ScalePad

SOC 3 Report

Program:

ScalePad Cloud SaaS Application Services

Period Covered

April 01, 2023 to March 31, 2024

Attest Report by

Accedere

Table of Contents

Executive Summary

Scope	ScalePad Cloud SaaS Application Services
Period Covered	April 01, 2023 to March 31, 2024
Applicable Trust Services Criteria	Security, Availability, and Confidentiality
Locations	3200-1021 W Hastings St Vancouver, BC V6E 0C3 Canada
Report Status	Unqualified

Section-I
Independent Service Auditor's Report

999, 18th Street, #3000
Denver, Colorado 80202
info@accedere.io
https://accedere.io

Independent Service Auditor's Report

To,
ScalePad Software Inc.
Locations: 3200-1021 W Hastings St Vancouver, BC V6E 0C3 Canada

Scope

We have examined ScalePad, accompanying its Description of Controls ("Description") for the effectiveness of controls for the period April 01, 2023, to March 31, 2024, specifically for its ScalePad Cloud SaaS Application Services and the suitability of the design of controls to meet the criteria for the principles outlined in Trust Services Criteria (TSC) 2017 for Security, Availability, and Confidentiality aspects as applicable and as stated in the Description. Since the scope of services is limited to ScalePad Cloud SaaS Application Services, processing integrity and privacy aspects have been scoped out. The Description may indicate that certain complementary user controls that may be suitably designed and implemented at the user level for related controls to be considered suitably designed to achieve the related criteria. We have not evaluated the suitability of the design or operating effectiveness of such complementary user controls and Sub-Service Organization Controls.

ScalePad offers ScalePad Cloud SaaS Application Services from the following Locations:

1. 3200-1021 W Hastings St Vancouver, BC V6E 0C3 Canada

ScalePad does not use any other sub-service organization that provides information or support to its ScalePad Cloud SaaS Application Services. Description includes only those criteria and related controls of ScalePad relating to their ScalePad Cloud SaaS Application Services.

ScalePad Responsibilities

ScalePad has provided the attached its Management Assertion "(Assertion") of ScalePad about the fairness of the presentation of the Description and suitability of the design of the controls to achieve the related TSC, for the criteria stated in the Description relating to its services. ScalePad is responsible for:

1. Preparing the Description and the Assertion;
2. The completeness, accuracy, and method of presentation of both the Description and Assertion;
3. Providing the services covered by the Description;
4. Specifying the controls that meet the applicable Trust Services Criteria and stating them in the Description; and
5. Designing, implementing, and documenting the controls to meet the applicable Trust Services Criteria.

ScalePad is also responsible for providing the details of ScalePad Cloud SaaS Application Services covered by the Description, specifying the TSC controls, identifying the risks that threaten the achievement of the TSC, selecting the criteria stated in the Assertion and designing, implementing, and documenting controls to achieve the related TSC controls for the criteria stated in the Description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on,

1. The fairness of the presentation of the Description is based on the description criteria outlined in the ScalePad Cloud SaaS Application Services.
2. Suitability of the design of the controls to meet the applicable Trust Services Criteria, based on our examination.

We conducted our examination under attestation standards SSAE 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 fairly presented based on the description criteria and the controls were suitably designed and operating effectively to achieve the related TSC stated in the Description, for the period April 01, 2023 to March 31, 2024.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the Description based on the Description criteria and the suitability of the design of those controls to meet the applicable Trust Services Criteria of Security, Availability, and Confidentiality only. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed to meet the applicable Trust Services Criteria. Our procedures also included evaluation of those controls that we consider necessary to provide reasonable assurance that the applicable Trust Services Criteria were met. Our examination also included evaluating the overall presentation of the Description. We believe that the evidence obtained is enough and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

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 and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable Trust Services Criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description or conclusions about the suitability of the design of the controls to meet the applicable Trust Services Criteria is subject to risks that the system may change or that controls at a service organization may become inadequate or fail. Cloud and cybersecurity risks are prevalent, malicious insiders or external third parties may be able to circumvent the controls at the service organization and may not be able to prevent such risks. Our examination or opinion does not cover such risks.

