



SOC 2 Type II Report

For the Period January 1, 2022 to December 31, 2022

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



CONFIDENTIAL INFORMATION

The information contained in this report is confidential and shall not be duplicated, published, or disclosed in whole or in part, or used for other purposes, without the prior written consent of JFrog Corporate Entity

Table of Contents

Section I – JFrog Ltd.’s Management Assertion	1
Section II – Independent service auditor’s report.....	2
Section III – Description of JFrog’s Platform relevant to Security, Availability, Confidentiality and Privacy for the Period January 1, 2022 to December 31, 2022	5
JFrog Overview and Background	5
Scope of the Report	5
Organizational Structure	5
Products and Services	7
JFrog Policies Relevant to Security, Availability, and Confidentiality	8
Control Environment, Risk Assessment Process, Information and Communications, and Monitoring Activities	9
Control Environment	9
Control Activities.....	10
Information and Communication	11
Risk Assessment.....	11
Monitoring	13
Security Procedures	13
Logical Access	14
Production Environment Logical Access	14
Access Control, User and Permissions Management.....	14
Access Revocation.....	15
Remote Access.....	16
Physical Access.....	16
Data Centers	16
Asset Management	16
Software Development Life Cycle (SDLC) Overview	16
Infrastructure Change Management Overview	18
JFrog’s Production Environments	18
Production Monitoring	19
Incident Management Process	19
Escalation Process.....	19
Support	19
Ticketing and Management	20
Availability Procedures	20
Backup	20
Monitoring	20
Disaster Recovery Plan (DRP).....	21
Business Continuity Plan (BCP)	21
Confidentiality Procedures.....	21
Data Encryption	22
Privacy Procedures	22
Management.....	22
Information Life Cycle.....	22
Notice.....	22
Privacy by Design	23
Data Subject Rights and Dispute Resolution.....	23
Restricted Transfers.....	23
Disclosure to Third Parties	23
Breach Management	23

User Responsibilities.....	24
Subservice Organization Carve-Out Controls: Amazon Web Services, Google Cloud Platform and Microsoft Azure	24

Section IV – Description of Criteria, Controls, Tests and Results of Tests25

Testing Performed and Results of Tests of Entity-Level Controls.....	25
Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE).....	25
Criteria and Controls.....	25
Control Environment	26
Communication and Information	28
Risk Assessment.....	32
Monitoring Activities	35
Control Activities.....	38
Logical and Physical Access Controls	39
System Operations.....	47
Change Management.....	50
Risk Mitigation	52
Availability.....	54
Confidentiality.....	56
Privacy.....	59



Section I – JFrog Ltd.’s Management Assertion

January 31, 2023

We have prepared the accompanying “Description of JFrog’s Platform relevant to Security, Availability, Confidentiality and Privacy for the Period January 1, 2022 to December 31, 2022” (Description) of JFrog Ltd. (Service Organization) in accordance with the criteria for a description of a service organization’s system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report (Description Criteria). The Description is intended to provide report users with information about the JFrog platform (System) that may be useful when assessing the risks from interactions with the System throughout the period January 1, 2022 to December 31, 2022, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security, availability, confidentiality and privacy set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria).

JFrog Ltd. uses Amazon Web Services, Google Cloud Platform and Microsoft Azure to provide infrastructure management services. The Description includes only the controls of JFrog Ltd. and excludes controls of the subservice organizations. The Description also indicates that certain trust services criteria specified therein can be met only if complementary subservice organization controls assumed in the design of JFrog Ltd.’s controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of the subservice organizations.

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of JFrog Ltd.’s controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

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

- a. The Description presents the System that was designed and implemented throughout the period January 1, 2022 to December 31, 2022 in accordance with the Description Criteria.
- b. The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls and the subservice organizations applied the controls assumed in the design of JFrog Ltd.’s controls throughout the period January 1, 2022 to December 31, 2022.
- c. The JFrog Ltd. controls stated in the Description operated effectively throughout the period January 1, 2022 to December 31, 2022 to achieve the service commitments and system requirements based on the applicable trust services criteria, if user entities applied the complementary user entity controls and the subservice organizations applied the controls assumed in the design of JFrog Ltd.’s controls throughout the period January 1, 2022 to December 31, 2022.

Very truly yours,

DocuSigned by:

75F1338FD5E4487...
Orit Goren, COO

Section II – Independent service auditor’s report

To the Management of JFrog Ltd.

Scope

We have examined JFrog Ltd.’s accompanying “Description of JFrog Ltd.’s JFrog platform throughout the period January 1, 2022 to December 31, 2022” (Description) in accordance with the criteria for a description of a service organization’s system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report* (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description throughout the period January 1, 2022 to December 31, 2022 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria for security, availability, confidentiality and privacy set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

JFrog Ltd. uses Amazon Web Services, Google Cloud Platform and Microsoft Azure (subservice organizations) to provide infrastructure management services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Jfrog, to achieve JFrog’s service commitments and system requirements based on the applicable trust services criteria. The description presents JFrog’s system; its controls; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and operating effectively at Amazon Web Services, Google Cloud Platform and Microsoft Azure. Our examination did not extend to the services provided by Amazon Web Services, Google Cloud Platform and Microsoft Azure and we have not evaluated whether the controls management assumes have been implemented at Amazon Web Services, Google Cloud Platform and Microsoft Azure have been implemented or whether such controls were suitably designed and operating effectively throughout the period January 1, 2022 to December 31, 2022.

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

JFrog’s responsibilities

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

Service auditor’s responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the Service Organization’s service commitments and system requirements, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- obtaining an understanding of the system and the service organization's service commitments and system requirements
- performing procedures to obtain evidence about whether the controls stated in the Description are 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.
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively based on the applicable trust services criteria.
- testing the operating effectiveness of those controls 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 users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs.

Because of their nature, controls at a service organization may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls based on the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

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

Opinion

In our opinion, in all material respects:

- a. the Description presents the JFrog platform system that was designed and implemented throughout the period January 1, 2022 to December 31, 2022 in accordance with the Description Criteria.
- b. the controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the

controls operated effectively and if the subservice organization[s] and user entities applied the controls assumed in the design of JFrog's controls throughout the period January 1, 2022 to December 31, 2022.

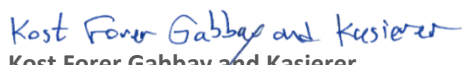
- c. the controls stated in the Description operated effectively to provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period January 1, 2022 to December 31, 2022, if the subservice organization and user entity controls assumed in the design of JFrog's controls operated effectively throughout the period January 1, 2022 to December 31, 2022.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Jfrog, user entities of JFrog's JFrog platform during some or all of the period January 1, 2022 to December 31, 2022 and prospective user entities, independent auditors and practitioners providing services to such user entities who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties, including complementary user entity controls and subservice organization controls assumed in the design of the service organization's controls
- Internal control and its limitations
- User entity responsibilities and how they interact with related controls at the service organization
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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


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

January 31, 2023
Tel-Aviv, Israel



Section III – Description of JFrog’s Platform relevant to Security, Availability, Confidentiality and Privacy for the Period January 1, 2022 to December 31, 2022

JFrog Overview and Background

JFrog is on a mission to enable continuous updates through Liquid Software, empowering developers to code high-quality applications that securely flow to end-users with zero downtime. JFrog is the creator of Artifactory, the heart of the end-to-end universal platform for automating, managing, securing, distributing, and monitoring all types of binaries. JFrog products are available as open source, on-premises, and in the cloud. JFrog’s platform empowers customers with trusted and expedited software releases.

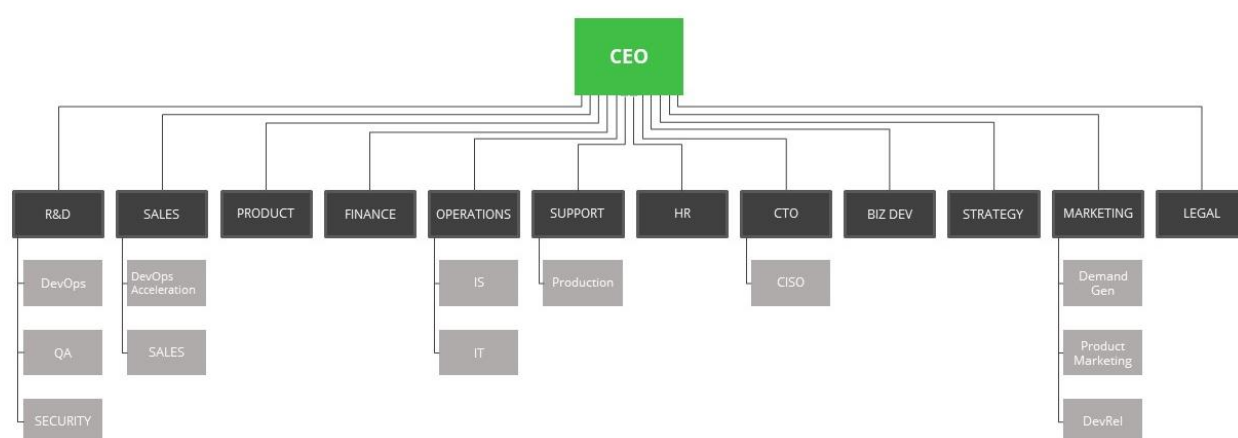
JFrog Ltd. is an Israeli JFrog, publicly traded on the NASDAQ, co-headquartered in Sunnyvale, California and in Netanya, Israel (JFrog and its subsidiaries, hereinafter, JFrog). JFrog’s products and services, as detailed below, are used by millions of developers and DevOps engineers around the world. JFrog is on a “Liquid Software” mission to enable the flow of software seamlessly and securely from developer’s keystrokes all the way to production. The end-to-end, hybrid JFrog Platform provides the tools and visibility required by modern software development organizations to fully embrace the power of DevOps.

Scope of the Report

The scope of this report is limited to the controls supporting JFrog products and services listed herein and does not extend to controls in place at third-party service providers.

Organizational Structure

JFrog’s organizational structure provides the overall framework for planning, directing, and controlling operations. Its approach segregates personnel and business functions into departments according to job responsibilities, reporting lines, and communications, which allows employees to focus on the specific business issues impacting the firm’s customers. JFrog documented an organization chart is approved by the Chief Executive Officer (CEO) and reviewed annually by management. (5).



Key JFrog Departments:

Sales: The Sales department is composed of specialized and experienced sales personnel. It is responsible for sales to new customers and optimizing sales to existing customers.



Human Resource (HR): The HR department is responsible for recruiting, hiring, orienting, and evaluating personnel.

Business Development: The Business Development department is responsible for identifying, building, and managing partnerships with third-party entities and oversees and implements growth opportunities.

Operations:

Operations personnel follow defined protocols for evaluating reported events. Security-related events are assigned to the Security group - CSO Office for evaluation, resolution, and escalation **(44)**.

- Information Technology (IT): The IT team is responsible for providing JFrog employees with required IT assistance.
- Information Systems (IS): The IS team is responsible for the information and technology JFrog uses, as well as for supporting JFrog's business operations.
- Legal Department: The Legal team is responsible for legal affairs and compliance matters at JFrog.

Marketing: The Marketing department is responsible for building JFrog's image, generating sales opportunities, and other international marketing activities.

Research and Development (R&D): The R&D department is responsible for developing JFrog's products, and for business services implemented within the production environment.

This department includes the following groups:

- Development teams for each of the following products:
 - *Artifactory*
 - *Xray*
 - *JAS*
 - *Mission Control*
 - *Pipelines*
 - *Enterprise Plus*
 - *JFrog connect*
 - *Vision*
- *Dev & Cloud Ops group (DevOps Group):* The DevOps Group is responsible for the production SaaS environments deployment, availability, security and scalability. The Group is also responsible for SDLC infrastructure and processes.
- *Quality Assurance (QA):* The QA *engineers* are responsible for testing and validating the R&D's deliverables according to pre-defined scenarios. The QA personnel are allocated per R&D team, and they work closely with the applicable R&D team.

JFrog's Security group - CSO Office is led by our VP Security Engineering & CISO, as part of CTO leadership. The Team is responsible for JFrog cybersecurity strategy and risk management, execution and management of the mitigation plan and secure development life cycle program. The team performs Penetration tests include procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own **(41)**.

JFrog Security: Composed of vulnerability researchers and threat intelligence engineers. This group is responsible for the continuous research on the different vulnerabilities in the wild.



Customer Support: The department is responsible for providing support to JFrog's customers, and works closely with DevOps, Production Engineering, R&D, QA, and Sales.

Production Engineering: The department is responsible for:

- Constantly monitoring the SaaS production availability KPIs and acting on them
- Ensure customer success & tight technical partnership by leveraging best in class processes and tools
- Setting the standard for cloud production readiness for JFrog product releases
- A single point of contact for production troubleshooting and investigations

Product: The Product department is responsible for defining JFrog's product lines and available services, as well as related requirements and priorities. This includes, among others, analyzing market needs and incorporating customer feedback into product roadmaps.

