System and Organization Controls (SOC) 2 Type II

Report on Management's Description of its

Highly Specialized CI/CD Services

And the Suitability of Design of Controls Relevant to the

Controls Placed in Operation and Test of Operating Effectiveness Relevant to the Security, Availability and Confidentiality Categories

For the Period
February 15, 2021 to May 15, 2021

Together with
Independent Service Auditors' Report

SPACELIFT

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITORS' REPORT

INDEPENDENT SERVICE AUDITORS' REPORT

To the Management of Spacelift, Inc. (Spacelift)

Scope

We have examined Spacelift's accompanying description of its Highly Specialized CI/CD Services titled "Description of Spacelift's Highly Specialized CI/CD Services" (description) throughout the period February 15, 2021 to May 15, 2021 (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* (AICPA, *Description Criteria*), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period February 15, 2021 to May 15, 2021, to provide reasonable assurance that Spacelift's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Spacelift uses subservice organizations to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Spacelift, to achieve Spacelift's service commitments and system requirements based on the applicable trust services criteria. The description presents Spacelift's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Spacelift's controls. Our examination did not include the services provided by the subservice organizations, 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 Spacelift, to achieve Spacelift's service commitments and system requirements based on the applicable trust services criteria. The description presents Spacelift's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Spacelift'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

Spacelift 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 Spacelift service commitments and system requirements were achieved. Spacelift has provided the accompanying assertion titled "Assertion of Spacelift Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Spacelift 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 Auditors' 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. 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.

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 the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or 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 listed in section IV.

Opinion

In our opinion, in all material respects,

a. the description presents Spacelift's Highly Specialized CI/CD Services that was designed and implemented throughout the period February 15, 2021 to May 15, 2021, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period February 15, 2021 to May 15, 2021, to provide reasonable assurance that Spacelift'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 Spacelift's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period February 15, 2021 to May 15, 2021, to provide reasonable assurance that Spacelift'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 Spacelift's controls operated effectively throughout that period.

Restricted Use

This report, including the description of test of controls and results thereof in section IV, is intended solely for the information and use of Spacelift, user entities of Spacelift's Highly Specialized CI/CD Services during some or all of the period February 15, 2021 to May 15, 2021, business partners of Spacelift subject to risks arising from interactions with the Highly Specialized CI/CD 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.

San Jose, California
June 16, 2021

II. ASSERTION OF SPACELIFT MANAGEMENT

ASSERTION OF SPACELIFT MANAGEMENT

We have prepared the accompanying description of Spacelift, Inc. (Spacelift) Highly Specialized CI/CD Services titled "Description of Spacelift's Highly Specialized CI/CD Services " throughout the period February 15, 2021 to May 15, 2021, (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* (AICPA, Description Criteria). The description is intended to provide report users with information about the highly specialized CI/CD Services that may be useful when assessing the risks arising from interactions with Spacelift's system, particularly information about system controls that Spacelift has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Spacelift uses subservice organizations to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Spacelift, to achieve Spacelift's service commitments and system requirements based on the applicable trust services criteria. The description presents Spacelift's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Spacelift's controls. The description does not disclose the actual controls at the subservice organizations.

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

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

a. the description presents Spacelift's Highly Specialized CI/CD Services that was designed and implemented throughout the period February 15, 2021 to May 15, 2021, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period February 15, 2021 to May 15, 2021, to provide reasonable assurance that Spacelift'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 Spacelift's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period February 15, 2021 to May 15, 2021, to provide reasonable assurance that Spacelift'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 Spacelift's controls operated effectively throughout that period.

Signed by Spacelift Management

June 16, 2021

III. DESCRIPTION OF **SPACELIFT'S HIGHLY SPECIALIZED CI/CD SERVICES**

DESCRIPTION OF SPACELIFT'S HIGHLY SPECIALIZED CI/CD SERVICES

Company Background

Spacelift, Inc. (Spacelift) is a Poland-born tech start-up that delivers the most flexible CI/CD for Terraform. Co-founded by Marcin Wyszynski and Pawel Hytry in 2020, the product enables collaborators to ship software reliably and more frequently via a "continuous integration and deployment" platform, giving back control and allowing teams to automate their workflows. Still in their early stages, they have attracted excitement and interest from a number of big investors.

The company was initially formed in February 2020 as a Polish entity, Spacelift.io sp. z o.o., with 4 shareholders: Marcin Wyszynski, Michal Piorkowski, Pawel Tymczyna, and Tomasz Kucharski. Approaching pre-seed round in April 2020, it was decided that Spacelift, Inc. would be formed in the US, with the same shareholder structure as Spacelift.io sp. z o.o. In May 2020, prior to pre-seed round, Spacelift, Inc. acquired 100% in Spacelift.io sp. z o.o. from all 4 initial shareholders. The $1.6M pre-seed round was completed in May 2020, with Hoxton Ventures and Inovo Venture Partners as the two lead investors. A number of angels also participated. In December 2020, Blossom Capital bought out common shares and converted them to preferred shares.

The Series A round was completed in December 2020, with participation from Blossom Capital as the lead investor. Hoxton Ventures and Inovo Venture Partners also participated in the round.

In March 2021 Inovo Venture Partners acquired all shares from one of the angels, STT Business Holding.

Services Provided

Spacelift is an integrated management platform for Infrastructure-as-Code, combining the functions of a highly specialized CI/CD tool with sophisticated state management and auditing features.

It enables collaboration, automates manual work and compliance, and lets teams customize and automate their workflows.

We focus on openness, flexibility, and customization and are aiming for power users. Our solution is built on top of well-known, well-loved open-source components like Docker and Open Policy Agent, so it allows full customization while maintaining sensible defaults.