Opinion

In our opinion, in all material respects, based on the description criteria identified in the Assertion of ScalePad and the applicable Trust Services Criteria of Security, Availability, and Confidentiality:

1. The Description fairly presents the effectiveness of controls for the period April 01, 2023 to March 31, 2024.
2. The controls stated in the Description were examined for effectiveness to provide reasonable assurance that the applicable Trust Services Criteria would be met for the period April 01, 2023, to March 31, 2024.
3. The controls tested, if operating effectively, were those necessary to provide reasonable assurance that the applicable Trust Services Criteria were met, operated effectively throughout the period April 01, 2023 to March 31, 2024.

Restricted Use

This report and the Description of Controls are intended solely for the information and use of ScalePad, user entities, prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have enough knowledge and understanding of the following:

- The nature of the ScalePad Cloud SaaS Application Services provided by ScalePad.
- How the ScalePad's Cloud SaaS Application Services system interacts with user entities or other parties.
- Internal controls and its limitations.
- Complementary user-entity controls and how they interact with related controls at ScalePad to meet the applicable Trust Services Criteria.
- The applicable Trust Services Criteria.
- The risks that may threaten the achievement of the applicable Trust Services Criteria 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.

Accedere Inc.
Certified Public Accountants
CPA License No: FRM 5000337
Denver, Colorado, USA
Place of Issue: Denver, CO
Date: March 31, 2024

Stamp & Signature
Ashwin Chaudhary
MBA, CPA, CITP, CISSP, CISA, CISM, CRISC, CGEIT, CDPSE, CCSK, ISO 27001LA, PMP.
info@accedere.io
https://accedere.io

Section-II
Management Assertion

Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within ScalePad and for provision of ScalePad Cloud SaaS Application Services throughout the period April 01, 2023 to March 31, 2024, to provide reasonable assurance that ScalePad service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality Only (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria. Our description of the boundaries of the system is presented in Section-I, and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 01, 2023 to March 31, 2024, to provide reasonable assurance that ScalePad service commitments and system requirements were achieved based on the applicable trust services criteria. ScalePad, objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section-III.

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

We assert that the controls within the system were effective throughout the period April 01, 2023, to March 31, 2024, to provide reasonable assurance that ScalePad, Cloud SaaS Application Services commitments and system requirements were achieved based on the applicable trust services criteria.

For ScalePad

Sd/-

Name: Francois Deschamps
Designation: CFO
Date: March 31, 2024

Section III
Description of Controls (Description)
of the ScalePad Cloud SaaS Application Services

A. Overview of Operations

Description of the Boundaries of ScalePad, ScalePad Cloud SaaS Application Services

Services Provided

Background

- ScalePad as an organization has been providing SaaS solutions to MSP companies since 2015.
- We aim to create a harmonious experience between our MSP partners and their clients. With products at the core of your business, ScalePad continues to innovate the best apps in your stack as we look towards our vision of a future in harmony.

Overview of Service

- **Lifecycle Manager**
  - Lifecycle Manager makes complex data simple for both MSPs and their clients. LM equips MSPs with planning tools and automatically generates client-facing collateral that facilitates strategic conversations.
- **Backup Radar**
  - Backup Radar is a backup monitoring platform delivering automated oversight of virtually any backup environment. It surfaces gaps in any backup process by highlighting unreported backups, with intelligent ticketing automation that integrates seamlessly into an MSP's existing workflow.
- **ControlMap**
  - Enabling MSPs to build and manage a multi-tenant compliance program, ControlMap simplifies the compliance journey. With turnkey tools, automation, and templates, MSPs and their clients can achieve compliance in weeks instead of months.
- **Lifecycle Insights**
  - Lifecycle Insights makes it easy for vCIOs to deliver a best-in-class experience to their clients. Its templated assessments and budgeting tools help MSPs evaluate their clients' technology risk and manage action plans.