Finance: The Finance department is responsible for JFrog's financial and control activities, including financial planning and accounts receivable.

Internal auditor: Performing the full audit cycle including risk management and control management over operations' effectiveness, financial reliability and compliance with publicly traded JFrog laws and regulations.

- Determining internal audit scope and developing annual plans.
- Obtaining, analyzing, and evaluating accounting documentation, reports, data, flowcharts etc.
- Prepare and present reports that reflect audit's results and document process.
- Conduct follow up audits to monitor management's interventions.

People: System controls are only as strong as the people that implement them. JFrog is committed to employing competent individuals who possess the skills required to successfully carry out JFrog's objectives. Products and services are created and delivered by JFrog's various departments. Members are hired in line with employment policies and procedures.

Products and Services

JFrog Artifactory stores, manages, and controls binaries throughout the software release life cycles. It remedies significant issues faced by software developers and DevOps teams by allowing them to manage, host, and control the flow of binary artifacts from development to production. JFrog Artifactory fully supports software packages created by almost any language or technology. It is the only universal, enterprise-ready repository manager available today, supporting secure, clustered, high-availability Docker registries. Artifactory integrates with all major CI/CD and DevOps tools, providing an end-to-end, automated and bullet-proof solution for tracking artifacts from development to production.

JFrog Xray is a universal software composition analysis (SCA) solution that natively integrates with Artifactory to give developers and DevSecOps teams an easy way to scan binaries. It proactively identifies vulnerabilities in source code and license compliance violations before they manifest in production releases, offering unique application-security value. JFrog Xray continuously scans JFrog Platform to secure all packages stored at a binary level and helps to achieve control and trust earlier in software release cycles by automating security workflows as part of our CICD pipeline.

ACCESS is a product for controlling access rights between the various services of the solution (API for SSO).

JFrog Mission Control offers centralized control, management, and monitoring of all the customer's global enterprise artifact assets. By providing a clear and instant picture of the relationships and flow between the customer's various development organizations, Mission Control offers a JFrog's IT and Ops leaders real-time visibility into their worldwide development, distribution, and consumption of software packages.



JFrog Pipelines is an automation solution for building, testing, and deploying software as part of the CI/CD pipeline. It provides end-to-end orchestration and optimization of all key processes of the DevOps pipeline.

JFrog Enterprise Plus is a product bundle that provides an end-to-end solution for the fast release and distribution of software through the following JFrog products: JFrog Artifactory, JFrog Xray, JFrog Pipelines and JFrog Mission Control.

JFrog Connect is a product for central management of IOT systems and connection to JFROG's other systems, providing an end-to-end solution from the key to updating the software on the end device. It is an agile solution for connected edge devices.

It is a plug-and-play device management platform for connected devices, enabling its users to update, manage, control, monitor and diagnose IoT and embedded devices. The solution also supports over-the-air updates to any device running Linux.

JFrog Distribution enables platform users to speed up deployments and concurrent downloads at scale throughout your SDLC: from CI, to CD, through device management – spanning remote sites, hybrid infrastructure, clouds, edges, embedded devices, and IoT fleets.

Vision platform can identify, prioritize, and mitigate a vast range of security issues. The platform addresses a diverse variety of security risks including supply chain threats, configuration risks, standard compliance, zero-day vulnerabilities, and more.

JFrog Policies Relevant to Security, Availability, and Confidentiality

JFrog is ISO 27001, ISO 27017, ISO 27701, and TISAX compliant, and formal information security policies for the principles and processes within the organization are developed and communicated so that personnel understand JFrog's objectives and commitments. The policies are reviewed annually, updated as needed, and approved by JFrog Management team (12).

System Documentation

A description of JFrog system and its boundaries is documented and communicated through JFrog website (11). The description is available to all JFrog employees. The information provided is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting JFrog's internal control components. JFrog's approved policies, as well as the process of informing JFrog about breaches of system security, availability, confidentiality, privacy, and processing integrity are communicated to the personnel responsible for implementing these. JFrog maintains employee training programs to promote awareness of JFrog's information security and privacy requirements as defined in JFrog's Security Awareness Training Policy (43). This training addresses the GDPR, privacy, and information security. Additionally, ad hoc training sessions are conducted, typically for new tools and periodic security updates. It is role of each manager to decide what training is required as it relates to specific job requirements. Formal information security policies for the principles and processes within the organization are developed and communicated so that personnel understand JFrog's objectives and commitments. The policies are reviewed annually, updated as needed, and approved by JFrog Management team (12). Policy and procedure documents for significant processes that pertain to system requirements, as well as relevant updates, are available via JFrog internal portal, or are otherwise accessible and made available to JFrog employees, as applicable.



Control Environment, Risk Assessment Process, Information and Communications, and Monitoring Activities

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

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its employees. It reflects the overall attitude, awareness, and actions of management, the board of directors, and others concerning the importance of controls and the emphasis given to them in JFrog's policies, procedures, methods, and organizational structure.

Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and made available to JFrog's employees through JFrog's internal portal **(4)**. JFrog's executive management recognizes its responsibility to direct and control operations, and to establish, communicate, and monitor control policies and procedures. Responsibility and accountability for developing and maintaining these are assigned to relevant personnel **(6)**.

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

- (1) management operating style
- (2) organizational structure
- (3) employee job descriptions, and
- (4) organizational policies and procedures

Board of Directors: The Board of Directors (BOD) of JFrog is comprised of nine directors, three of whom Co-founders. The Board of Directors is actively engaged in the governance of JFrog and its strategic direction. The Board's responsibilities include but are not limited to (1) monitoring the actual performance of JFrog through its financial results; (2) monitoring JFrog's compliance with legal and regulatory requirements; (3) analysis of the budget against actual results; (4) guiding JFrog in the way it funds its operation; (5) approving arrangements with executive officers relating to their employment relationships with JFrog, including, without limitation, employment agreements, severance agreements, change in control agreements, and restrictive covenants, and (6) approving equity-based compensation plans in which directors, officers or employees may participate. The Board meets on a quarterly basis. The Board meeting has a fixed agenda that includes, as applicable (1) financial (2) HR (3) Security (4) business updates (5) Marketing and Sales (6) other matters (management discussion) (7) updates from the Board's committees **(1)**.

The Board's Committees (Audit, Compensation and Nominating Governance) meet quarterly to discuss a preset agenda and to evaluate threats and risks during risk assessment meetings according to each respective committee's charter **(2)**.

Management Philosophy and Operating Style: The BOD has delegated to the executive team, chaired by the CEO, the responsibility of managing JFrog and its day-to-day business operations. The team has proven expertise in software management and distribution. It assigns authority and responsibility for operating activities and establishes reporting relationships and authorization hierarchies. The Management team also designs policies and communications that clearly set forth for JFrog personnel JFrog's objectives, explain how their individual actions interrelate and contribute to those objectives, and detail for what and how they will be held accountable. The executive team meets at least on a monthly basis, in order to evaluate risks and threats and discuss, inter alia, security and non-compliance issues and address them **(3)**.



Integrity and Ethical Values: Essential elements of the control environment are integrity and ethical values, that affect the design, administration, and monitoring of key processes. Integrity and ethical behavior are the products of JFrog's ethical and behavioral standards, and how these are communicated, monitored, and enforced in the course of JFrog's business activities. They include the "Codex", which is provided to all new JFrog employees. The document informs personnel of management actions that will be taken to remove or reduce inappropriate incentives, extraneous pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. The Codex also communicates organizational values and behavioral standards through JFrog policy statements and statements from its corporate executives. The BOD and the Management team recognize their responsibility to foster a strong ethical environment within JFrog, to determine that its business affairs are conducted with integrity and in accordance with highest standards of personal and corporate conduct. This is reflected in JFrog's Code of Business Conduct and Ethics, Anti-Corruption Policy and other relevant corporate governance policies.

Compliance: The Compliance team is part of the Legal department. It is dedicated to overseeing a broad range of compliance issues related to JFrog's products, third-party due diligence, training, and internal audits. The team ensures that JFrog complies with applicable laws, regulations, and rules, including the European Union's General Data Protection Regulation (EU GDPR), the California Consumer Privacy Act (CCPA) and that JFrog policies and procedures are being followed. JFrog is ISO 27001, ISO 27017, ISO 27701, and TISAX certified, thus ensuring compliance with information security best practices.

Human Resource Policy and Practices: Human resource policies and practices cover hiring, orienting, training, evaluating, promoting, and compensating personnel. The competence and integrity of JFrog's personnel are essential elements of its control environment. To a great extent, JFrog's ability to recruit and retain highly trained, competent, and responsible personnel is dependent on its human resource policies and practices. Job descriptions are documented and posted on JFrog's website. Candidates go through screening which include checking references and recommendations as well as background checks in accordance with local laws and regulations (7). Teams are expected to adhere to JFrog policies on delivery of services and development of products. These policies are kept on JFrog's internal portal and can be accessed by all JFrog employees. Other policies are communicated to others by email on an as-needed basis.

Commitment to Competence: JFrog's commitment to competence is designed to (1) identify and hire skilled and capable personnel, (2) provide employees with the training and information they need to perform their jobs, (3) evaluate the performance of employees to determine their ability to carry out job assignments, and (4) through the performance evaluation process, identify opportunities for job performance improvement and advancement. New employees are required to sign a standard employment agreement and an NDA addressing business practices, conflicts of interest, confidentiality, and intellectual property (9). New employees go through a dedicated orientation program that was developed by the HR department to train these individuals about core values, significant policies and procedures and goals, as well as introduce them to other key functions and systems (8). All employees undergo an annual review, which includes a manager-employee open discussion on job perception and performance feedback.

Control Activities

Control activities include, but are not limited to JFrog's Information Security Policy, Information Security Incident Management Policy, Information Classification Policy, and its Security Awareness Program. These policies and procedures enable management directives to be carried out to address risks which may hinder the achievement of JFrog's objectives. JFrog's operating and functional units are required to implement control activities that help achieve business objectives associated with:

- (1) the reliability of financial reporting,
- (2) the effectiveness and efficiency of operations, and
- (3) compliance with applicable laws and regulations



Control activities are designed to address specific risks associated with JFrog's operations and are reviewed as part of the risk assessment process. JFrog has developed formal policies and procedures covering various operational matters, which document the requirements for the performance of many control activities.

Information and Communication

Information and communication are integral components of JFrog's internal control system. JFrog identifies, captures, and exchanges information in the form and timeframe necessary to conduct, manage, and control the organization's operations. At JFrog, information is identified, captured, processed, and reported by various information systems, as well as through conversations with customers, third-party vendors, regulators, and employees. Monthly management meetings are held to discuss operational efficiencies within applicable functional areas and to disseminate new policies, procedures, controls, and information about other strategic initiatives. Senior executives who lead these meetings use information gathered from formal, automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to organization-wide security policies and procedures are usually communicated to the appropriate JFrog personnel via email messages and shared with appropriate audiences through the use of JFrog's internal channels. Internal support meetings are held on a weekly basis to discuss open issues registered in JFrog's customer relationship management (CRM) system.

Communication

JFrog internal content is managed via shared documents in JFrog's Google account, which serves as an internal platform for the sharing of relevant information among JFrog's employees. To access this account, each employee is provided with a unique username and password. Availability, confidentiality, processing integrity, privacy, and security-related obligations are communicated to JFrog's employees through non-disclosure agreements (NDAs), while customer obligations and commitments are disclosed within JFrog contracts. Customers sign an NDA that appears within the Terms and Conditions of their JFrog-provided contracts or within personalized contracts that are drawn up between JFrog and particular customers who request contractual language customized to their individual circumstances. Information regarding JFrog's newly-released versions is available to JFrog customers through JFrog customer portal and for JFrog employees within JFrog's internal communications. New employees are required to sign a standard employment agreement and an NDA addressing business practices, conflicts of interest, confidentiality, and intellectual property (9).

Risk Assessment

Risk Identification: The process of identifying, assessing, and managing risks is a critical component of JFrog's internal control system. The purpose of JFrog's risk assessment process is to identify, assess, and manage risks that affect the organization's ability to achieve its objectives. Risk analysis includes identification of key business processes in which potential exposures of some consequence exist. Potential exposures defined by JFrog consider both internal and external influences that may harm JFrog's ability to provide reliable products and services. These definitions are arrived at by: (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying threats to information assets from intentional (including malicious) and unintentional acts, and environmental events; and (4) identifying the vulnerabilities of the identified assets. Identifying potential exposures also includes analyzing potential threats and vulnerabilities arising from vendor-supplied goods and services, business partners, customers, and others with access to JFrog's information systems.