Here's what is possible with Spacelift:

- Build sophisticated Git-based workflows
- Use Open Policy Agent to declare rules around your infrastructure, access control, state changes, and more
- Author and maintain reusable modules for your organization; we even have a full CI solution for modules to make sure they're healthy
- Declare who can log in (and under what circumstances) and what their level of access to each of the managed projects should be (SAML 2.0 SSO out of the box!) using login and access policies respectively

- Use Spacelift's trigger policies to create arbitrary workflows and dependencies spanning multiple Infrastructure-As-Code stacks
- Manage stacks, contexts, modules, and policies in a declarative way using Terraform or Pulumi

Principal Service Commitments and System Requirements

At Spacelift, customers' security is our first and foremost priority. We're aware of the utmost importance of security in our service and we're grateful for our customers' trust. Here's what we're doing to earn and maintain this trust:

Encryption -

All of our data is encrypted at rest and in transit. With the exception of intra-VPC traffic between the web server and the load balancer protected by a restrictive Amazon Web Services (AWS) security group, all other traffic is handled using secure transport protocols. All the data sources (S3, database, SNS topics and SQS queues) are encrypted at rest using AWS KMS keys with restricted and audited access.

Customer secrets are encrypted at rest in a way that should withstand even an internal attacker.

Responsible disclosure **-**

If customers discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask customers to help us better protect our clients and our systems.

We ask customers to do the following:

- E-mail the findings to security@spacelift.io;
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data;
- Do not reveal the problem to others until it has been resolved;
- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties, and;
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible.

What we promise:

- We will respond to your report within 3 business days with our evaluation of the report and an expected resolution date;
- If you have followed the instructions above, we will not take any legal action against you regarding the report;
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission;
- We will keep you informed of the progress towards resolving the problem;

- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise), and;
- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known to us. The amount of the reward will be determined based on the severity of the leak and the quality of the report.

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.

Components of the System

Infrastructure

We're fully cloud-based with all our infrastructure hosted by AWS. Where possible, we are using a serverless approach (ECS Fargate, Lambda). In a small number of isolated cases, we are running virtual machines (EC2) - t3.small in eu-west-1 region (Ireland). With regards to firewalls, we are using the software-based approach in the form of AWS VPC and security groups.

Software

Our software is primarily written in Go and distributed either as statically linked, compiled binaries for AMD64 Linux or as Docker containers. Running in AWS serverless environments we have no control over the operating system. In cases where we use virtual machines, we are running Amazon Linux 2 with Datadog, AWS and Vanta agents running for monitoring and auditing purposes.

People

12 people work for Spacelift:

2 founders:

- Marcin Wyszynski (CEO & CTO)
- Pawel Hytry (COO & CFO)

10 contractors:

- 6 Software engineers
- 1 Operations manager
- 1 Security engineer
- 1 Head of BI
- 1 HRBP

The company does not have any employees.

Data

The company processes personal data of its employees/contractors in very limited scope, it's mainly the personal data of employees (none at the moment) and contractors.

We use GitHub as an identity provider. To limit users' access, we depend on identity provider assertions (GitHub, SAML), which can optionally be processed by declarative access policies using Open Policy Agent.

For authenticating users, we depend on 3rd party identity providers. Customers may set up API keys for programmatic access. In those cases, the API key secret is only displayed once to the creator, and we store bcrypt hash in the database. We do not have out-of-band access to customer data or a management interface.

Data is stored in eu-west-1 Europe (Ireland). There's no physical access to the data center, we're fully on AWS. We use KMS encryption for all data at rest.

We do have policies for data deletion. It's a combination of DB deletion with backup expiration, and S3 deletion and expiration. We don't use any other storage mechanisms. We generally delete everything once the account is closed. One exception to that is the versioned data in S3 which after deletion is subject to 30-day expiry.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Spacelift policies and procedures that define how services should be delivered. These are located on the company's intranet and can be accessed by any Spacelift team member.

Physical Security

All data is hosted by AWS. AWS data centers do not allow Spacelift employees physical access. At present, all work is conducted remotely.

Logical Access

We use GitHub as an identity provider.

To limit users' access, we depend on identity provider assertions (GitHub, SAML, OIDC), which can optionally be processed by declarative access policies using Open Policy Agent. For authenticating users, we depend on 3rd party identity providers. Customers may set up API keys for programmatic access. In those cases, the API key secret is only displayed once to the creator, and we store bcrypt hash in the database.

We do not have out-of-band access to customer data or a management interface.

Computer Operations – Backups

We have a tiered backup system using AWS Backup, creating tiered daily, weekly and monthly backups stored for up to a year. Those backups are encrypted and copied to a dedicated AWS backup's account, to which only engineering leadership has access.

No customer data is stored on any of the employees' working stations. All of our tools are cloud-based.

Computer Operations – Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents.

Spacelift monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. Spacelift evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space, power and cooling
- Disk storage
- Tape storage
- Network bandwidth

Spacelift has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Spacelift system owners review proposed operating system patches to determine whether the patches are applied. Customers and Spacelift systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Spacelift staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

Spacelift's Change Management Policy describes how changes to the Spacelift system are proposed, reviewed, deployed, and managed. This policy covers all changes made to the Spacelift software, regardless of their size, scope, or potential impact.

This policy is designed to mitigate the risks of:

- Corrupted or destroyed information
- Degraded or disrupted computer performance
- Productivity losses
- Introduction of new vulnerabilities, configuration errors and software bugs in infrastructure and code

- Exposure to reputation risk

Version Control

All of our software is version controlled and synced between contributors (developers). Access to the central repository is restricted based on an employee's role.

Using a decentralized version control system allows multiple developers to work simultaneously on features, bug fixes, and new releases; it also allows each developer to work on their own local code branches in a local environment.

All code is written, tested, and saved in a local repository before being synced to the origin repository. Writing code locally decouples the developer from the production version of our code base and insulates us from accidental code changes that could affect our users. In addition, any changes involving the persistence layer (database) are performed locally when developing new code, where errors or bugs can be spotted before the change is deployed to users.