Cloud Organization

ScalePad Systems utilizes different cloud services:

- Amazon Web Services, AWS
- Microsoft Azure
- Google Cloud Platform, GCP

It is taking advantage of several key cloud services, including:

- managed Kubernetes services
- managed relational databases
- serverless functions
- S3 compliant storage
- data warehousing (DataBricks on AWS)
- fully managed app environments

The controls at AWS, Azure, and GCP are out of Scope for this report. Business continuity is ensured within each cloud (i.e. BCM environment for AWS is in AWS).

Boundaries of the System

The specific services included in the scope are development and maintenance of ScalePad products, establishing business processes in various departments, monitoring compliance, etc. supported from the remote and office locations at ScalePad.

All material activities and operations relating to ScalePad software development and operations are performed by ScalePad in Canada**.** No data is stored on the ScalePad office networks or stationary inside the office. The office(s) are to be considered a dedicated collaboration space and location for physical mail. All company operations are to be considered "remote". ScalePad DevOps teams manage the deployed solutions.

Geographic locations covered by the report include:

Office Location	Address
ScalePad Vancouver (main)	3200 - 1021 W Hastings St Vancouver, BC, V6E 0C3 Canada
ScalePad Montreal	104-1012 av du Mont-Royal Montreal, QC, H2J 1X6
ScalePad Markham	Unit 102 - 85 Enterprise Boulevard Unionville, ON, L6G 0B5

For the scope of the SOC2 audit, only one office (Vancouver) should be considered and only for the scope of providing a mailing address.

For all offices access to the building and maintenance are to be considered included in the lease.

The report excludes all processes and activities that are executed by others than ScalePad employees.

B. Principal Service Commitments and System Requirements

Product Team

Product & Customer Success teams are involved in the analysis of client requirements, coordinate with technical teams to propose the solution, obtain necessary approvals and confirmations from the client, and manage delivery.

ScalePad products are hosted in a SaaS environment on AWS setups. Only authorized DevOps personnel have access to the AWS cloud environment for ongoing operations and support of hosted systems being accessed by the customers. In scenarios, where a customer requests to host ScalePad products behind the customer's firewall, the customer would provide necessary access to their cloud environment. In such scenarios, ScalePad consultants take the remote connection to perform activities associated with operations and maintenance of live setups. The customers will access the setup as a service based on the access given to them, considering the deployment is multitenant. Any changes to the production environment are the responsibility of the ScalePad DevOps Team. There is no data stored locally in the ScalePad network.

The product team manages and includes sub-teams for software development, software support, software testing & quality control.

DevOps Team

This team has a primary responsibility to ensure:

- System availability & confidentiality requirements
- Incident management in ScalePad environment
- Change management/ patch management
- Network/ OS hardening
- Access Control
- VA/PT, Antivirus updates and control

People and Culture

P&C team governs the work environment and promotes ethics and integrity. The main responsibilities include,

- Recruitment
- Onboarding of employees
- Training
- Salary payments
- Background checks
- Severance on resignation or termination
- Performance evaluations including cases of non-performance
- Rewards and incentives
- Analyzing the cases of disgruntled employees and possibilities of fraud

Key infrastructure components include the following:

- **Cloud platform** – key AWS, GCP, and/or Azure services.
- **Internet** – Facilitate communication between the cloud infrastructure, customers, and employees.
- **Endpoint protection** – Detect and respond to treats, attacks and abnormal behavior.
- **Infrastructure, Development, Platform and Service Management Tools** - These tools are used to monitor services and facilitate operations.

Components of the System used to provide the Services

Cloud Platform

ScalePad Systems utilizes AWS, Microsoft Azure, and GCP, taking advantage of several key cloud services, including managed Kubernetes, DNS, S3 compliant storage, managed databases, etc. For the purposes of the SOC 2 Attestation, the controls at the sub-service organization are out of scope.