Risk Assessment: Ongoing monitoring and risk assessment procedures are built into the normal recurring activities of JFrog, which include regular management and supervisory activities. Identified risks are analyzed through a process that includes estimating the potential significance of any given risk. Each assessment considers how a given risk should be managed and whether to accept, avoid, reduce or share the risk. Managers of each department are regularly in communication with personnel and may question the accuracy of information that differs significantly from their knowledge of operations. A comprehensive risk assessment is periodically performed to identify and evaluate changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the



achievement of business objectives. As part of this process, threats to system security are identified and evaluated, and the risk(s) from these threats are formally assessed. The process is documented and maintained **(15)**. Key JFrog stakeholders evaluate threats and risks, also through internal audit, internal controls and risk review, which is presented to the audit committee, which takes place on a semiannual basis. The audit committee minutes and actions are documented in written form **(16)**. On an annual basis, JFrog assesses the risks that vendors and business partners (as well as the vendors and business partners of said) represent to the achievement of JFrog's objectives **(17)**. The Management Team considers the significance of each identified risk by determining its criticality and the potential impacts of that risk. Periodic reports on security related events are discussed during meetings of the Security Group.

Fraud Assessment: The assessment of fraud considers:

- fraudulent reporting
- possible loss of assets
- incentives and pressures
- corruption resulting from the various ways that fraud and misconduct can occur, and
- how management and other personnel might engage in or justify inappropriate actions

Controls and governance policies are in place at JFrog to evaluate and monitor the risks of fraud.

Risk Mitigation

Once the severity and likelihood of a potential risk has been assessed, management considers how the risk should be mitigated. The mitigation process involves making inferences based on assumptions about the risk and carrying out a cost-benefit analysis. Necessary actions are taken to reduce the risk's level of severity and the likelihood of occurring, and control activities necessary to mitigate the risk are identified. In working toward the advancement of JFrog's objectives, JFrog selects and develops control activities that contribute to acceptable-level risk mitigation. The risk mitigation process is a direct result of JFrog's risk assessment activities. Risk mitigation activities include the development of policies, procedures, communications, and alternate processing solutions in response to, and in order to recover from security events that disrupt business operations. The policies and procedures include the monitoring of processes, information, and communications in accordance with JFrog's objectives, during response, mitigation, and recovery efforts.

The Management team considers how the environment, complexity, nature, and scope of operations affect the selection and development of control activities. Relevant business processes are thoroughly controlled using a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls. Financial impacts of given risks are also taken in consideration during the mitigation process. JFrog periodically assesses risks associated with their vendors and third-party partners.

Network Security

JFrog has implemented a variety of controls and network-based security measures to protect its enterprise network. A combination of hardware and software-based tools has been deployed to protect the network and help control access to and maintain the integrity of data residing on its systems. This includes the use of firewalls, routers, switches, and near real-time monitoring. JFrog also maintains a network diagram, updated as needed. JFrog network access is authenticated using an industry-standard security protocol, which requires at least two factors of authentication. Memory storage of JFrog's operational devices (i.e., workstations and laptops) is encrypted by automated software to ensure the safety of sensitive information. Access to, exchange of, and extraction from memory storage is allowed only to registered and authorized JFrog devices **(38)**. JFrog employs an industry-standard intrusion detection system/intrusion prevention system (IDS/IPS) to provide network-based monitoring. The IDS/IPS is configured to send automated, real-time alerts, which are being monitored on an ongoing basis. Moreover, JFrog uses an enterprise mobility management (EMM) solution to enforce various policies, in accordance with JFrog's internal and external compliance including, but not limited to, full disk encryption and local firewall policy. To ensure another layer of protection to JFrog's data, JFrog maintains a



data loss prevention (DLP) solution **(40)**. All devices undergo daily security scans to identify potential vulnerabilities. Vulnerability scans to detect potential security breaches are also performed using external tools on the code **(42)**.

Virtualized endpoints in the internal and external (e.g., IaaS and PaaS) environments are protected through virtual and hypervisor security hardening, application endpoint control, host-based firewalls, secure browsing controls, malware protection, intrusion detection and prevention, and continuous monitoring. We have an EDR in place, which includes malware protection. We also have a secure browsing and host-based firewall in our endpoints. Our IaaS and PaaS, which are fully cloud-native, are hardened by design.

Antivirus

Antivirus software is installed on each employee's workstation to help detect and prevent the transmission of data or files that contain virus signatures recognized by the antivirus software. The antivirus software is configured to monitor for updates to antivirus definitions and to update workstations daily. In addition, the EDR provides an immediate, scan less solution for comprehensive vulnerability assessment, management, and prioritization for IT analysts. All data is encrypted at transit **(46)**. Antivirus reports are sent to relevant stakeholders on a regular basis. All JFrog's laptops are centrally managed. Security settings are hardened and cannot be changed by users. When deficiencies are discovered, automatic alerts and remediation actions are triggered **(45)**.

Third Parties

JFrog evaluates its vendors as part of the risk assessment process, addressing issues of security, IT, privacy, and legal obligations, in order to confirm that they meet a certain threshold prior to the commencement of their engagement by JFrog. Related party and vendor systems are subject to review as part of the vendor risk management process. When available and applicable, attestation (i.e., SOC 2) reports are obtained and evaluated **(69)**. New vendors, business partners, and subcontractors are required to sign a standard NDA agreement, which contains clauses regarding confidentiality and the use of intellectual property **(77)**. JFrog's Procurement team helps to manage this process and validates that all the aforementioned considerations have been addressed and that minimum requirements have been met prior to any given third-party engagement.

Monitoring

Management uses automated reports created through various applications and processes to monitor the efficiency of certain processes and the effectiveness of particular key controls. Metrics produced from these systems are used to identify strengths and achievements, as well as weaknesses, inefficiencies, or potential performance issues with respect to a given process. Managers are given the responsibility to inform their employees about these items at the appropriate time. JFrog uses a suite of monitoring tools to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules within internal wiki. The notifications are reviewed and processed according to their level of urgency. The Management team regularly monitors progress with respect to JFrog Service processes. Analyses of root causes are performed through various tools and meetings. To prevent future occurrences, corrective measures are communicated to relevant groups through monitor tools **(61)**.

Security Procedures

The Security group - CSO Office keeps track of and reviews all changes of the products to ensure their high quality and alignment with JFrog's business objectives. The team runs secure code reviews on selective changes in order to adhere to JFrog's security and compliance requirements.

As part of JFrog's multi-layer protection approach, JFrog uses a cloud provider-managed DDoS mitigation service. JFrog utilizes a next-gen WAF, an API protection, advanced rate limiting and bot protection to protect JFrog's production environments from intrusions and advanced application attacks.

As part of JFrog's cyber security strategy program, JFrog uses a Security Information and Event Management (SIEM) system to monitor their various systems. Events are escalated and resolved in a timely manner **(98)**.



JFrog has implemented a security awareness training program, detailing the secure handling of JFrog's confidential information, which includes personal information and customer data.

Security by Design

To ensure the delivery of highly secure services to JFrog's customers, security is an inherent part of JFrog Secure Software Development Life Cycle. For applications to be designed and implemented with proper security requirements, secure coding practices, with a focus on security risks, are integrated into day-to-day operations and development processes. For each feature, the product manager or an R&D security champion assesses if a security review is required. If so, a request is submitted in the change management tool, and a security architecture review is performed by the security team **(99)**.

Vulnerability Management

JFrog has vulnerability management program that assess, monitor and manages vulnerabilities from multiple sources on the production and related environments and resolved them based on internal SLA **(100)**.

Bug Bounty and Vulnerability Disclosure Programs

JFrog manages a bug bounty and vulnerability disclosure programs on a regular basis, to identify vulnerabilities. Issues are evaluated and investigated by the security team and resolved, based on their possible impact and level of criticality, where deemed appropriate **(97)**.

Penetration Testing

Penetration tests help to ensure the overall security status of the production platform and consistency with the confidentiality policy are performed at least annually by a reputable third-party vendor, as well as internally by the security team. Penetration tests include procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own **(41)**. In addition, security scans are performed on an-going basis.

Logical Access

JFrog has established a JFrog-wide Physical and Environmental Security policy designed to protect information at a level commensurate with its values. The policy dictates security controls for media where information is stored, the systems that process it, as well as the infrastructure components that facilitate its transmission.

Production Environment Logical Access

Access to the production environment is restricted to authorized personnel. Access is accomplished via a unique account with one-time access token **(30)**. Only relevant Operations personnel from the DevOps and site reliability engineer (SRE) groups and selected R&D employees are granted access. Users are identified through the use of a user ID/password combination using JFrog's identity management system. Where applicable, strong password configuration settings are enabled to ensure (1) a minimum password length, (2) a limit on the number of attempts to enter a password before the user ID is suspended, and (3) password complexity **(25)**. Access is provided using a change management (CM) tool, which allows for the creation of individual user accounts that have a one-time access token to the Kubernetes, hosts and production stack.

Access restrictions and revocations are accomplished using the vendor's identity and access management (IAM) mechanism. Employees are provided with the minimal access rights required to carry out their duties, based on segregation of duty practice. Permission is granted after an approval process by authorized personnel.

Access Control, User and Permissions Management

JFrog builds its production environments based on one of its CTO office-approved cloud-computing Infrastructure as a Service (IaaS) providers (Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft's Azure). Access to the GCP is restricted to authorized individuals and is performed using a two-factors authentication method **(26)**. Access



to the Azure platform is restricted to authorized individuals and is performed using a two-factors authentication method **(27)**. Also, access to the AWS is restricted to authorized individuals and is performed using a two-factors authentication method **(28)**. In addition, single sign-on (SSO) is used for identity and access management (IAM) that enables users to securely authenticate with multiple applications and websites by logging with one set of credentials. The application relies on a trusted third party to verify the users **(37)**.

Infrastructure management of hardware firewalls and other hardware network components is performed by SOC 2-compliant, cloud SaaS providers. Global management of JFrog infrastructure is carried out by JFrog using dedicated web-interfaces. These interfaces allow JFrog to, among other things, (1) add, modify, and manage hosts and services, (2) create server security configuration policies, (3) configure networks and firewall parameters, (4) manage databases, and (5) manage users. Access to data center management interfaces, as well as vendor ticketing systems, is restricted to authorized individuals. Additionally, JFrog's internal communications network implements a logical segmentation principal which assures that network segments are connected through a firewall and not directly to each other. Firewalls separate the internal network from the internet. Firewall settings are configured to allow only authorized traffic and to assure compliance with JFrog's Information Security Policy. Also, customers are restricted to their own application web interface environment and do not have access to viewing of data from other environments or neighboring customer applications.

JFrog manages and delivers its services using a variety of systems and environments. As previously described, information security controls and procedures are implemented throughout these systems to help prevent unauthorized access to data. Access to system resources is protected through a combination of firewalls, VPNs, native operating system security mechanisms, access controls, database management system security mechanisms, and application controls **(24)**. The database servers reside within the production environment. Access to production environment hosts is restricted to authorized personnel (see the Production Environment: Logical Access).

Recertification of Access Permissions

JFrog has implemented a recertification process to help ensure that only authorized personnel have access to the production interface, servers, environments, and databases. Users, administrators, and permissions within the production environment servers and databases are reviewed on a quarterly basis. New users of JFrog system are granted access upon notification from the HR department, using an on-boarding tool, first to staging and, later, following internal accreditation, to production. Access is only possible via SSO, managed centrally by the IT team. When new user access is granted, a detailed ticket is opened in the IT management ticketing system using a new employee template which includes all details pertaining to user permissions. Access to production environments, databases, and other production-related systems and services, is granted by the DevOps Group based on the employee's role and is documented within a dedicated tool. Other relevant JFrog employees are granted permissions on a need-to-know (least privilege) basis, where access to relevant systems and applications is authenticated using MFA. All accounts are unique and for individual use. Employees whose job functions have changed such that they no longer require access to specific user permissions will immediately have their access disabled or modified. User access is reviewed on a quarterly basis and adjusted based on the ongoing policy of providing only the permissions required to fulfill an employee's role in JFrog **(31)**. New employees are granted access to relevant environments following a notification from HR to the IT team. Permission credentials depend on a given employee's department and role **(36)**.

Access Revocation

To assist in the prevention of unauthorized access to data, user accounts within JFrog's production environment and support tools are disabled promptly upon termination of employment. Terminated employees complete a termination clearance process on their last day at JFrog. The termination notification is documented and accessible within JFrog Internal IT management ticketing system. The process includes revocation of access permissions to JFrog's systems and premises, as well as the timely return of JFrog property, data, equipment, and other JFrog assets. Upon an employee's



notification of job termination by their direct manager, user accounts are disabled on or deleted automatically from JFrog's production platform, applications, and databases **(39)**.

Remote Access

JFrog's internal networks are protected using commercial firewalls configured and administered by JFrog's IT department. JFrog employees are granted remote access to the internal production network environment based on the need-to-know principle. Traffic entering JFrog's internal resources is monitored and screened by a firewall and monitoring tools. All JFrog employees can access internal resources remotely, but only via a VPN and SSO, using 2FA.

