve changes to the production environment prior to release.	No exceptions noted.

Change Management (continued)

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
8.9	Ledidi restricts the ability to implement changes into the production environment to only those individuals who require the ability to implement changes as part of their job function.	For all users with the ability to implement changes into the production environment, *inspected* the employee information and noted that each individual was a current employee and access appeared appropriate based on the job role. For all users with the ability to implement changes into the production environment, *inquired* of management and noted that each individual was a current employee, and access was authorized and appropriate based on the job role. *Inspected* branch protection rules and noted that rules were in place requiring changes to be approved prior to production deployment.	No exceptions noted. No exceptions noted. No exceptions noted.
8.10	Changes and enhancements impacting the functionality of the Ledidi software are communicated internally to employees and externally to system users as necessary.	*Inspected* sample internal and external communications and noted that they provided information on changes and enhancements to the Ledidi platform.	No exceptions noted.

Risk Mitigation

Ref	Controls Specified by Ledidi	Testing Performed by Linford & Company	Results of Testing
9.1	Ledidi has a supplier management procedure document that is followed for onboarding new suppliers.	*Inspected* the supplier management procedure and associated process document for onboarding of new suppliers and noted that a risk assessment and compliance checks were performed as part of the supplier onboarding process.	No exceptions noted.
9.2	An inventory of suppliers is maintained that includes the services provided and general compliance information.	*Inspected* the documented supplier inventory and noted that Ledidi maintains an inventory of suppliers that provide infrastructure and security services.	No exceptions noted.
9.3	Ledidi completes an annual review of key suppliers that includes obtaining and reviewing the supplier's SOC examination.	*Inspected* the documented review of a key supplier's SOC report and noted that Ledidi completed a review of the SOC report, including review of the complementary user entity controls defined in the report.	No exceptions noted.
9.4	Ledidi documents the results of the review and includes the review of the complementary subservice organization controls included in the supplier SOC reports.	*Inspected* the documented review of a key supplier's SOC report and noted that Ledidi monitored the complementary user entity controls included in the vendor's SOC report during the period.	No exceptions noted.

Section V – Trust Services Criteria

The Ledidi management team is responsible for establishing and maintaining effective controls over its Ledidi services. The controls are designed to provide reasonable assurance to Ledidi management and the board of directors that the following SOC 2 security criteria were achieved.

In the table that follows, the columns have the following meaning:

SOC 2 Criteria – This column contains, for each criterion evaluated, the reference citation. Each criterion sources from a requirement of the trust services criteria.

Requirement(s) – This column contains the text of the criterion (requirement) directly from the trust services criteria.

Reference – This column contains the reference to the control activities in *Section III – Ledidi's Description of Its Ledidi Services,* which are relevant to the achievement of the criterion.

The purpose of this table is to demonstrate that all SOC 2 control criteria in scope were assessed and that the control activities described in *Section III – Ledidi's Description of Its Ledidi Services,* address the SOC 2 control criteria.

Many of the criteria used to evaluate a system are shared amongst all of the criteria. For example, the criteria related to risk management apply to the security, availability, processing integrity, confidentiality, and privacy criteria. As a result, the criteria for the security criteria are organized into the criteria that are applicable to all five criteria (common criteria). The common criteria (CC1.0 through CC9.0 in the tables that follow) constitute the complete set of criteria for the security criteria.

Common/Security Criteria

Security. Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives.

Security refers to the protection of:

i. information during its collection or creation, use, processing, transmission, and storage and
ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft, or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CC1.0 Common Criteria Related to Control Environment

SOC 2 Criteria	Requirement(s)	Reference
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	1.1-1.3
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	1.1-1.2
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	1.1-1.2, 1.4-1.6

CC1.0 Common Criteria Related to Control Environment (continued)

SOC 2 Criteria	Requirement(s)	Reference
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	1.8-1.11
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	1.6, 1.12

CC2.0 Common Criteria Related to Information and Communication

SOC 2 Criteria	Requirement(s)	Reference
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	2.1-2.2, 2.5-2.7
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.	2.1-2.3, 2.7
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	2.5-2.7

CC3.0 Common Criteria Related to Risk Assessment

SOC 2 Criteria	Requirement(s)	Reference
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	3.1
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.	3.1-3.7
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	3.6
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	3.1-3.7

CC4.0 Common Criteria Related to Monitoring Activities

SOC 2 Criteria	Requirement(s)	Reference
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.	4.1-4.5
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.	4.1-4.5, 5.3-5.6

CC5.0 Common Criteria Related to Control Activities

SOC 2 Criteria	Requirement(s)	Reference
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.	5.1-5.6
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	5.1-5.3
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.	5.1-5.4

CC6.0 Common Criteria Related to Logical and Physical Access

SOC 2 Criteria	Requirement(s)	Reference
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.	6.1-6.24
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.	6.1-6.4

CC6.0 Common Criteria Related to Logical and Physical Access (continued)

SOC 2 Criteria	Requirement(s)	Reference
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.	6.1-6.5
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	6.16, AWS CSOC
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.	6.23-6.24, AWS CSOC
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	6.6-6.15
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.	6.7, 6.10
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.	4.1-4.5, 6.15, 7.1-7.3, 7.7-7.8

CC7.0 Common Criteria Related to System Operations

SOC 2 Criteria	Requirement(s)	Reference
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.	4.1-4.5, 7.1-7.3
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.	4.1-4.5, 7.1-7.13, AWS CSOC
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.	7.1-7.3, AWS CSOC
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.	7.1-7.3, AWS CSOC
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	7.1-7.6, AWS CSOC

CC8.0 Common Criteria Related to Change Management

SOC 2 Criteria	Requirement(s)	Reference
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.	8.1-8.10

CC9.0 Common Criteria Related to Risk Mitigation

SOC 2 Criteria	Requirement(s)	Reference
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	9.1-9.4
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	3.1-3.7, 9.1-9.4