Production branch

The production branch reflects the current state of the application in production.

Staging branch

The default (main or master) branch reflects the current state of the application on the staging (preprod) server.

Feature branches

Feature branches are used to develop new features for a future release, the specifics of which might not be known when development starts. A given feature branch will exist as long as the feature is in development; the branch will eventually either be merged back into the default (main or master) branch, to add the new feature to an upcoming release with a pull request, or discarded (if the feature will not be added to an upcoming release).

Feature branches may branch off from and would normally merge back into the default (main or master) branch.

Security bugs

Spacelift recognizes that security bugs represent key issues that should be resolved quickly to maintain the security, confidentiality, privacy, processing integrity, and availability of the service. Spacelift commits to resolving security bugs within reasonable timelines as outlined by company procedural commitments in Vanta.

Hotfix branches

Hotfix branches are meant for new, unplanned production releases that address the live system being in an undesired state. A hotfix branch is made off of the production branch when a critical production bug must be resolved. This allows team members on the master branch to continue their work while someone else prepares the bug fix.

When finished, the bug fix needs to be merged back into the production branch, so it is deployed to production. The merge should be done through a pull request. The fix should also be merged into the current default (main or master) branch.

Hotfixes that are merged directly into production, without going through the default (main or master), are exceptions that should be used only when a critical bug in the production system needs to be addressed immediately.

Permission for a hotfix should be obtained from the engineering leadership and should be noted in the pull request.

Change Initiation

To initiate a change, the developer first creates a feature branch on their local machine. Code changes are grouped into diffs, each of which represents a proposed change to the codebase.

Pull Requests

When a developer finishes a feature branch, they make a pull request to merge those changes into master. This submits the changes for peer review. For all code changes, the reviewer should be different from the author.

Pull requests allow developers to describe the changes they're making; co-workers can review the set of changes in a code review. Pull requests also trigger automated testing and code-quality checks that must be completed and returned successfully before merging is allowed. Testing and approval are logged by the system.

A pull request's details section should be used to note any non-code changes (e.g. environment or database changes) needed before the commits are merged. Once tests pass and the code is approved, the author can merge the code to the default (main or master) branch.

Merging a Pull Request

Before merging a pull request, the developer should check that all prerequisites have been met, including environment changes or database migrations. Once non code changes have been implemented, the pull request can be merged.

If the application is deployed through our standard, zero-downtime automated deployment pipeline, the developer's job is complete.

If any of these changes necessitate system down-time, this needs to be treated as an exception, and communicated to the engineering leadership, and an explicit permission must be obtained. Any change that requires downtime must come with a risk assessment and detailed plan with steps to be taken during the downtime period, and the merge should take place within a scheduled and pre-announced window when customers are less likely to be affected.

Code Reviews, Change Review, and Change Approval

When the developer wants to merge a feature into the default (main or master) branch, a code review should be performed. Code reviews are performed by a second developer (i.e. not the one who wrote the code), who considers questions like:

- Are there any obvious logic errors in the code?
- Are all cases specified in the requirements fully implemented?
- Is there sufficient automated testing for the new code? Do existing automated tests need to be rewritten to account for code changes? Does the new code conform to existing style guidelines?
- Are there any egregious security errors as defined by the OWASP Top 10?

Initially a pull request should be marked as draft, and a code review should take place after all code has been written and automated tests have been run and passed, as this ensures the reviewers' time is spent checking what automation misses. The code review is requested by marking the pull request as ready for review, selecting the appropriate reviewers and communicating the need for review through one of the platforms used internally by the company (e.g. Slack).

The reviewer should note all potential issues with the code; it is the responsibility of the author(s) to address those issues or explain why they are not applicable.

Once the review process finishes, each reviewer should approve the pull request. Only when the pull request is accepted may the original author(s) merge their change into the release branch.

If reviewers are specified as a group (e.g. "backend") then an approval from a single member of that group is sufficient for a merge. In some cases, a member of the requested approvers' group may also approve the change but request an extra approval from another engineer. In that case, that approval becomes necessary for the merge.

Automated Testing

When a pull request is initiated, our automated test suite is triggered to run against the new code.

Deployment

The system is deployed automatically, and some basic health checks prevent the obviously broken code from taking the site down. In those cases, the previous version of the code remains deployed. Failed deployments are visible in the repository but do not trigger code changes.

Zero Downtime Deployment

Zero downtime deployments allow us to make changes without waiting for a change window and allow us to return the application to a previous state easily.

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Spacelift management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

The engineering leadership team is responsible for ensuring this policy is followed.

Data Communications

Data is encrypted in transit (SSL) and at rest (customer-managed AWS KMS keys + custom AES/RSA). All data processing occurs inside our AWS VPC with external traffic going through a NAT Gateway.

Redundancy: all our services are deployed in 3 separate availability zones in the eu-west-1 AWS region (Ireland).

Penetration testing

- Pen testing performed at least annually;
- Latest available report from Federacy;
- Test’s executive summary.

Spacelift engaged Federacy to perform a penetration test and vulnerability assessment. The objective of the penetration test was to verify that Spacelift's application and its supporting infrastructure are adequately protected with appropriate controls, based on industry standards and best practices. Vulnerabilities, flaws, and defects in the design or implementation of the application, system, and network were sought.

The following categories were covered:

- Authentication Session Management
- Access Control
- Validation, Serialization, and Encoding
- Data Protection
- Communication Security
- Application Integrity
- Business Logic
- File and Resource Handling
- API Security

- Configuration and Dependency Security

The target of the penetration test covered app.spacelift.dev. Two security researchers conducted this penetration test between February 26, 2021 and April 1, 2021 where testing was performed against a staging environment it was confirmed to be an environment that mirrored production, including code and infrastructure.