Physical Access

JFrog recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures, and controls have been implemented to help prevent unauthorized access to data, assets, and restricted areas. Physical access to JFrog's offices is restricted to authorized personnel. Permissions to grant access are restricted to the office manager and the authorized designees **(34)**. JFrog visitors are accompanied while on JFrog premises **(35)**.

Data Centers

All of the physical security for JFrog's production environment is managed by JFrog's cloud infrastructure service providers. In fact, JFrog employees do not have access to any of the firm's data centers. JFrog's IaaS providers are responsible for implementing an appropriate set of controls to address physical security issues. In its deployments and configurations, JFrog uses its cloud providers' best practices. In addition, JFrog databases are encrypted within the cloud. JFrog end-point disks are encrypted as well **(75)**.

Asset Management

JFrog assets are tracked and managed throughout each asset's life cycle. Every asset is assigned an "owner" to ensure there is an individual responsible for securing that asset. Tracked assets include production components, as well as employee devices.

Software Development Life Cycle (SDLC) Overview

The software secure development lifecycle includes architectural reviews, static and dynamic code analysis, and open-source analysis. Its SDLC security, including by:

- Further restricting access rights to its build environment
- Reviewing the build environment's architecture, the privileged and non-privileged users with access to it, and the network surrounding it

Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the Management team within JFrog's Change Management application. Change management tickets are prioritized and labeled based on development phase and urgency **(47)**. Software development and change management at JFrog include development and production changes to all JFrog solutions. The processes are carried out in a manner that helps ensure JFrog's products are properly designed, tested, approved, and aligned with the business objectives and security standards of JFrog and its customers. As part of JFrog's practices, we follow the OWASP standards and updates, adopting their secure coding checklist, and sharing them with the relevant teams. Personnel are trained with secure development using a development secure training application, educational sessions, security vulnerabilities demos from penetration tests, bug bounty programs, CTF and more.

Product release has security requirements: Design review, security code review, security vulnerability scans (SAST/DAST/XRAY), Internal pen Test. Static application security testing (SAST), or static analysis, is a testing methodology that analyzes source code to find security vulnerabilities that make applications susceptible to attack. SAST tools scan an



application before the code is compiled. SAST tools give developers real-time feedback as they code, helping them fix issues before they move the code to the next phase of the SDLC. This prevents security-related issues from becoming an afterthought. DAST (Dynamic Application Security Testing) solutions evaluate application inputs and outputs, focusing only on the attack surface. DAST solutions test running binaries to find vulnerabilities that SAST tools cannot, such as those found in dynamically generated code. JFrog incorporated SAST and DAST tools as part of our development lifecycle and runs SAST and DAST scans every time code is checked in, as well as when code is released. JFrog's R&D teams regularly receive relevant training which increases their awareness, knowledge, and capabilities to design and develop features more securely.

We use JFrog Xray as part of our development process, to scan for security vulnerabilities and in a case of vulnerability, they block the process. Several groups are involved in software development life cycle (SDLC) and change management process, including Product, R&D, and CTO, all participate in defining the change roadmap. Changes are documented and approved by authorized employees. As detailed above, personnel responsible for the design, development, deployment, and operation of systems affecting security, availability, and confidentiality are trained on a regular basis. Additionally, changes that may affect system security, availability, or confidentiality are communicated to management and affected users. Such communication is carried out via the change management tool, as well as via email **(13)**. The development and test environments are logically separated from the production environment. In addition, there is a segregation of duties between the environments, e.g., developers must not have administrative access in the production environment. Likewise, production data must not be used in test or development environments. In accordance with AD groups. Permissions are role-based; Users don't receive additional access upon request. Only developers and R&D have access to the development environment.

Change Initiation: Change requests and reporting of production bugs occur in the change management application and are reviewed during sprint meetings, managed by the Product team. Requests are reviewed from various angles, as applicable (e.g., DevOps, or security). Decisions to approve, reject, or prioritize requirements are made on an ongoing basis by the code owner/approval owner. Changes are documented in meeting minutes and actions taken are recorded in the change management tool. Production bugs are tracked in a dedicated Customer Support portal, as well as in the change management application. Changes impacting customers are communicated to them through release notes posted to the portal, while internal employees receive notifications via JFrog's internal portal or other applicable methods of internal communication **(14)**. Bugs are assigned to a developer until they are resolved. Once a bug is fixed, the developer updates that bug's status within the change management application. The fix is then tested by the QA engineer and needs to be approved on the PR level by the code owner and the team leader prior to moving to the production environment. Administrative access to the change management application, which allows the creation of builds and the publication of versions, is restricted to authorized personnel, and only possible via SSO. Access to the deployment tool is equally restricted to authorized personnel.

Software Testing and QA Process: New roadmap features are subject to constant review by the CTO office and lead developers before being introduced to R&D by the Product Management team. Once the change management application issues a notification, the QA engineer begins testing. All new features are presented by product managers to relevant parties (developers and QA engineers) and a basic testing plan is formulated using a dedicated tool. Tested database scripts are incorporated into the Change Management application. This stage also includes a risk assessment that addresses integration with other products. Development is performed on a custom branch. JFrog's testing infrastructure is capable of running all such tests on these specific branches. During development, complete test spec and automation testing is developed by the QA engineers and R&D developers. All pull requests must be submitted to code review before being merged into a master branch. Permission to approve code review and merges are restricted to authorized personnel and are required as part of the change management process in order to deploy a version to production **(48)**. All master builds are submitted to a scanning tool for static code analysis. Unit, integration, functional UI, black box, and system tests are performed on all supported environments. All builds are scanned by JFrog Xray for security vulnerabilities. If critical, high or medium severity vulnerability will be discovered, the build will be failed until



the vulnerability will be fixed. Permissions to close a task in the Change Management application are restricted to authorized personnel, and all bug regressions are closed only after automation tests are added. A log containing all test results is available for review by QA and R&D team leaders. The R&D and product teams meet on a set frequency to review sprint planning and bugs (53). As bugs are addressed, prior to deployment, the company tests integration of all internal components and approve new versions for upload by the DevOps Group to a non-customer-facing production-like (staging) environment. The purpose of this action is to determine that new versions will behave normally within an environment similar to production. Builds are transferred to a staging environment by an automated tool after successfully passing the testing pipeline (51). Once approved, new versions are promoted for public use while, in parallel, each released build must pass unit and integration tests using the orchestrator tool.

The DevOps team deploys changes to the production environment. Through the use of an orchestrator coverage tool, every merge request undergoes unit testing and integration testing (55). Vulnerability code scanning findings trigger an alert to relevant personnel. Findings are documented, tracked and resolved in a ticketing system prior to deployment (56). Appropriate JFrog personnel are notified when new versions are deployed to production. Changes impacting customers are reviewed in go/no-go meetings and, where applicable, are communicated through release notes emails. Database changes are developed by the developers and tested as part of the QA process (see above).

Monitoring the Change Management Processes

To assess identified risks and review changes applied to the application, a risk assessment meeting of the Management team is held at least every quarter. Changes applied to JFrog application are documented within the change management application. Action items are updated within JFrog management tools. Additionally, metric reports are regularly issued to the Management team, which provide them with key indicators regarding the change management process. Risk assessment issues relevant to each member of the Management team are included in the monthly report submitted to the management forum.

Infrastructure Change Management Overview

In response to evolving customer and market needs, JFrog regularly makes changes within its production environment. These include adding, removing, or changing the configuration policies of existing servers or performing routine maintenance activities, executing software updates, or implementing other infrastructure-related changes, according to available possibilities provided by the third-party vendors. Infrastructure changes are documented within the Change Management tool. Emergency changes are executed and updated as part of hot fixes, which follow for the same, aforementioned processes, albeit typically within a shorter timeframe. Moreover, sprint meetings take place every two weeks. There are also planning meetings where tasks are discussed and prioritized, as well as daily standup status meetings.

JFrog's Production Environments

The processes described below are executed within JFrog's production environments, which are hosted in multiple data centers and operated by a variety of cloud providers (AWS, GCP, Azure). JFrog's production environment is located in multi regions. To maintain high availability standards, the regions have replica in a different availability zone (64). Permission to access the version control, build, and change management tools is restricted to authorized personnel and is granted through personal identity permissions to the SSO via 2FA. After, the user accesses the production environment via a one-time unique token (33). Developers have restricted permissions to the production environment based on predefined policies (52). Access to DevOps Group ("management") tools and servers is restricted to authorized personnel. JFrog Artifactory and JFrog Platform SaaS services are offered via Amazon Web Services (AWS), the Google Cloud Platform (GCP), and Azure (Microsoft's cloud computing platform), with data centers located around the globe. JFrog Connect and Vision are offered on AWS in different regions.

The architecture of JFrog production environments assumes each cloud provider's best practices. Infrastructure management of security and access standards is performed using a given cloud provider's tools. JFrog uses a dedicated web interface, as well as infrastructure as a code (Terraform), which allows JFrog to, among other things, (1) add, modify,



and manage servers, (2) create security policies as they relate to these servers, (3) configure network and firewall parameters, (4) manage databases, and (5) manage users. Access to the management interface of individual cloud providers is restricted to authorized individuals. Customers are permitted to choose a preferred cloud provider, as well as a region in which their application(s) will run. Customers may also opt for an isolated solution, which entitles them to dedicated resources. Interactions between customers and JFrog's production environment are generally restricted to an encrypted channel on an authenticated SSL connection.

Production Monitoring

JFrog's production network encompasses numerous components, including web services, application and data server types, databases, monitoring tools, and redundant network equipment provided as part of AWS, GCP and Azure services. To provide high service availability to customers and to support the operations of the cloud environments, JFrog maintains a dedicated DevOps Group, a Production engineering and NOC teams responsible for ongoing work within the production environment and investigating escalated issues. The production environment, including servers and the application, is monitored 24/7/365 by the DevOps Group, the Production engineering and NOC teams. Key JFrog management staff members are notified of events related to security, availability, and confidentiality.

Incident Management Process

When an incident is detected, per internal policy, a JFrog-wide cooperative effort is triggered. The incident is classified based upon its security, availability, and/or confidentiality impact, and security incident management proceeds in three main stages:

- (i) containment and resolution of the problem;
- (ii) communication of the problem to customers, focusing on those impacted by the incident, while minimizing the impact on others;
- (iii) analysis of the incident and planning to prevent similar occurrences

Incidents are classified via an impact assessment process and are communicated to senior management as required. In accordance with JFrog's Incident Response Plan, each incident is resolved by allocating tasks to Security Incident Response Team members, as well as to any other relevant JFrog staff or departments, and by managing communications between the parties executing a resolution plan. In the event of a service outage or issue, customers are notified via JFrog's customer support portal.

Escalation Process

JFrog's goal is to resolve issues in an efficient manner. All issues are tracked and updated in the CRM system. The escalation process is defined and documented by the Customer Support department. Tickets are escalated as deemed necessary by the Production Engineering, R&D, Product, or Solution Engineering teams. Based on JFrog's escalation procedures and SLA notification thresholds, service interruptions are communicated to customers via email **(19)**. Response time to customer issues is defined in the SLA. The SLA is communicated to customers via JFrog website **(20)**. Additionally, JFrog uses release notes to provide notification to customers on the availability of important fixes and improvements to help them ensure their systems are up-to-date. Changes impacting customers are communicated to them through release notes posted to the portal, while internal employees receive notifications via JFrog's internal portal or other applicable methods of internal communication **(14)**.

Support

JFrog's Service Level Agreements (SLAs) assure 24/7 support for Pro X and Enterprise customers. Issues are reported to the Support department via the customer support portal, a dedicated email, or by phone **(21)**. To maintain visibility on current support issues and potential problem trends, support metrics including Key Performance Indicators (KPIs), are available to JFrog's stakeholders within the CRM application **(22)**. JFrog's customer support procedures are designed to provide end-to-end support for diagnosing and triaging issues arising in production. Monthly meetings are convened to



report major open issues to the Management team **(23)**. This infrastructure ensures the efficient identification of root causes, appropriate resolution of problems, and rapid resumption of normal operations.

A Customer Ticket Portal is available for faster support and to allow:

- tracking the current status and history of all tickets
- new support tickets to be opened
- quick access to JFrog products knowledge base

JFrog's support desk is available 24/7/365 from different locations around the world ("follow the sun"). Issues raised are documented within the CRM tool

Ticketing and Management

A ticket is opened when an issue is raised by a customer or when an issue is proactively identified. JFrog uses a third-party CRM application to manage, classify, and ticket customer support-related issues. Tickets are classified by urgency level and assigned to the appropriate support tier for resolution.

Availability Procedures

JFrog's production environment and application level are fully managed and monitored by JFrog's DevOps Group using tools provided by JFrog's third-party cloud providers, as well as internal tools. JFrog has implemented the operations management controls described above to manage and execute production operations. DR restore tests are performed on an annual basis **(63)**. JFrog's production environment is located in multi regions. To maintain high availability standards, the regions have replica in a different availability zone **(64)**.