Boundaries of the System

The infrastructure comprises physical and virtual / cloud components.

Hardware components of a system

ScalePad office is equipped with the latest hardware, software, and networking infrastructure. The infrastructure comprises physical and hardware components of the System including facilities, equipment, software and networks located at ScalePad facilities consisting of. The office infrastructure does not play a role in or elevate any privileges for the purpose of supporting the system, therefore it is out of scope.

Test & Production Segregation

There exists a logically separate environment for Test and Production infrastructure. Developer access to the production environment is highly restricted.

Physical Infrastructure Overview

ScalePad's physical infrastructure is limited to employee workstations & mobile devices.

Software & Vendors

The list of the software and tools that are used to manage business requirements and control environment at ScalePad:

Name	Purpose
1Password	Password management
Alarm.com	Security monitoring of offices
Apple Push Notification Service	Dependency of JAMF MDM, allows to push changes to Apple devices
Asana	Task tracking, to-do lists
Atlassian (Jira, Confluence, StatusPage)	Agile work management, documentation and availability monitoring/communication platform
AWS	Cloud infrastructure provider
BambooHR	HR / people management tool
Buildkite	CI/CD service
Canada Post	Address verification, lookup and autocomplete service for Canada
ControlMap	Compliance management platform
DataBricks	Data warehouse and compute platform
DocuSign	Electronic signature platform
Gandi	Domain name management, registrar
Gitlab	Version control, development tooling
Google Workspace (GCP)	Cloud infrastructure provider
Grafana Cloud	Cloud monitoring and alerting

Name	Purpose
HubSpot	CRM tool
Jamf Cloud	Apple mobile device management tool
Microsoft (Azure)	Cloud infrastructure provider
Mondev	Landlord / office space provider
OOK	MSP, reseller for business related services
Proxy-N-VPN	Service providing proxy and VPN solutions
SendGrid	Email sending service
Sophos	Endpoint protection suite
Stripe	Payment provider
Zoom	Communication provider (meeting, collaboration, calling)

People

Executive Leadership

Business activities at ScalePad are under the direction of the Executive Leadership Team (ELT).

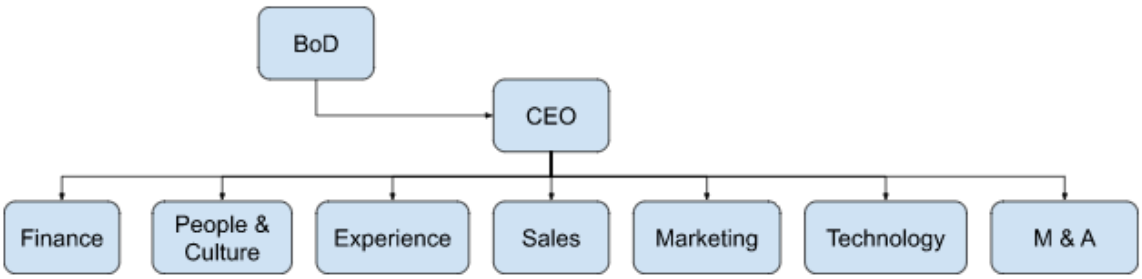
Management's Philosophy and Operating Style

At ScalePad we use the Entrepreneurial Operating System (EOS). EOS focuses on the six key components of every business: vision, people, data, issues, process, and traction.

- Getting everyone in the organization 100% on the same page with where your company is going and how you're going to get there.
- Getting the right people in the right seats.
- Using a handful of numbers that give everyone an exact pulse on where things are and when they are off track.
- Strengthening your organization's ability to identify issues, address them, and make them go away forever.

Organizational Structure

The organizational structure of ScalePad provides the overall framework for planning, directing, and controlling operations. It has segregated personnel and business functions into functional groups.