All significant vulnerabilities discovered were remediated by Spacelift, which was verified by Federacy.

Vulnerability scanning (pre-deploy and post-deploy)

- GitHub Dependabot for source code;
- Gosec for Go source code;
- CodeQL from GitHub for source code;
- Trivy vulnerability scanner for Docker image;
- AWS ECR built-in scanning for Docker images.
-

Boundaries of the System

The scope of this report includes the highly specialized CI/CD services performed by Spacelift.

This report does not include the data center hosting services provided by AWS.

The applicable trust services criteria and the related controls

Common Criteria (to the Security, Availability, and Confidentiality Categories)
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.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality
Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Spacelift's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Spacelift's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgement form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Spacelift's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

Spacelift's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility

Spacelift's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Spacelift's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Spacelift is an equal opportunity employer. We eagerly seek applicants of diverse backgrounds and hire without regard to race, color, gender identity, religion, national origin, ancestry, citizenship, physical abilities (or disabilities), age, sexual orientation, veteran status, or any other characteristic protected by law. Cultivating inclusivity and diversity is a top priority.

Spacelift's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Spacelift's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment Process

Risk Assessment & Management Program

Spacelift's Risk Assessment principles, policies, procedures and methodology describes what systems Spacelift has in place to identify new business and technical risks and how often those risks are mitigated.

Principles

Spacelift is proactive in its approach to risk management, balances the cost of managing risk with anticipated benefits, and undertakes contingency planning in the event that critical risks are realized. Spacelift has the primary duty to ensure the security, availability, and/or confidentiality of critical systems and customer data. A duty to ensure a secure, available infrastructure requires Spacelift to identify and manage risks. Spacelift believes that effective risk management involves:

1. A commitment to the security, availability, and/or confidentiality of Spacelift infrastructure and services from senior management; The involvement, cooperation and insight of all Spacelift staff;
2. A commitment to initiating risk assessments, starting with discovery and identification of risks;
3. A commitment to the thorough analysis of identified risks;
4. A commitment to a strategy for treatment of identified risks;
5. A commitment to communicate all identified risks to the company;
6. A commitment to encourage the reporting of risks and threat vectors from all Spacelift staff.

Spacelift believes that the following events can trigger a risk assessment to occur:

1. A significant and major change to existing infrastructure, product or business practices;
2. A significant amount of time (e.g. a year) having passed since the last risk assessment.

Risk assessments can be as high level or detailed to a specific organizational or technical change as Spacelift stakeholders and technologists see fit.

Risk assessments can be conducted by unbiased and qualified parties such as security consultancies or qualified internal staff.

Scope

This Risk Assessment & Management program and policy applies to all systems and data on the Spacelift network, owned by Spacelift or its customers, or operated on behalf of the organization. Risk assessments should evaluate infrastructure such as computer infrastructure containing networks, instances, databases, systems, storage, and services. Spacelift risk assessments will also include an analysis of business practices, procedures, and physical office spaces as needed. Risk assessments for vendors are covered under Spacelift's Vendor Management Program, which includes a thorough risk assessment targeted at a vendor's security, business practices, legal commitments and insurance postures.

Definitions

Risk

Risk is the probability that a harmful consequence may result when exposed to a hazard.

Risk is characterized and rated by considering two factors:

1. Probability or likelihood (L) of occurrence; and
2. Consequence (C) of occurrence.

This is expressed as R (risk) = L (likelihood) x C (consequence).

Threat

A potential incident or activity which may be deliberate, accidental, or caused by nature which may cause physical harm to a person or financial harm to an organization.

Likelihood

Likelihood is a qualitative description of probability or frequency. The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities). The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts).

Consequence

Consequence is the outcome of an event and is a loss, disadvantage, or gain. There are a range of possible outcomes associated with an event. Consequence and impact are used interchangeably. The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Risk Assessment

A risk assessment is the process of evaluating and comparing a level of risk against predetermined acceptable levels of risk. It is an examination of all possible risks along with implemented and non-implemented solutions to reduce, eliminate, or manage the risks.

Risk Management

Risk management is the application of a management program that addresses organizational and technical risk. This management program includes identification, analysis, treatment, and monitoring.

Risk Owner

A risk owner is the person responsible for managing an individual risk. The risk owner is typically the person directly responsible for the strategy, activity, or function that relates to that risk.

Risk Assessment & Management Policy

This risk assessment policy specifies how and when risk assessments will be done and who will be responsible for conducting risk assessments and implementing solutions to address any risk assessment findings.

It is the responsibility of all Spacelift staff to identify, analyze, evaluate, monitor, and communicate risks associated with any activity, technology, function, or process within their relevant scope of responsibility and authority. Staff identifying potential risks or vulnerabilities are to report them to internal staff and/or external parties.

Overall, the execution, development, and implementation of risk assessments and remediation programs is the joint responsibility of Spacelift's engineering leadership and the department or individuals responsible for the surface area being assessed. All staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff are further expected to work with the risk assessment project lead in the development of a remediation plan for each risk assessment performed.

- Spacelift performs at least one risk assessment, at a minimum, every year using qualified internal staff and/or external parties who have experience performing risk assessments.
- A risk assessment should be done or reviewed on critical systems and applications no less than every two years.

- Risk assessments may be used to assess all risks to the organization.
- All staff involved with a risk assessment must fully cooperate with the risk assessment project lead in conducting the assessment and developing a remediation strategy.
- Any staff members or external consultants who perform any Spacelift risk assessments are required to be familiar with computer technology and computer security in particular. The risk assessment project leader should be the security officer, or a staff member designated by the security officer to conduct the risk assessment.
- Risk assessment deliverables include a risk assessment report with a risk reduction action plan to manage or mitigate any unacceptable risks. The action plan may be included with the risk assessment report, or separately. The action plan will be a plan for implementing additional controls and solutions to mitigate or manage the risk. The action plan may define participants and actions to be taken during the implementation of the action plan.
- The risk assessment process and methodology will be updated as required due to results of audits and incidents.
- All identified vulnerabilities will be assessed for impact and criticality. Vulnerabilities must be remediated as soon as possible as mandated by the Spacelift Vulnerability and Patch Management Program.