Backup

The applications' database is backed up automatically on a daily basis. Weekly full-system and daily incremental backups are also performed **(58)**. The backups are maintained up to 35 days. To accomplish these tasks, JFrog maintains a backup server infrastructure. Backups are performed from a remote location in a neighboring region, database servers have multi-availability zones **(60)**. JFrog maintains two copies of its most recently executed full backups; the content of incremental backups is retained for a period of 35 days. The access to the backup and database storage is restricted to authorized individuals **(32)**. JFrog's Artifactory Cloud backup is based on the following procedure:

- Filestore data (S3 content) - Event-based, cross-region replication to a secondary, disaster recovery (DR) bucket. There is a real-time backup, with a retention period of fourteen days.
- Buckets maintain at least seven-day retention for older versions of overwritten/deleted objects (main & DR).
- Databases - Databases are retained in region clusters (at least two nodes in different zones), Multi-Zone Relational Database Service (MZ-RDS) on AWS, and Main Failover nodes on GCP and the geo-redundant storage (GRS) setup on Azure. In AWS, a read replica is also established in a DR neighbor region for DR readiness/backup.
- Databases are backed up daily and retained for up to 35 days. Databases also keep binlogs for replay purposes and point-in-time recovery from any 24-hour back-up.
- Server and customer configurations are managed, updated, and pulled from an internal central configuration system, which itself is backed up and maintained.

Monitoring

As they arise, security, confidentiality, and availability non-compliance issues are brought to the attention of the Management team, which addresses them on an as-needed basis. Such issues are documented as part of a Root Cause Analysis (RCA) report created by the Support team, Production Engineering team, or Senior Director of DevOps. Change reports from the Change Management Tool, vulnerability reports from production, monitoring tools, and support metrics are reviewed and discussed by Management in relation to JFrog's system security, availability, and confidentiality policies.



Additionally, environmental, regulatory, and technological changes are monitored. Their effects are assessed, and policies are updated, accordingly. A summarized monitoring protocol is made available to relevant managers and team members.

Disaster Recovery Plan (DRP)

JFrog has developed a Disaster Recovery Plan (DRP) that sets forth the means and manner by which it can continue to provide critical services in the event of disaster **(62)**. A disaster is defined as an incident that results in the loss of computer processing for an entire region in the AWS, GCP, Azure for Artifactory Cloud. Business measures, as well as data loss and customer downtime (impact) must be considered. A disaster can result from a number of accidental, malicious, or environmental events (e.g., fire, flood, terrorist attack, human error, software or hardware failure). The primary objective of this plan is to ensure the continued operation of identified, business-critical systems in the event of a disaster. Artifactory Cloud objectives consist of:

- being operational in the DR region with a Recovery Time Objective (RTO) of twenty-four hours following a DR migration invocation. JFrog's Recovery Point Objective (RPO) is one hour;
- operating in the DR region for up to thirty days;
- reinstating main facility (or, in case of complete loss, an alternative) in the AWS, GCP, or Azure premises within thirty days; .and
- minimizing disruption to JFrog's services and business

After assessing a given situation following a disaster or crisis, the decision to initiate DR procedures will be made by the CTO or the DevOps Group director. DR restore tests are performed on an annual basis **(63)**.

Business Continuity Plan (BCP)

JFrog BCP's objective is to guide JFrog's management in connection with business continuity and to ensure the timely maintenance or recovery of operations, including services to customers, when confronted with adverse events such as natural disasters, technological failures, human error, or terrorism, and to ensure that safety of all personnel are assured when activating the BCP.

The primary objective of the BCP is to ensure the continued operation of business-critical systems and the continuity of provision of the services, without interruption or deterioration in the event of a disaster.

The BCP is designed to protect data, of JFrog and of third parties. To ensure that data of any kind is never compromised, and should a data loss event or equipment failure situation take place, the BCP sets forth processes and procedures to ensure a timely and predetermined course of action is followed in connection with such events.

JFrog will maintain a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) consistent with industry best practices for JFrog Platform, which will be tested at least annually. In addition, the BCP and DRP will ensure: (i) that installed systems used to provide JFrog Platform will be restored in case of interruption; (ii) JFrog's ability to restore the availability and access to the customer data in a timely manner in the event of a physical or technical incident; and (iii) the ongoing confidentiality, integrity, availability, and resilience of systems JFrog uses to provide JFrog Platform.

Confidentiality Procedures

JFrog understands that confidentiality issues are critical as they relate to services provided. Information handled by JFrog is considered private and subject to the highest levels of security (see Logical Access and Security above). JFrog discloses its confidentiality practices through various media, such as JFrog website, its applications, and its contracts. JFrog notifies the impacted customers whenever a disclosed confidentiality practice is discontinued or changed to be less restrictive **(71)**. Customers' sensitive data is encrypted within JFrog application **(65)**. Additionally, to maintain the levels of system confidentiality that conform with JFrog's confidentiality commitments, third-party infrastructure providers sign confidentiality agreements with JFrog **(66)**. Logical access to stored data is restricted to application and database administrators. Data is stored in encrypted format using software supporting the advanced encryption standard (AES). Access permissions are reviewed on an annual basis **(67)**. Moreover, the enterprise requires a minimum of AES 256-bit level encryption for data at rest and secures production data containers, using server-side encryption **(72)**. Related party and vendor systems are subject to review as part of the vendor risk management process. When available and applicable,



attestation (i.e., SOC 2) reports are obtained and evaluated **(69)**. Also, confidentiality agreement is disclaimed as it relates to contracts with infrastructure third party providers in accordance with JFrog security policy **(70)**. JFrog places heavy emphasis on logical security segregation built within its hosted applications as a means of separating one tenant's users from others. Encryption between JFrog customers and JFrog application is enabled using best industry standards and practices **(74)**. JFrog customers are restricted to their own web interface environment (server) and do not have access to view data in other JFrog environments **(73)**. An automatically generated log entry is produced after every access to a JFrog-hosted environment or database **(76)**. Additionally, new vendors, business partners, and subcontractors are required to sign a standard NDA agreement, which contains clauses regarding confidentiality and the use of intellectual property **(77)**.

Data Encryption

Data in Transit - Data in transit is defined as data that is actively transferring between different destinations (e.g., applications to databases or object storage) over the same network or over the internet. In JFrog SaaS solution, every customer's data is encrypted in transit using HTTPS over TLS V1.2, with strong cipher suites.

Data at Rest - Data at rest is defined as data that is physically stored and hosted in any digital form (e.g., cloud storage, databases, data warehouses, or cloud backups) and not actively transferring between different destinations. In JFrog SaaS solution, all hosted data at rest is securely stored in a database and object storage using 256-bit AES encryption.

Key Management - All our encryption keys are stored hashed and are managed in a cloud-hosted key management service, which lets us create and manage cryptographic keys and control their use across a wide range of services and in your applications. It lets us generate, use, rotate, and destroy cryptographic keys.

Privacy Procedures

Management

Responsibility and accountability for compliance with data privacy requirements is managed by JFrog's Senior Compliance Manager and its General Counsel. To help ensure that JFrog employees are aligned with privacy practices and aware of their duties with regards to data privacy, JFrog has mandatory annual trainings for all new and existing employees and contractors covering information about privacy awareness, and best practices for data protection. Additionally, privacy and information security training are conducted during the employee onboarding process. Upon customer request, at the conclusion of a contractual agreement, JFrog will dispose of customer confidential information **(68)**.

Information Life Cycle

Personal information is collected consistent with JFrog's objectives related to privacy **(82)**. Customers sign contracts that address how their personal information will be handled **(81)**. Additionally, JFrog collects and maintains accurate, up-to-date, complete, and relevant personal information to meet JFrog's objectives related to privacy **(95)**. Access to personal information in databases is restricted to authorized JFrog employees, including help desk personnel. Access review is conducted on a quarterly basis. **(83)**. Further, JFrog retains personal information consistent with JFrog's objectives related to privacy **(84)**. JFrog securely disposes of personal information in keeping with JFrog's objectives related to privacy **(85)**, as well as upon customer request or at the conclusion of a contractual agreement, JFrog shall delete personal information provided by the customer pursuant to such contractual agreement, within sixty days.

Notice

To satisfy JFrog's objectives related to privacy, JFrog provides data subjects with an accounting of the personal information held and, upon their request, disclosure of their personal information held **(94)**. JFrog's privacy statement, which fully discloses the type of personal information JFrog may collect, as well as how JFrog may use this information, is available on JFrog's website **(79)**. JFrog's privacy statement is reviewed and updated on at least an annual basis **(80)**.



Privacy by Design

To ensure the delivery of highly secure services to JFrog's customers, security and privacy are an inherent part of JFrog Secure Software Development Life Cycle. For applications to be designed and implemented with proper security requirements, secure coding practices, with a focus on privacy and security risks, are integrated into day-to-day operations and development processes. Changes affecting the level of security, privacy, availability, and confidentiality within the production environment are reviewed as part of the risk assessment process. Moreover, responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies. The names of such person or group and their responsibilities are defined **(78)**.

Data Subject Rights and Dispute Resolution

JFrog utilizes a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others, and periodically monitors compliance to satisfy JFrog's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner **(96)**. JFrog grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides electronic copies of that information, or erase it. If access is denied, data subjects are informed of the denial and, as required, the reason for such denial **(86)**. In addition, to satisfy JFrog's objectives related to privacy, JFrog corrects, amends, or appends personal information based on information provided by data subjects. If a request for correction is denied, data subjects are informed of the denial and the reason for such denial **(87)**.

Restricted Transfers

In accordance with Chapter IV of the GDPR on "Transfers of personal data to third countries or international organizations", JFrog will execute the EU Standard Contractual Clauses, and the UK International Data Transfer Addendum, as applicable, with regards to transfer of personal information to third countries from the EU and the UK, respectively. If the mechanism for Restricted Transfers of personal information outside of the EU and/or the UK will change or require an update, JFrog will put in place alternative arrangements for such Restricted Transfers, as required by applicable data protection laws.

Disclosure to Third Parties

To satisfy JFrog's objectives related to privacy, JFrog creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to third parties **(89)**. Privacy commitments are obtained from vendors and other third parties who have access to personal information. On a periodic and as-needed basis, JFrog assesses compliance on the part of those parties and, if necessary, takes corrective action **(91)**. In addition, JFrog discloses Customer personal information to third parties with Customer's prior approval when needed **(88)**. Upon receipt of any request for disclosure of personal information by any government, including governmental bodies and law enforcement agencies, JFrog shall, to the extent allowed by law, (i) promptly forward and notify the customer of receipt of such request; (ii) make reasonable efforts to oppose the request if possible; and (iii) limit the scope of any disclosure to what is strictly necessary to respond to the request.

Breach Management

JFrog creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information **(90)**. JFrog obtains commitments from vendors and other third parties with access to personal information to notify JFrog in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures **(92)**. To satisfy JFrog's objectives related to privacy, JFrog will provide notification of breaches and incidents to affected data subjects, regulators, and others **(93)**, as applicable, within 72 hours from JFrog's validation, unless such notification is delayed or prohibited by an act or order of supervising authority. JFrog will provide the customer with a description of (i) the nature of the breach; (ii) likely consequences of the breach; and (iii) mitigation measures taken to address the breach. JFrog shall take all necessary steps consistent with industry best practices,



considering the severity of the risk, to resolve such breach as quickly as possible and to prevent its recurrence. JFrog will reasonably assist Customer with conducting investigations and analysis regarding the breach.

User Responsibilities

In order to achieve JFrog's control objectives, below are suggested user responsibility actions to be taken:

- Establishing controls and procedures to comply with contractual requirements.
- Providing accurate and up-to-date contact information.
- Training the users of the platform and account administrators.
- Manage user's accounts (this includes but is not limited to: user management, permissions etc.).
- Defining, configuring and monitoring security controls for user's accounts (this includes but is not limited to: password policy, user permissions, communication protocols (http/https), masking of user's sensitive data within chat transcripts, activation of encryption).
- Establishing procedures for confidentiality guidelines to be reviewed and updated on a regular basis so that user is in compliance with user organization's current confidentiality policy.
- Appropriately managing physical and logical security at user locations for hardware and software that is used to connect to JFrog.
- Having appropriate personnel available to report issues and to discuss them with JFrog's Customer Support

Subservice Organization Carve-Out Controls: Amazon Web Services, Google Cloud Platform and Microsoft Azure

Subservice organizations are expected to:

- Implement controls to enable security and monitoring tools within the production environment.
- Implement logical access security measures for infrastructure components, including native security or security software, and appropriate configuration settings.
- Restrict access to virtual and physical servers, software, firewalls, and physical storage devices to authorized individuals, and to review their lists of users and permissions granted on a regular basis.
- Implement controls to provision access only to authorized persons and remove access when such permission is no longer appropriate.
- Secure their facilities to permit access only to authorized persons.
- Monitor access to their facilities.
- Be consistent as regards to defined system security, processing integrity availability, and security as it relates to the design, acquisition, implementation, configuration modification, and management of infrastructure and software.
- Maintain system components, including configurations, consistent with the defined system security and related policies.