Procedures

New Hire Procedures

New employees are required to read ScalePad's corporate policies and procedures and sign an acknowledgment form stating that they have read and understood them.

Before hiring, candidates undergo background checks consisting of prior employer references, educational references, and a check for criminal offenses. Discrepancies noted in background investigations are documented and investigated by the People and Culture Department. All employees must sign an employment agreement with ScalePad containing a code of conduct, and commitments regarding security & confidentiality.

External consultants or third-party are evaluated before contracting. They are required to read and sign the contract and/or statement of work as well as an NDA before commencing the assignment with ScalePad.

Performance Evaluation

Employees performance reviews, promotion, and compensation adjustment are performed (at least) every 12 months. The performance evaluation is reviewed with the employee.

New Joiner Training

Once new employees join their teams, additional process training is imparted either on a one-on-one basis, through an online course(s) or in a classroom setting.

Employee Exit Procedure

When an employee leaves the organization, the People & Culture group initiates the 'Exit Process' and informs the other stakeholders/teams as well as communicates the last working day. The process is then tracked by People & Culture.

Change Management

All major changes must be initiated by appropriate personnel, analyzed for impact, tested, and approved before deployment. Change requests are always tracked and recorded.

Service Monitoring

The uptime of the ScalePad platform & service health is constantly monitored through various means. The vital parameters are monitored 24/7 by monitoring solutions. In case of abnormality, an alert is sent to ScalePad personnel.

Customer Onboarding

When a customer is signed up, they will self-onboard using the provided documentation. ScalePad will assist in case of issues or questions.

Product Development Lifecycle

ScalePad follows the Agile methodology for the product development lifecycle. The sprint cycle is generally two weeks. A quarterly and yearly product roadmap is defined by the management based on customer requirement and company vision.

Patch Management

The engineering division ensures that all patches to services, software and operating systems are well tested and deployed in a timely fashion. All the critical & security patches are applied on a priority basis.

Endpoint Protection

Endpoint protection solution has been deployed to servers, desktops, laptops, and other mobile devices within the scope of ScalePad. Definition updates for the solution are provided continuously.

Data

Data Backup and Restoration

ScalePad has developed formal policies and procedures relating to backup and recovery. ScalePad production applications & databases are backed automatically and configured to fulfill all requirements related to availability, integrity, and confidentiality. The backup process is monitored to ensure proper operation.

Business Continuity Process

ScalePad takes adequate measures to ensure business continuity even in adverse situations.

Data Security & Confidentiality

ScalePad applications are accessed via a web browser over the internet through HTTPS protocol using a TLS certificate adhering to the latest best practices.

Access to data is restricted to authorized uses only. All agreements with third parties and vendors include confidentiality commitments consistent with the company's policies.

Data is encrypted at rest where possible. Additionally, PII data is point encrypted in data processing applications.

ScalePad is committed to establishing, implementing, and improving an Information Security Management System. Information security Policy and supporting documents have been approved by the leadership team and provide guiding principles for information security implementation and operations across ScalePad.

At the ScalePad has exhibited its commitment by:

- Establishing ISMS scope and information security objectives.
- Providing sufficient resources for implementation and improvement of security systems and controls.
- Establishing and communicating the roles and responsibilities for the smooth operation of ISMS;

    a) Communicating to all the employees the importance of meeting information security objectives, conforming to the information security policy, and the need for continual improvement of the implemented ISMS;
    b) Conducting periodic reviews of the ISMS to ensure that gaps (if any) are identified, and remediation plans (if applicable) are in place;
    c) Establishing a framework to promote timely reporting of security events by identifying weaknesses, which might impact the organization’s ISMS or result in any disruptive incidents;
    d) Ensuring continual improvement of the security posture of ScalePad.

ScalePad management has determined the roles needed to establish, implement, operate, and maintain ISMS. Management has also provided the nominations for the identified roles as per the required competency. Responsibilities and authorities of the resources have been defined and documented.