Risk Assessment Process

Spacelift risk assessment methodology is based off NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments.

- Management defines the scope of risk assessment and creates the risk assessment team with a point person to guide the process (risk assessment project lead).
- If risk assessment procedures are not defined, the team should define them. The proper time and method of communicating the selected risk treatment options to the affected IT and business management should be included.
- Evaluate the system - Determine if the system is critical to the organization's business processes and determine the data classification and security needs of the data on the system according to the Spacelift Data Classification Policy, considering security, availability, and/or confidentiality needs.
- List the threats - List possible threat sources such as an exploitation of a vulnerability.
- Identify vulnerabilities.
- Evaluate potential security controls already in place to assess if they adequately address the risk.
- Identify probability of exploitation. Additional security controls may need to be in place before the probability of exploitation is lowered.
- Quantify damage (impact) - Categorize the damage and possibly place a dollar amount on the damage where possible. This will help when looking at cost of controls to reduce the risk.
- Determine risk level - Use likelihood times impact to quantify the amount of risk.
- Evaluate and recommend controls to reduce or eliminate risk - Identify existing controls and those that may further reduce probabilities or mitigate specific vulnerabilities. List specific threats and vulnerabilities for the system to help identify mitigating controls.

- Create the risk assessment report.
- Communicate the selected risk treatment options to the affected IT and business management and staff.
- Take recommended risk mitigation actions. Record such actions as changes per the Spacelift Change Management program.
- Monitor the effectiveness of the risk mitigation actions and document the results.

Risk Mitigation Standards

Acceptable Risks

When the probability of threat materialization times maximum damage amount is less than $1,000 annually, the risk is acceptable. For higher amounts, on a yearly basis, acceptance of the risk will depend on the cost of implementing measures to reduce the risk. If the risk cannot be reduced and the amount per year is greater than $50,000, the risk should be transferred by purchasing insurance.

Risk Mitigation

Options for mitigating risk shall include the following possibilities:

- Reducing the chance of an occurrence of an event
- Reducing the damage due to occurrence
- Avoiding the risk
- Transferring the risk by taking an action such as purchasing insurance

Some guidelines and standards applicable to Spacelift:

- Costs of implementing each control are considered and compared to the benefits, pecuniary and non-pecuniary, of implementing each control.
- Cost and benefit analysis is done to evaluate proposed controls versus risks. When the controls are evaluated, the benefits, costs, and cost savings of applying the controls both individually and in combination should be determined. Performance measures for determining the effectiveness of the new controls are created.
- Risks shall be ranked, and controls are selected, and a plan created to implement the controls. Responsibilities for implementing the controls are determined and communicated. Budgeting and schedules are set and the expected outcomes from mitigating the risks with the controls are documented. Residual risk after full implementation is considered.
- Decisions regarding residual risk are made. Specifically, whether to accept the risk, transfer the risk, or take other action, including adding additional controls.
- Safeguard options for addressing high risk scenarios must be considered and utilized appropriately while the extent of risk reduction and benefits are considered. Cost and benefit analysis is done to evaluate safeguard options.
- If the cost of safeguard options or recommended risk controls is greater than the available budget, the options and controls are prioritized to reduce as much risk as possible within the budget.

- When the risk assessment report is completed, results shall be communicated to the affected IT and business management and staff.

Non-Compliance

Since risk assessments are an important part of protecting data and systems for Spacelift, employees that purposely violate this policy may be subject to disciplinary action up to and including denial of access, legal penalties, and/or dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

Responsibility

The engineering leadership is responsible for communicating detected risks and remediation steps needed to the appropriate staff for resolution. Those staff members are then responsible for resolving detected risks in a timely manner, guided by the severity of the detected risk.

Information and Communications Systems

Information and communication is an integral component of Spacelift's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Spacelift, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Spacelift personnel via e-mail messages.

Specific information systems used to support Spacelift's system are described in the Services Provided section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Spacelift's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Spacelift's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Spacelift's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Spacelift's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

We've implemented the following technical and organizational security measures:

- SOC 2 examination for Security, Availability, and Confidentiality
- Limited access to information resources, including Multi-factor Authentication, password policies and approval process for permissions, led by the CTO organization.
- Role-based security to limit and control access for systems
- 3rd Party Penetration Testing
- Anti-Malware and vulnerability scanning for all endpoints
- Secure Data Transfer and Encryption at Rest
- Annual Privacy and Information Security Training

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Criteria Not Applicable to the System

All Common, Availability, and Confidentiality criteria were applicable to the Spacelift highly specialized CI/CD services.

Subservice Organizations

Spacelift's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all the Trust Services Criteria related to Spacelift's services to be solely achieved by Spacelift control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Spacelift.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met.

Subservice Organization – AWS		
Category	Criteria	Control
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.

Subservice Organization – AWS		
Category	Criteria	Control
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

Spacelift management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Spacelift performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Complementary User Entity Controls

Spacelift's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Spacelift's services to be solely achieved by Spacelift control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Spacelift's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Spacelift.
2. User entities are responsible for notifying Spacelift of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Spacelift services by their personnel.

5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Spacelift services.
6. User entities are responsible for providing Spacelift with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Spacelift of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

IV. DESCRIPTION OF CRITERIA, SPACELIFT CONTROLS, TESTS AND RESULTS OF TESTS

DESCRIPTION OF CRITERIA, SPACELIFT CONTROLS, TESTS AND RESULTS OF TESTS

Relevant trust services criteria and Spacelift related controls are an integral part of management's system description and are included in this section. Sensiba San Filippo LLP performed testing to determine if Spacelift's controls were suitably designed and operating effectively to achieve the specified criteria for the security, availability and confidentiality categories set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria)*, throughout the period February 15, 2021 to May 15, 2021.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of Spacelift activities and operations and inspection of Spacelift documents and records. The results of those tests were considered in the planning, the nature, timing and extent of Sensiba San Filippo LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all Spacelift controls, this test was not listed individually for every control in the tables below.