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

Testing Performed and Results of Tests of Entity-Level Controls

In planning the nature, timing and extent of its testing of the controls specified by JFrog, KFGK considered the aspects of the JFrog control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

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

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

Criteria and Controls

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of JFrog. The testing performed by Kost Forer Gabbay and Kasierer (KFGK) and the results of tests are the responsibility of the service auditor. Refer to the Trust Services criteria mapping section for the mapping of these controls to the Trust Services criteria.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
9	New employees are required to sign a standard employment agreement and an NDA addressing business practices, conflicts of interest, confidentiality, and intellectual property.	For the selected employees, inspected the NDA's signed and determined that they addressed the business practices, conflicts of interest, security and confidentiality clauses.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The Board meets on a quarterly basis. The Board meeting has a fixed agenda that includes, as applicable (1) financial (2) HR (3) security (4) business update (5) Marketing and Sales (6) other matters (management discussion) (7) updates from the Board's committees	Inspected an agenda example and invitations and determined that the board met on a quarterly basis. The board meeting had a fixed agenda.	No deviations noted.
2	The Board's Committees (Audit, Compensation and Nominating Governance) meet quarterly to discuss a preset agenda and to evaluate threats and risks during risk assessment meetings according to each respective committee's charter.	Inspected an agenda example and invitations and determined that the Board's Committees met on a quarterly basis. The Board's Committees meeting had a fixed agenda.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The Board meets on a quarterly basis. The Board meeting has a fixed agenda that includes, as applicable (1) financial (2) HR (3) security (4) business update (5) Marketing and Sales (6) other matters (management discussion) (7) updates from the Board's committees	Inspected an agenda example and invitations and determined that the board met on a quarterly basis. The board meeting had a fixed agenda.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	The Board's Committees (Audit, Compensation and Nominating Governance) meet quarterly to discuss a preset agenda and to evaluate threats and risks during risk assessment meetings according to each respective committee's charter.	Inspected an agenda example and invitations and determined that the Board's Committees met on a quarterly basis. The Board's Committees meeting had a fixed agenda.	No deviations noted.
3	The executive team meets at least on a monthly basis, in order to evaluate risks and threats and discuss, inter alia, security and non-compliance issues and address them.	Inspected an agenda example and invitations and determined that the management team met on a weekly basis. The management meeting had a fixed agenda.	No deviations noted.
4	Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and made available to the Company's employees through JFrog's internal portal.	Inspected the policies and procedures of the company and a screenshot of the company internal portal and determined that policies and procedures were documented, reviewed and approved on an annual basis by the management team and are made available to JFrog employees.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
7	Job descriptions are documented and posted on JFrog's website. Candidates go through screening which include checking references and recommendations as well as background checks in accordance with local laws and regulations.	Inspected an example of job descriptions and a sample of reference check for new employees and determined that job descriptions were documented and posted on JFrog's website and candidates went through screening and appropriate background checks, which included checking references and recommendations.	No deviations noted.
8	New employees go through a dedicated orientation program that was developed by the HR department to train these individuals about core values, significant policies and procedures and goals, as well as introduce them to other key functions and systems.	Inspected the JFrog on-boarding documentation and a sample of an orientation day scheduled for new employees and determined that new employees went through a dedicated orientation program that was developed by the HR department to train these individuals about core values, significant policies and	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		procedures and goals, as well as introduce them to other key functions and systems.	

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and made available to the Company's employees through JFrog's internal portal.	Inspected the policies and procedures of the company and a screenshot of the company internal portal and determined that policies and procedures were documented, reviewed and approved on an annual basis by the management team and are made available to JFrog employees.	No deviations noted.
5	JFrog documented an organization chart is approved by the Chief Executive Officer (CEO) and reviewed annually by management.	Inspected the JFrog organization chart and determined that an organizational chart was documented. Management authorities and reporting hierarchy were clearly defined.	No deviations noted.
6	Responsibility and accountability for developing and maintaining these are assigned to relevant personnel.	Inspected a sample of policies and determined that they were assigned to the relevant personnel and approved on an annual basis by the management team.	No deviations noted.

Communication and Information

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
22	To maintain visibility on current support issues and potential problem trends, support metrics including Key Performance Indicators (KPIs), are available to the Company's stakeholders within the CRM application.	Inspected the evidence and determined that support metrics including Key Performance Indicators were available to the Company's stakeholders within the CRM application.	No deviations noted.
23	JFrog's customer support procedures are designed to provide end-to-end support for diagnosing and triaging issues arising in production. Moreover,	Inspected the evidence and determined that JFrog's customer support procedures were designed to provide	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	quarterly meetings are convened to report major open issues to the Management team.	end-to-end support for diagnosing and triaging issues in production.	

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
11	A description of the JFrog system and its boundaries is documented and communicated through the JFrog website.	Inspected screenshots from the internal portal and JFrog Cloud Architecture document and determined that a description of the JFrog system and its boundaries was documented and communicated to JFrog employees within the internal portal and to customers through the JFrog website.	No deviations noted.
13	Changes that may affect system security, availability, or confidentiality are communicated to management and affected users. Such communication is carried out via the change management tool, as well as via email.	Inspected the evidence and determined that changes that may affect system security, availability, or confidentiality were communicated to management and affected users.	No deviations noted.
14	Changes impacting customers are communicated to them through release notes posted to the portal, while internal employees receive notifications via JFrog's internal portal or other applicable methods of internal communication.	Inspected a screenshot of release notes published on the JFrog external portal and emails that were sent to the company employees and determined that changes impacting customers were communicated to them through release notes posted to the portal, while internal employees receive notifications via JFrog's internal portal or other applicable methods of internal communication.	No deviations noted.
22	To maintain visibility on current support issues and potential problem trends, support metrics including Key Performance Indicators (KPIs), are available to the Company's stakeholders within the CRM application.	Inspected the evidence and determined that support metrics including Key Performance Indicators were available to the Company's stakeholders within the CRM application.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
23	JFrog's customer support procedures are designed to provide end-to-end support for diagnosing and triaging issues arising in production. Moreover, quarterly meetings are convened to report major open issues to the Management team.	Inspected the evidence and determined that JFrog's customer support procedures were designed to provide end-to-end support for diagnosing and triaging issues in production.	No deviations noted.
68	Upon customer request, at the conclusion of a contractual agreement, JFrog will dispose of customer confidential information.	Inspected the evidence and determined the upon customer request, at the conclusion of a contractual agreement, JFrog disposed of customer confidential information.	No deviations noted.
71	JFrog discloses its confidentiality practices through various media, such as the Company website, its applications, and its contracts. JFrog notifies the impacted customers whenever a disclosed confidentiality practice is discontinued or changed to be less restrictive.	Inspected the evidence and determined that JFrog disclosed its confidentiality practices through various media, such as the company website, its applications, and its contracts. JFrog notified the impacted customers whenever a disclosed confidentiality practice was discontinued or changed to be less restrictive.	No deviations noted.
79	The Company's privacy policy, which fully discloses the type of personal information the Company may collect, as well as how the Company may use this information, is available on JFrog's website.	Inspected the company website and privacy policies, and determined that JFrog's privacy policy was available on its website and fully disclosed the type of information the company may collect from the JFrog application, as well as how JFrog may use this information.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
11	A description of the JFrog system and its boundaries is documented and communicated through the JFrog website.	Inspected screenshots from the internal portal and JFrog Cloud Architecture document and determined that a description of the JFrog system and its boundaries was documented and communicated to JFrog employees within the internal portal and to customers through the JFrog website.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
14	Changes impacting customers are communicated to them through release notes posted to the portal, while internal employees receive notifications via JFrog's internal portal or other applicable methods of internal communication.	Inspected a screenshot of release notes published on the JFrog external portal and emails that were sent to the company employees and determined that changes impacting customers were communicated to them through release notes posted to the portal, while internal employees receive notifications via JFrog's internal portal or other applicable methods of internal communication.	No deviations noted.
19	Based on the Company's escalation procedures and SLA notification thresholds, service interruptions are communicated to customers via email.	Inspected screenshots of the service interruption email that was sent to customers and a screenshot of the internal status page and determined that based on the company's escalation procedures and SLA notification thresholds, service interruptions were communicated to customers via email.	No deviations noted.
20	Response time to customer issues is defined in the SLA. The SLA is communicated to customers via the JFrog website.	Inspected the evidence and determined that response time to customer issues was defined in the SLA. The SLA was communicated to customers via the JFrog website.	No deviations noted.
68	Upon customer request, at the conclusion of a contractual agreement, JFrog will dispose of customer confidential information.	Inspected the evidence and determined the upon customer request, at the conclusion of a contractual agreement, JFrog disposed of customer confidential information.	No deviations noted.
71	JFrog discloses its confidentiality practices through various media, such as the Company website, its applications, and its contracts. JFrog notifies the impacted customers whenever a disclosed confidentiality practice is discontinued or changed to be less restrictive.	Inspected the evidence and determined that JFrog disclosed its confidentiality practices through various media, such as the company website, its applications, and its contracts. JFrog notified the impacted customers whenever a disclosed confidentiality practice was discontinued or changed to be less restrictive.	No deviations noted.
79	The Company's privacy policy, which fully discloses the type of personal information the Company may	Inspected the company website and privacy policies and determined that JFrog's privacy policy was available on its website and fully disclosed the type of information	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	collect, as well as how the Company may use this information, is available on JFrog's website.	the company may collect from the JFrog application, as well as how JFrog may use this information.	

Risk Assessment

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
15	A comprehensive risk assessment is periodically performed to identify and evaluate changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives. As part of this process, threats to system security are identified and evaluated, and the risk(s) from these threats are formally assessed. The process is documented and maintained.	Obtained and reviewed the risk assessment evidence and determined that a risk assessment process was carried out.	No deviations noted.
16	Key JFrog stakeholders evaluate threats and risks, also through internal audit, internal controls and risk review, which is presented to the audit committee, which takes place on a semiannual basis. The audit committee minutes and actions are documented in written form.	Inspected the risk assessment meeting minutes and an invitation and determined that Key JFrog stakeholders evaluated threats and risks during risk assessment meetings, which took place on a semiannual basis.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The Board meets on a quarterly basis. The Board meeting has a fixed agenda that includes, as applicable (1) financial (2) HR (3) security (4) business update (5) Marketing and Sales (6) other	Inspected an agenda example and invitations and determined that the board met on a quarterly basis. The board meeting had a fixed agenda.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	matters (management discussion) (7) updates from the Board's committees		
2	The Board's Committees (Audit, Compensation and Nominating Governance) meet quarterly to discuss a preset agenda and to evaluate threats and risks during risk assessment meetings according to each respective committee's charter.	Inspected an agenda example and invitations and determined that the Board's Committees met on a quarterly basis. The Board's Committees meeting had a fixed agenda.	No deviations noted.
3	The executive team meets at least on a monthly basis, in order to evaluate risks and threats and discuss, inter alia, security and non-compliance issues and address them.	Inspected an agenda example and invitations and determined that the management team met on a weekly basis. The management meeting had a fixed agenda.	No deviations noted.
15	A comprehensive risk assessment is periodically performed to identify and evaluate changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives. As part of this process, threats to system security are identified and evaluated, and the risk(s) from these threats are formally assessed. The process is documented and maintained.	Obtained and reviewed the risk assessment evidence and determined that a risk assessment process was carried out.	No deviations noted.
16	Key JFrog stakeholders evaluate threats and risks, also through internal audit, internal controls and risk review, which is presented to the audit committee, which takes place on a semiannual basis. The audit committee minutes and actions are documented in written form.	Inspected the risk assessment meeting minutes and an invitation and determined that Key JFrog stakeholders evaluated threats and risks during risk assessment meetings, which took place on a semiannual basis.	No deviations noted.
17	On an annual basis, JFrog assesses the risks that vendors and business partners (as well as the vendors and business partners of said) represent to the achievement of the Company's objectives.	Inspected the evidence and determined that on an annual basis, JFrog assessed the risks that vendors and business partners represented to the achievement of the Company's objectives.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The Board meets on a quarterly basis. The Board meeting has a fixed agenda that includes, as applicable (1) financial (2) HR (3) security (4) business update (5) Marketing and Sales (6) other matters (management discussion) (7) updates from the Board's committees	Inspected an agenda example and invitations and determined that the board met on a quarterly basis. The board meeting had a fixed agenda.	No deviations noted.
2	The Board's Committees (Audit, Compensation and Nominating Governance) meet quarterly to discuss a preset agenda and to evaluate threats and risks during risk assessment meetings according to each respective committee's charter.	Inspected an agenda example and invitations and determined that the Board's Committees met on a quarterly basis. The Board's Committees meeting had a fixed agenda.	No deviations noted.
3	The executive team meets at least on a monthly basis, in order to evaluate risks and threats and discuss, inter alia, security and non-compliance issues and address them.	Inspected an agenda example and invitations and determined that the management team met on a weekly basis. The management meeting had a fixed agenda.	No deviations noted.
15	A comprehensive risk assessment is periodically performed to identify and evaluate changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives. As part of this process, threats to system security are identified and evaluated, and the risk(s) from these threats are formally assessed. The process is documented and maintained.	Obtained and reviewed the risk assessment evidence and determined that a risk assessment process was carried out.	No deviations noted.
16	Key JFrog stakeholders evaluate threats and risks, also through internal audit, internal controls and risk review, which is presented to the audit committee, which takes place on a semiannual basis. The audit	Inspected the risk assessment meeting minutes and an invitation and determined that Key JFrog stakeholders evaluated threats and risks during risk assessment meetings, which took place on a semiannual basis.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	committee minutes and actions are documented in written form.		
17	On an annual basis, JFrog assesses the risks that vendors and business partners (as well as the vendors and business partners of said) represent to the achievement of the Company's objectives.	Inspected the evidence and determined that on an annual basis, JFrog assessed the risks that vendors and business partners represented to the achievement of the Company's objectives.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	The Board's Committees (Audit, Compensation and Nominating Governance) meet quarterly to discuss a preset agenda and to evaluate threats and risks during risk assessment meetings according to each respective committee's charter.	Inspected an agenda example and invitations and determined that the Board's Committees met on a quarterly basis. The Board's Committees meeting had a fixed agenda.	No deviations noted.