The information security team determines the overall information security risk appetite. The risk appetite is periodically measured, monitored, and reviewed. The information security team meets at least once in a year to review information security status, and challenges, and drive information security initiatives. In the interim period, the ScalePad reviews the risks, with all the respective stakeholders.

Governance

At ScalePad governance is all about maintaining high availability, physical security, data security, occupational safety, and adherence to statutory guidelines. Doing so ScalePad strives to add value to the experience which all interested parties have with ScalePad. The Company has put in place an internal governance structure with defined roles and responsibilities of every constituent of the system.

Management is responsible for creating, maintaining, and monitoring the policies, standards, and procedures that constitute the internal controls. A fundamental component of this oversight is the information security steering committee, which includes business representatives, has quarterly agenda for reporting review risks and incidents with reasonable assurance of the integrity and reliability of the services being provided, protection of customer information and assets against unauthorized use and compliance with policies and statutory requirements.

Quantitative, replicable, and auditable KPIs have been defined with regular schedules of audit and management reviews. These KPIs are reported and reviewed at various levels periodically.

ScalePad goes through a series of internal and external audits and exhibits conformity to the following globally acclaimed standards.

- ISO/IEC 27001:2013, Information Security Management Standard.
- SSAE SOC2 Type 2 and SOC3 (System and Organization Controls).

ScalePad engages the respective physical security, information security, and audit teams to facilitate the smooth functioning of the audit, compliance, and governance activities in the organization.

Internal Communications

The ISMS program uses various mechanisms to communicate security requirements and expectations to the stakeholders. Assurance that the stakeholders are informed and understand the security policies and expectations is driven by:

- Acknowledgment of the ScalePad ethics code/security pledge.
- Training and assessment of the security policies and standards.

During onboarding and annually thereafter, ScalePad provides mandatory annual security awareness training.

Security communication is sent on an annual basis covering:

- Importance of adhering to the ScalePad information security policy.
- Organization's responsibilities under the applicable laws & regulations.
- The criticality of continual improvement.
- The latest version of the information systems policy & objectives.
- Link to ISMS policies and standards intranet page.
- Link to the ISMS roles and responsibilities document containing roles, responsibilities, and authorities.

External Communications

ScalePad has implemented various methods of external communication with all relevant stakeholders as required.

Supplier Management

ScalePad has a vendor risk management program to ensure that vendors have appropriate practices to ensure compliance with ScalePad information security policies. Vendors must sign a non-disclosure agreement. Suppliers enter into an agreement that covers supplier duties, service obligations, license, and intellectual property rights, confidentiality, integrity, and availability of their products and services. Supplier contracts include security requirements and service level agreements.

Suppliers are required to report information security events and breaches impacting ScalePad Cloud SaaS Application Services. Need-based reviews occur for all key suppliers. Reviews cover the handling of non-public information, and legal impacts, the security of the system, external certifications, as well as pertinent organizational structure changes if they will affect the supply and support reliability of the vendor.

Security Controls

ScalePad Cloud SaaS Application Services are protected by several layers of security technologies and processes.

Below are examples of controls:

- **Network access control –** The ScalePad Cloud SaaS Application Services network perimeter is protected by firewalls. Any network traffic entering or leaving the ScalePad Cloud SaaS Application Services is continuously monitored using an intrusion prevention system (IPS). The ScalePad network is also segmented into multiple security zones. Traffic between the zones is controlled by firewalls and access control lists (ACLs).

- **Infrastructure and management controls –** Every component of infrastructure, including network devices, application servers, OS, and databases, is hardened according to stringent security guidelines. It is also subject to regular scans to identify and address any security vulnerabilities.

- **Logical access control –** Access to systems is allowed only on a need-to-know basis.

- Employee and contractor access to these systems is also reviewed quarterly for compliance. Passwords are encrypted following ScalePad's encryption policy.

End of Document