Trust Services Criteria for the Security Category	*Description of Spacelift Controls*	*Service Auditor Test of Controls*	*Result of Test of Controls*
Control Environment			
CC1.1 *The entity demonstrates a commitment to integrity and ethical values.*	CC1.1.1 Spacelift has established a Code of Conduct and requires all employees to agree to it. Management monitors employees' acceptance of the code.	Inspected the policy that documents the company's Code of Conduct to determine that it was in place and provides guidance on workforce conduct standards.	No exceptions noted
		Inspected the signed Code of Conduct for a sample of employees to determine that they had agreed to the company's Code of Conduct.	No exceptions noted
CC1.2 *The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.*	CC1.2.1 Spacelift demonstrates a commitment to integrity and ethical values by completing an annual review of ethical management and hiring practices.	Inspected management's statement of ethics to determine that Spacelift demonstrates a commitment to integrity and ethical values.	No exceptions noted
CC1.3 *Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.*	CC1.3.1 Company management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication and escalation. The organizational charts are made available to employees through the company's HR Information System to facilitate communication in their role with the company.	Inspected Spacelift's HR Information System to determine that organizational charts are accessible for employees.	No exceptions noted

Trust Services Criteria for the Security Category	*Description of Spacelift Controls*	*Service Auditor Test of Controls*	*Result of Test of Controls*
Control Environment			
CC1.4 *The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.*	CC1.4.1 All positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Spacelift.	Inspected a sample engineering job description from Spacelift.	No exceptions noted
		Inspected the signed offer letters for a sample of new hires to determine that new hires are required to sign a contract upon hire.	No exceptions noted
CC1.5 *The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.*	CC1.5.1 Spacelift has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the Company's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete these trainings annually.	Inspected the security awareness training completion for a sample of employees to determine that Spacelift has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the Company's security policies and procedures	No exceptions noted
	CC1.5.2 Management has approved Spacelift security policies, and all employees agree to these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected the signed security policies for a sample of employees to determine that all employees had agreed to the security policies.	No exceptions noted
Information and Communication			
CC2.1 *The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.*	CC2.1.1 Spacelift uses a SOC 2 compliance platform called Vanta which objectively and continuously monitors the Spacelift control environment and alerts management when internal control and security issues arise.	Inspected the Vanta tool configurations to determine that Spacelift uses a SOC 2 compliance platform called Vanta which objectively and continuously monitors the Spacelift control environment and alerts management when internal control and security issues arise	No exceptions noted
CC2.2 *The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.*	CC2.2.1 Spacelift has policies and procedures in place to establish acceptable use of information assets approved by management, posted on the company wiki, and accessible to all employees. All employees must agree to the Acceptable Use Policy on hire.	Inspected company records to determine that a policy that establishes the acceptable use of information assets is in place, has been approved by management, and is accessible to employees.	No exceptions noted

Trust Services Criteria for the Security Category	*Description of Spacelift Controls*	*Service Auditor Test of Controls*	*Result of Test of Controls*
Information and Communication			
		Inspected the signed Acceptable Use Policy for a sample of new hires to determine that they had agreed to the company's Acceptable Use Policy.	No exceptions noted
CC2.3 *The entity communicates with external parties regarding matters affecting the functioning of internal control.*	CC2.3.1 Spacelift maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	Inspected the Spacelift Privacy Policy to determine that it is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	No exceptions noted
	CC2.3.2 Spacelift maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems. Where the Terms of Service may not apply, the company has Client Agreements or Master Service Agreements in place.	Inspected the Spacelift Terms of Service to determine that it is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems.	No exceptions noted
Risk Assessment			
CC3.1 *The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.*	CC3.1.1 Spacelift's Risk Assessment and Management Program policy describes the processes Spacelift has in place to identify new business and technical risks and how frequently those risks are mitigated.	Inspected the risk management policy to determine that Spacelift has a formal program for identifying and managing risks.	No exceptions noted
CC3.2 *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.*	CC3.2.1 Spacelift maintains a risk register that continuously documents risks facing the company and in-progress remediation programs to address those risks.	Inspected the security risk assessment to determine that Spacelift maintains a risk register that continuously documents risks facing the company and in-progress remediation programs to address those risks.	No exceptions noted
CC3.3 *The entity considers the potential for fraud in assessing risks to the achievement of objectives.*	CC3.3.1 Spacelift identifies and performs forensics regarding potential fraud activity (e.g., fraudulent reporting, loss of assets, unauthorized acquisitions, etc.).	Inspected the risk report to determine that the entity identifies and performs forensics regarding potential fraud activity (e.g., fraudulent reporting, loss of assets, unauthorized acquisitions, etc.)	No exceptions noted

Trust Services Criteria for the Security Category	*Description of Spacelift Controls*	*Service Auditor Test of Controls*	*Result of Test of Controls*
Risk Assessment			
CC3.4 *The entity identifies and assesses changes that could significantly impact the system of internal control.*	CC3.4.1 Spacelift uses a SOC 2 compliance platform called Vanta which objectively and continuously monitors the Spacelift control environment and alerts management when internal control and security issues arise.	Inspected the Vanta tool configurations to determine that Spacelift uses a SOC 2 compliance platform called Vanta which objectively and continuously monitors the Spacelift control environment and alerts management when internal control and security issues arise.	No exceptions noted
Monitoring Activities			
CC4.1 *The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.*	CC4.1.1 Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inspected the monitoring dashboard to determine that monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted
CC4.2 *The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including management and executive leadership, as appropriate.*	CC4.2.1 Spacelift has an established incident response policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the Incident Response Plan to determine that it outlines formal procedure for responding to security events.	No exceptions noted
	CC4.2.2 Spacelift provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	Inspected the contact form to determine that Spacelift provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	No exceptions noted
Control Activities			
CC5.1 *The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.*	CC5.1.1 A list of Spacelift's system components is maintained for management's use.	Inspected the inventory listing of information assets the company maintains in order to protect inventory from security events, maintain data confidentiality, and ensure system availability.	No exceptions noted