Monitoring Activities

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
19	Based on the Company's escalation procedures and SLA notification thresholds, service interruptions are communicated to customers via email.	Inspected screenshots of the service interruption email that was sent to customers and a screenshot of the internal status page and determined that based on the company's escalation procedures and SLA notification thresholds, service interruptions were communicated to customers via email.	No deviations noted.
21	Issues are reported to the Support department via the customer support portal, a dedicated email, or by phone.	Inspected a screenshot of the customer support portal and determined that issues were reported to the Support department via the customer support portal, a dedicated email, or by phone.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
23	JFrog's customer support procedures are designed to provide end-to-end support for diagnosing and triaging issues arising in production. Moreover, quarterly meetings are convened to report major open issues to the Management team.	Inspected the evidence and determined that JFrog's customer support procedures were designed to provide end-to-end support for diagnosing and triaging issues in production.	No deviations noted.
61	JFrog uses a suite of monitoring tools to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules within internal wiki. The notifications are reviewed and processed according to their level of urgency. The Management team regularly monitors progress with respect to JFrog Service processes. Analyses of root causes are performed through various tools and meetings. To prevent future occurrences, corrective measures are communicated to relevant groups through monitor tools.	<p>Inspected the evidence and determined that JFrog used a suite of monitoring tools to monitor its service. Alerts were sent to relevant stakeholders based on pre-defined rules within the internal wiki. The notifications were reviewed and processed according to their level of urgency.</p> <p>Inspected the evidence and determined that the Management team regularly monitored progress with respect to JFrog Service processes. Analysis of root causes was performed through various tools and meetings. To prevent future occurrences, corrective measures were communicated to relevant groups through email and meetings.</p>	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
19	Based on the Company's escalation procedures and SLA notification thresholds, service interruptions are communicated to customers via email.	Inspected screenshots of the service interruption email that was sent to customers and a screenshot of the internal status page and determined that based on the company's escalation procedures and SLA notification thresholds, service interruptions were communicated to customers via email.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
21	Issues are reported to the Support department via the customer support portal, a dedicated email, or by phone.	Inspected a screenshot of the customer support portal and determined that issues were reported to the Support department via the customer support portal, a dedicated email, or by phone.	No deviations noted.
23	JFrog's customer support procedures are designed to provide end-to-end support for diagnosing and triaging issues arising in production. Moreover, quarterly meetings are convened to report major open issues to the Management team.	Inspected the evidence and determined that JFrog's customer support procedures were designed to provide end-to-end support for diagnosing and triaging issues in production.	No deviations noted.
61	JFrog uses a suite of monitoring tools to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules within internal wiki. The notifications are reviewed and processed according to their level of urgency. The Management team regularly monitors progress with respect to JFrog Service processes. Analyses of root causes are performed through various tools and meetings. To prevent future occurrences, corrective measures are communicated to relevant groups through monitor tools.	<p>Inspected the evidence and determined that JFrog used a suite of monitoring tools to monitor its service. Alerts were sent to relevant stakeholders based on pre-defined rules within the internal wiki. The notifications were reviewed and processed according to their level of urgency.</p> <p>Inspected the evidence and determined that the Management team regularly monitored progress with respect to JFrog Service processes. Analysis of root causes was performed through various tools and meetings. To prevent future occurrences, corrective measures were communicated to relevant groups through email and meetings.</p>	No deviations noted.
76	An automatically generated log entry is produced after every access to a JFrog-hosted environment or database.	Inspected the evidence and determined that an automatically generated log entry was produced after access to JFrog-hosted environment or database.	No deviations noted.

Control Activities

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
15	A comprehensive risk assessment is periodically performed to identify and evaluate changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives. As part of this process, threats to system security are identified and evaluated, and the risk(s) from these threats are formally assessed. The process is documented and maintained.	Obtained and reviewed the risk assessment evidence and determined that a risk assessment process was carried out.	No deviations noted.
16	Key JFrog stakeholders evaluate threats and risks, also through internal audit, internal controls and risk review, which is presented to the audit committee, which takes place on a semiannual basis. The audit committee minutes and actions are documented in written form.	Inspected the risk assessment meeting minutes and an invitation and determined that Key JFrog stakeholders evaluated threats and risks during risk assessment meetings, which took place on a semiannual basis.	No deviations noted.
17	On an annual basis, JFrog assesses the risks that vendors and business partners (as well as the vendors and business partners of said) represent to the achievement of the Company's objectives.	Inspected the evidence and determined that on an annual basis, JFrog assessed the risks that vendors and business partners represented to the achievement of the Company's objectives.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
15	A comprehensive risk assessment is periodically performed to identify and evaluate changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives. As part of this process, threats to system	Obtained and reviewed the risk assessment evidence and determined that a risk assessment process was carried out.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	security are identified and evaluated, and the risk(s) from these threats are formally assessed. The process is documented and maintained.		
17	On an annual basis, JFrog assesses the risks that vendors and business partners (as well as the vendors and business partners of said) represent to the achievement of the Company's objectives.	Inspected the evidence and determined that on an annual basis, JFrog assessed the risks that vendors and business partners represented to the achievement of the Company's objectives.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
5	JFrog documented an organization chart is approved by the Chief Executive Officer (CEO) and reviewed annually by management.	Inspected the JFrog organization's chart and determined that an organizational chart was documented. Management authorities and reporting hierarchy were clearly defined.	No deviations noted.
6	Responsibility and accountability for developing and maintaining these are assigned to relevant personnel.	Inspected a sample of policies and determined that they were assigned to the relevant personnel and approved on an annual basis by the management team.	No deviations noted.