Trust Services Criteria for the Security Category	*Description of Spacelift Controls*	*Service Auditor Test of Controls*	*Result of Test of Controls*
Control Activities			
CC5.2 *The entity also selects and develops general control activities over technology to support the achievement of objectives.*	CC5.2.1 Spacelift has implemented a vulnerability management program to detect and remediate system vulnerabilities in software packages used in company infrastructure.	Inspected the configuration for the tool that continuously monitors software packages and confirmed that it is active and alerts on vulnerabilities.	No exceptions noted
	CC5.2.2 Spacelift engages third-parties to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	Inspected the penetration test results to determine that Spacelift engages third-parties to conduct penetration tests of the production environment at least annually.	No exceptions noted
CC5.3 *The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.*	CC5.3.1. Management has approved Spacelift security policies, and all employees agree to these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected Spacelift's security policies to determine that they outline requirements for securing the company's operations, services, and systems.	No exceptions noted
		Inspected the security policy acknowledgement for a sample of new hires to determine that all employees agree to these procedures when hired.	No exceptions noted
Logical and Physical Access			
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.*	CC6.1.1 Access to corporate network, production machines, network devices, and support tools requires a unique ID.	Inspected the configuration for the company's infrastructure provider to determine that permissions are assigned to groups.	No exceptions noted
		Inspected the configuration for the company's infrastructure tool to determine that employees have unique accounts on the service.	No exceptions noted

Trust Services Criteria for the Security Category	*Description of Spacelift Controls*	*Service Auditor Test of Controls*	*Result of Test of Controls*
Logical and Physical Access			
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.*	CC6.2.1 Access to infrastructure and code review tools is granted to new employees within one week of their start date.	Inspected the employee access tracker for a sample new hire to determine that employee access to infrastructure is granted within one week of the initial request.	No exceptions noted
	CC6.2.2 Access to infrastructure and code review tools is removed as a component of the termination process.	Inspected the employee access tracker to determine that employee access to infrastructure is removed as a component of the termination process.	No exceptions noted
CC6.3 *The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.*	CC6.3.1 Access is restricted to authorized personnel. Access approval and modification to access list are logged. Access is removed when appropriate.	Inspected access lists for the infrastructure provider to determine that access is limited to authorized personnel and removed when appropriate.	No exceptions noted
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.*	CC6.4.1 Spacelift relies on AWS's physical and environmental controls, as defined and tested within the AWS SOC 2 reports.	Not Applicable - Control is Carved Out	The Criterion is carved out and the responsibility of the subservice organization (AWS).

Trust Services Criteria for the Security Category	*Description of Spacelift Controls*	*Service Auditor Test of Controls*	*Result of Test of Controls*
Logical and Physical Access			
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.*	CC6.5.1 Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	Inspected the Data Deletion Policy to determine that procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	No exceptions noted
CC6.6 *The entity implements logical access security measures to protect against threats from sources outside its system boundaries.*	CC6.6.1 Access to sensitive systems and applications requires two factor authentication in the form of user ID, one- time password (OTP) and/or certificate.	Inspected all user accounts with access to company infrastructure to determine that each is configured with multi-factor authentication (MFA).	No exceptions noted
	CC6.6.2 Management uses configurations that ensure only approved networking ports and protocols are implemented, including firewalls.	Inspected the virtual private cloud network configuration to determine that access control lists were used to filter unwanted network traffic.	No exceptions noted
CC6.7 *The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.*	CC6.7.1 Company management ensures that all company-issued laptop hard drives are encrypted using full disk encryption.	Inspected employee computers to determine that each was protected with full-disk encryption.	No exceptions noted
	CC6.7.2 Customer data stored in databases is encrypted at rest.	Inspected the database configurations to determine that data is encrypted at rest.	No exceptions noted
	CC6.7.3 Encryption is used to protect user authentication and administrator sessions of the internal admin tool transmitted over the Internet.	Inspected the encryption configurations to determine that all connections happen over SSL/TLS with a valid certificate from a reliable Certificate Authority.	No exceptions noted

Trust Services Criteria for the Security Category	Description of Spacelift Controls	Service Auditor Test of Controls	Result of Test of Controls
Logical and Physical Access			
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.*	CC6.8.1 Spacelift deploys malware detection software on all workstations that can access the production environment and has configured malware detection software to perform daily scans with immediate notification if malware is detected.	Inspected the antivirus configurations to determine that Spacelift deploys malware detection software on all workstations that can access the production environment and has configured malware detection software to perform daily scans with immediate notification if malware is detected.	No exceptions noted
System Operations			
CC7.1 *To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.*	CC7.1.1 Spacelift has established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking (e.g. "high," "medium," or "low") to newly discovered security vulnerabilities.	Inspected the vulnerability management tool to determine that Spacelift has established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking (e.g. "high," "medium," or "low") to newly discovered security vulnerabilities.	No exceptions noted
CC7.2 *The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.*	CC7.2.1 Spacelift uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system administrator.	Inspected the company's version control system and confirmed it is actively used.	No exceptions noted
		Inspected the users of the company's version control tool and confirmed that all accounts were authenticated to the company's account.	No exceptions noted

Trust Services Criteria for the Security Category	*Description of Spacelift Controls*	*Service Auditor Test of Controls*	*Result of Test of Controls*
System Operations			
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.*	CC7.3.1 Remediation of security deficiencies are tracked through internal tools.	Inspected the security incident ticket for a sample of incidents to determine that security issues are tagged and prioritized accordingly.	N/A – Non-Occurrence (No security incidents during the period)
	CC7.3.2 Security deficiencies tracked through internal tools are closed once remediated.	Inspected the security incident ticket for a sample of incidents to determine that security issues are resolved within Spacelift's specified time frame.	N/A – Non-Occurrence (No security incidents during the period)
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.*	CC7.4.1 Spacelift has an established incident response policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the Incident Response Plan to determine that it outlines formal procedure for responding to security events.	No exceptions noted
	CC7.4.2 Remediation of security deficiencies are tracked through internal tools.	Inspected the security incident ticket for a sample of incidents to determine that security issues are tagged and prioritized accordingly.	N/A – Non-Occurrence (No security incidents during the period)
	CC7.4.3 Security deficiencies tracked through internal tools are closed once remediated.	Inspected the security incident ticket for a sample of incidents to determine that security issues are resolved within Spacelift's specified time frame.	N/A – Non-Occurrence (No security incidents during the period)
CC7.5 *The entity identifies, develops, and implements activities to recover from identified security incidents.*	CC7.5.1 Spacelift has created a Disaster Recovery Plan to define the organization’s procedures to recover information technology (IT) infrastructure and IT services within set deadlines in the case of a disaster or other disruptive incident.	Inspected Spacelift's Disaster Recovery Plan to determine that it outlines steps to take in the event of a disaster and has been updated in the past year.	No exceptions noted

Trust Services Criteria for the Security Category	*Description of Spacelift Controls*	*Service Auditor Test of Controls*	*Result of Test of Controls*
Change Management			
CC8.1 *The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.*	CC8.1.1 Spacelift uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Access to the system must be approved by a system administrator.	Inspected the company's version control system and confirmed it is actively used.	No exceptions noted
		Inspected the users of the company's version control tool and confirmed that all accounts were authenticated to the company's account.	No exceptions noted
	CC8.1.2 System changes must be approved by an independent technical resource prior to deployment to production.	Inspected the change ticket for a sample of changes to determine that system changes must be approved by an independent technical resource prior to deployment to production.	No exceptions noted
		Inspected the change ticket for a sample of changes to determine that application changes are tested prior to deployment to production.	No exceptions noted
Risk Mitigation			
CC9.1 *The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.*	CC9.1.1 Spacelift's Risk Assessment and Management Program policy describes the processes Spacelift has in place to identify new business and technical risks and how frequently those risks are mitigated.	Inspected the risk management policy to determine that Spacelift has a formal program for identifying and managing risks.	No exceptions noted
	CC9.1.2 Spacelift has created a business continuity plan to define the criteria for continuing business operations for the organization in the event of a disruption.	Inspected Spacelift's Business Continuity Plan to determine that it defined an operational and organizational strategy in the event of a disruption and has been updated in the past year.	No exceptions noted
CC9.2 *The entity assesses and manages risks associated with vendors and business partners.*	CC9.2.1 The Spacelift team collects and reviews the SOC reports of its sub-service organizations on an annual basis.	Inspected the written policy governing the use of external service providers to determine that the sub-service organization approval process includes collecting and reviewing the provider's SOC report(s).	No exceptions noted

Trust Services Criteria for the Security Category	*Description of Spacelift Controls*	*Service Auditor Test of Controls*	*Result of Test of Controls*
Risk Mitigation			
	CC9.2.2 Spacelift has implemented a Vendor Risk Management program with a framework for managing the lifecycle of vendor relationships.	Inspected the company's vendor management tool to determine that security documentation, including SOC 2 reports, are collected from sub-service organizations and key vendors.	No exceptions noted

Trust Services Criteria for Availability	*Description of Spacelift Controls*	*Service Auditor Test of Controls*	*Result of Test of Controls*
Additional Criteria for Availability			
A1.1 *The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.*	A1.1.1 Processing capacity and usage is monitored and expanded as necessary to provide for the continued availability of the system in accordance with system commitments and requirements.	Inspected the monitoring dashboard to determine that processing capacity and usage is monitored and expanded as necessary to provide for the continued availability of the system in accordance with system commitments and requirements.	No exceptions noted
A1.2 *The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.*	A1.2.1 Spacelift relies on AWS's physical and environmental controls, as defined and tested within the AWS SOC 2 reports.	Not Applicable - Control is Carved Out	The Criterion is carved out and the responsibility of the subservice organization (AWS).
A1.3 *The entity tests recovery plan procedures supporting system recovery to meet its objectives.*	A1.3.1 Backups are performed daily and retained in accordance with a pre-defined schedule in the Backup Policy.	Inspected the database configuration to determine that backups are made daily using the infrastructure provider's automated backup service.	No exceptions noted

Trust Services Criteria for Confidentiality	*Description of Spacelift Controls*	*Service Auditor Test of Controls*	*Result of Test of Controls*
Additional Criteria for Confidentiality			
C1.1 *The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.*	C1.1.1 Management has approved Spacelift security policies, and all employees agree to these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected Spacelift's security policies to determine that they outline requirements for securing the company's operations, services, and systems.	No exceptions noted
	C1.1.2 Management has approved Spacelift security policies, and all employees agree to these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	Inspected the security policy acknowledgement for a sample of new hires to determine that all employees agree to these procedures when hired.	No exceptions noted
	C1.1.3 Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.	Inspected the data classification and data deletion policies to determine that procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.	No exceptions noted
C1.2 *The entity disposes of confidential information to meet the entity's objectives related to confidentiality.*	C1.2.1 Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.	Inspected the data deletion policy to determine that procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.	No exceptions noted