Logical and Physical Access Controls

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
24	Access to system resources is protected through a combination of firewalls, VPNs, native operating system security mechanisms, access controls, database management system security mechanisms, and application controls.	Inspected the evidence and determined that the access to system resources was protected through a combination of firewalls, VPNs, native operating system security, database management system security, application controls and intrusion detection monitoring software.	No deviations noted.
25	Users are identified through the use of a user ID/password combination using the Company's	Inspected the password configuration policy for the Active Directory and determined that users were	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	identity management system. Where applicable, strong password configuration settings are enabled to ensure (1) a minimum password length, (2) a limit on the number of attempts to enter a password before the user ID is suspended, and (3) password complexity.	identified through the use of a user ID/password combination using the Company's identity management system. Where applicable, strong password configuration settings were enabled to ensure (1) a minimum password length, (2) a limit on the number of attempts to enter a password before the user ID is suspended, and (3) password complexity.	
26	Access to GCP is restricted to authorized individuals and is performed using a two-factors authentication method.	Inspected the GCP user list and configuration and determined that access to the GCP was restricted to authorized individuals and was performed using a two-factor authentication method.	No deviations noted.
27	Access to the Azure platform is restricted to authorized individuals and is performed using a two-factors authentication method.	Inspected the Azure user list and configuration and determined that access to the Azure platform was restricted to authorized individuals and was performed using a two-factor authentication method.	No deviations noted.
28	Access to the AWS is restricted to authorized individuals and is performed using a two-factors authentication method.	Inspected the AWS user list and configuration and determined that access to the AWS platform was restricted to authorized individuals and was performed using a two-factor authentication method.	No deviations noted.
30	Access to the production environment is restricted to authorized personnel. Access is accomplished via a unique account with one-time access token.	Inspected the list of users with access to the production environment and determined that access was restricted to authorized personnel using a time limited token.	No deviations noted.
31	User access is reviewed on a quarterly basis and adjusted based on the ongoing policy of providing only the permissions required to fulfill an employee's role in the Company.	Inspected screenshots of the user access review documentation and the ticket that was managed for a quarterly review and determined that user access was reviewed on a quarterly basis and adjusted based on the ongoing policy of providing only the permissions required to fulfill an employee's role in the Company.	No deviations noted.
32	The access to the backup and database storage is restricted to authorized individuals.	Inspected the list of users with access to the backup and database storage and determined that the access to the	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		backup and database storage was restricted to authorized individuals.	
33	Permission to access the version control, build, and change management tools is restricted to authorized personnel and is granted through personal identity permissions to the SSO via 2FA. After, the user accesses the production environment via a one-time unique token.	Inspected the list of users with access to the different tools and a screenshot of MFA configuration and determined that permission to access the version control, build, and change management tools was restricted to authorized personnel and was granted through a two-factor authentication process.	No deviations noted.
36	New employees are granted access to relevant environments following a notification from HR to the IT team. Permission credentials depend on a given employee's department and role.	Inspected the evidence and determined that new employees were granted access to relevant environments following a notification from HR to the IT Team.	No deviations noted.
65	Customers' sensitive data is encrypted within the JFrog application.	Inspected the evidence and determined that customers' password were encrypted within the JFrog application.	No deviations noted.
73	JFrog customers are restricted to their own web interface environment (server) and do not have access to view data in other Company environments.	Inspected the evidence and determined that JFrog customers were restricted to their own web interface environment and did not have access to view data in other company environments.	No deviations noted.
76	An automatically generated log entry is produced after every access to a JFrog-hosted environment or database.	Inspected the evidence and determined that an automatically generated log entry was produced after access to JFrog-hosted environment or database.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
31	User access is reviewed on a quarterly basis and adjusted based on the ongoing policy of providing only the permissions required to fulfill an employee's role in the Company.	Inspected screenshots of the user access review documentation and the ticket that was managed for a quarterly review and determined that user access was reviewed on a quarterly basis and adjusted based on the	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		ongoing policy of providing only the permissions required to fulfill an employee's role in the Company.	
36	New employees are granted access to relevant environments following a notification from HR to the IT team. Permission credentials depend on a given employee's department and role.	Inspected the evidence and determined that new employees were granted access to relevant environments following a notification from HR to the IT Team.	No deviations noted.
39	Upon an employee's notification of job termination by their direct manager, user accounts are disabled on or deleted automatically from JFrog's production platform, applications, and databases.	Inspected the evidence and determined that upon an employee's notification of job termination by their direct manager, user accounts were disabled on or deleted from JFrog's production platform, applications, and databases.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
31	User access is reviewed on a quarterly basis and adjusted based on the ongoing policy of providing only the permissions required to fulfill an employee's role in the Company.	Inspected screenshots of the user access review documentation and the ticket that was managed for a quarterly review and determined that user access was reviewed on a quarterly basis and adjusted based on the ongoing policy of providing only the permissions required to fulfill an employee's role in the Company.	No deviations noted.
36	New employees are granted access to relevant environments following a notification from HR to the IT team. Permission credentials depend on a given employee's department and role.	Inspected the evidence and determined that new employees were granted access to relevant environments following a notification from HR to the IT Team.	No deviations noted.
39	Upon an employee's notification of job termination by their direct manager, user accounts are disabled on or deleted automatically from JFrog's production platform, applications, and databases.	Inspected the evidence and determined that upon an employee's notification of job termination by their direct manager, user accounts were disabled on or deleted from JFrog's production platform, applications, and databases.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and made available to the Company's employees through JFrog's internal portal.	Inspected the policies and procedures of the company and a screenshot of the company internal portal and determined that policies and procedures were documented, reviewed and approved on an annual basis by the management team and are made available to JFrog employees.	No deviations noted.
34	Physical access to the Company's offices is restricted to authorized personnel. Permissions to grant access are restricted to the office manager and the authorized designees.	Inspected the Physical policy and determined that physical access was restricted to authorized personnel.	No deviations noted.
35	JFrog visitors are accompanied while on Company premises.	Inspected the Physical policy and determined that visitors were accompanied while on premises.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and made available to the Company's employees through JFrog's internal portal.	Inspected the policies and procedures of the company and a screenshot of the company internal portal and determined that policies and procedures were documented, reviewed and approved on an annual basis by the management team and are made available to JFrog employees.	No deviations noted.
34	Physical access to the Company's offices is restricted to authorized personnel. Permissions to grant access are restricted to the office manager and the authorized designees.	Inspected the Physical policy and determined that physical access was restricted to authorized personnel.	No deviations noted.
35	JFrog visitors are accompanied while on Company premises.	Inspected the Physical policy and determined that visitors were accompanied while on premises.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
3	The executive team meets at least on a monthly basis, in order to evaluate risks and threats and discuss, inter alia, security and non-compliance issues and address them.	Inspected an agenda example and invitations and determined that the management team met on a weekly basis. The management meeting had a fixed agenda.	No deviations noted.
37	Single sign-on (SSO) is used for identity and access management (IAM) that enables users to securely authenticate with multiple applications and websites by logging with one set of credentials. The application relies on a trusted third party to verify the users.	Inspected the and determined that single sign-on was used for identity and access management that enables users to securely authenticate with multiple applications and websites by logging with one set of credentials.	No deviations noted.
41	Penetration tests include procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own.	Inspected the penetration test report and determined that it was performed on an annual basis and included procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own.	No deviations noted.
66	To maintain the levels of system confidentiality that conform with the Company's confidentiality commitments, third-party infrastructure providers sign confidentiality agreements with JFrog.	Inspected the evidence and determined that to maintain the levels of system confidentiality that conform with the Company's confidentiality commitments, third-party infrastructure providers signed confidentiality agreements with JFrog.	No deviations noted.
67	Logical access to stored data is restricted to application and database administrators. Data is stored in encrypted format using software supporting the advanced encryption standard (AES). Access permissions are reviewed on an annual basis.	Inspected the evidence and determined that logical access to stored data was restricted to application and database administrators. Data was stored in encrypted format using software supporting the advanced encryption standard. Access permissions were reviewed on an annual basis.	No deviations noted.
70	Confidentiality agreement is disclaimed as it relates to contracts with infrastructure third party providers in accordance with JFrog security policy.	Inspected the evidence and determined that the confidentiality agreement was disclaimed as it relates to	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		contracts with infrastructure third-party providers in accordance with JFrog security policy.	
72	The enterprise requires a minimum of AES 256-bit level encryption for data at rest and secures production data containers, using server-side encryption.	Inspected the evidence and determined that the enterprise required a minimum of AES 256-bit level encryption for data at rest and secures production data containers, using server-side encryption.	No deviations noted.
73	JFrog customers are restricted to their own web interface environment (server) and do not have access to view data in other Company environments.	Inspected the evidence and determined that JFrog customers were restricted to their own web interface environment and did not have access to view data in other company environments.	No deviations noted.
74	Encryption between JFrog customers and the JFrog application is enabled using best industry standards and practices.	Inspected a screenshot of the TLS certificate and determined that the encryption between JFrog customers and the JFrog application was enabled.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
26	Access to GCP is restricted to authorized individuals and is performed using a two-factors authentication method.	Inspected the GCP user list and configuration and determined that access to the GCP was restricted to authorized individuals and was performed using a two-factor authentication method.	No deviations noted.
27	Access to the Azure platform is restricted to authorized individuals and is performed using a two-factors authentication method.	Inspected the Azure user list and configuration and determined that access to the Azure platform was restricted to authorized individuals and was performed using a two-factor authentication method.	No deviations noted.
28	Access to the AWS is restricted to authorized individuals and is performed using a two-factors authentication method.	Inspected the AWS user list and configuration and determined that access to the AWS platform was restricted to authorized individuals and was performed using a two-factor authentication method.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
30	Access to the production environment is restricted to authorized personnel. Access is accomplished via a unique account with one-time access token.	Inspected the list of users with access to the production environment and determined that access was restricted to authorized personnel using a time limited token.	No deviations noted.
37	Single sign-on (SSO) is used for identity and access management (IAM) that enables users to securely authenticate with multiple applications and websites by logging with one set of credentials. The application relies on a trusted third party to verify the users.	Inspected the and determined that single sign-on was used for identity and access management that enables users to securely authenticate with multiple applications and websites by logging with one set of credentials.	No deviations noted.
40	To ensure another layer of protection to the Company's data, JFrog maintains a data loss prevention (DLP) solution.	Inspected the evidence and determined that JFrog maintained a data loss prevention solution.	No deviations noted.
73	JFrog customers are restricted to their own web interface environment (server) and do not have access to view data in other Company environments.	Inspected the evidence and determined that JFrog customers were restricted to their own web interface environment and did not have access to view data in other company environments.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
38	Memory storage of JFrog's operational devices (i.e., workstations and laptops) is encrypted by automated software to ensure the safety of sensitive information. Access to, exchange of, and extraction from memory storage is allowed only to registered and authorized Company devices.	Inspected the evidence and determined that memory storage of JFrog's operational devices was encrypted by automated software to ensure the safety of sensitive information.	No deviations noted.
40	To ensure another layer of protection to the Company's data, JFrog maintains a data loss prevention (DLP) solution.	Inspected the evidence and determined that JFrog maintained a data loss prevention solution.	No deviations noted.
41	Penetration tests include procedures to prevent customers, groups of individuals, or other entities	Inspected the penetration test report and determined that it was performed on an annual basis and included	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	from accessing confidential information other than their own.	procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own.	
45	All Company's laptops are centrally managed. Security settings are hardened and cannot be changed by users. When deficiencies are discovered, automatic alerts and remediation actions are triggered.	Inspected the evidence and determined that company laptops were centrally managed and that security settings were hardened.	No deviations noted.
46	The EDR provides an immediate, scan less solution for comprehensive vulnerability assessment, management and prioritization for IT analysts. All data is encrypted at transit.	Inspected the evidence and determined that the EDR provided a solution for vulnerability assessment for the IT analysts and data was encrypted in transit.	No deviations noted.

System Operations

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
12	Formal information security policies for the principles and processes within the organization are developed and communicated so that personnel understand JFrog's objectives and commitments. The policies are reviewed annually, updated as needed, and approved by JFrog Management team.	Inspected the JFrog's security policy and determined that formal information security policies for the principles and processes within the organization were developed and communicated so that personnel understand JFrog's objectives and commitments. The policies were reviewed annually, updated as needed and approved by the JFrog Management team.	No deviations noted.
44	Operations personnel follow defined protocols for evaluating reported events. Security-related events are assigned to the Security group - CSO Office for evaluation, resolution, and escalation.	Inspected the evidence and determined that operations personnel followed defined protocols for evaluating reported events.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
38	Memory storage of JFrog's operational devices (i.e., workstations and laptops) is encrypted by automated software to ensure the safety of sensitive information. Access to, exchange of, and extraction from memory storage is allowed only to registered and authorized Company devices.	Inspected the evidence and determined that memory storage of JFrog's operational devices was encrypted by automated software to ensure the safety of sensitive information.	No deviations noted.
41	Penetration tests include procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own.	Inspected the penetration test report and determined that it was performed on an annual basis and included procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own.	No deviations noted.
42	Vulnerability scans to detect potential security breaches are performed using external tools on the code.	Inspected the evidence and determined that vulnerability scans to detect potential security breaches were performed using external tools.	No deviations noted.
45	All Company's laptops are centrally managed. Security settings are hardened and cannot be changed by users. When deficiencies are discovered, automatic alerts and remediation actions are triggered.	Inspected the evidence and determined that company laptops were centrally managed and that security settings were hardened.	No deviations noted.
46	The EDR provides an immediate, scan less solution for comprehensive vulnerability assessment, management and prioritization for IT analysts. All data is encrypted at transit.	Inspected the evidence and determined that the EDR provided a solution for vulnerability assessment for the IT analysts and data was encrypted in transit.	No deviations noted.
61	JFrog uses a suite of monitoring tools to monitor its service. Alerts are sent to relevant stakeholders based on pre-defined rules within internal wiki. The notifications are reviewed and processed according to their level of urgency. The Management team	Inspected the evidence and determined that JFrog used a suite of monitoring tools to monitor its service. Alerts were sent to relevant stakeholders based on pre-defined rules within the internal wiki. The notifications	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	regularly monitors progress with respect to JFrog Service processes. Analyses of root causes are performed through various tools and meetings. To prevent future occurrences, corrective measures are communicated to relevant groups through monitor tools.	were reviewed and processed according to their level of urgency. Inspected the evidence and determined that the Management team regularly monitored progress with respect to JFrog Service processes. Analysis of root causes was performed through various tools and meetings. To prevent future occurrences, corrective measures were communicated to relevant groups through email and meetings.	

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
44	Operations personnel follow defined protocols for evaluating reported events. Security-related events are assigned to the Security group - CSO Office for evaluation, resolution, and escalation.	Inspected the evidence and determined that operations personnel followed defined protocols for evaluating reported events.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
44	Operations personnel follow defined protocols for evaluating reported events. Security-related events are assigned to the Security group - CSO Office for evaluation, resolution, and escalation.	Inspected the evidence and determined that operations personnel followed defined protocols for evaluating reported events.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
44	Operations personnel follow defined protocols for evaluating reported events. Security-related events are assigned to the Security group - CSO Office for evaluation, resolution, and escalation.	Inspected the evidence and determined that operations personnel followed defined protocols for evaluating reported events.	No deviations noted.
68	Upon customer request, at the conclusion of a contractual agreement, JFrog will dispose of customer confidential information.	Inspected the evidence and determined the upon customer request, at the conclusion of a contractual agreement, JFrog disposed of customer confidential information.	No deviations noted.
71	JFrog discloses its confidentiality practices through various media, such as the Company website, its applications, and its contracts. JFrog notifies the impacted customers whenever a disclosed confidentiality practice is discontinued or changed to be less restrictive.	Inspected the evidence and determined that JFrog disclosed its confidentiality practices through various media, such as the company website, its applications, and its contracts. JFrog notified the impacted customers whenever a disclosed confidentiality practice was discontinued or changed to be less restrictive.	No deviations noted.

Change Management

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The Board meets on a quarterly basis. The Board meeting has a fixed agenda that includes, as applicable (1) financial (2) HR (3) security (4) business update (5) Marketing and Sales (6) other matters (management discussion) (7) updates from the Board's committees	Inspected an agenda example and invitations and determined that the board met on a quarterly basis. The board meeting had a fixed agenda.	No deviations noted.
3	The executive team meets at least on a monthly basis, in order to evaluate risks and threats and discuss, inter alia, security and non-compliance issues and address them.	Inspected an agenda example and invitations and determined that the management team met on a weekly basis. The management meeting had a fixed agenda.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
47	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are documented and approved by the Management team within the Company's Change Management application. Change management tickets are prioritized and labeled based on development phase and urgency.	Inspected the evidence and determined that changes were documented and approved by the Management team within the change management application. Change Management tickets were prioritized and labeled based on development phase and urgency.	No deviations noted.
48	Permission to approve code review and merges are restricted to authorized personnel and are required as part of the change management process in order to deploy a version to production.	Inspected the evidence and determined that permission to approve merge requests was restricted to authorized personnel.	No deviations noted.
50	A code review process is enforced throughout the continuous integration process.	Inspected the evidence and determined that a code review process was enforced throughout the continuous integration process.	No deviations noted.
51	Builds are transferred to a staging environment by an automated tool after successfully passing the testing pipeline.	Inspected the evidence and determined that tested builds were transferred to a staging environment by an automated tool.	No deviations noted.
52	Developers have restricted permissions to the production environment based on predefined policies.	Inspected the evidence and determined that developers had restricted permissions based on predefined policies.	No deviations noted.
53	A log containing all test results is available for review by QA and R&D team leaders. The R&D team holds weekly meetings to discuss open bugs, as recorded in the change management tool.	Inspected meeting invitations and determined that the R&D team held weekly meetings to discuss open bugs, as recorded in the bug tracking system.	No deviations noted.
54	Sprint meetings take place every two weeks. There are also planning meetings where tasks are discussed and prioritized, as well as daily standup status meetings.	Inspected sprint meeting invitations and determined that sprint meetings took place every two weeks.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
55	Each released build must pass unit and integration tests using the orchestrator tool. The DevOps team deploys changes to the production environment. Through the use of an orchestrator coverage tool, every merge request undergoes unit testing and integration testing.	Inspected the evidence and determined that successful unit tests and integration tests were performed using the orchestrator coverage tool. Inspected the evidence and determined that the Operations team deployed changes to the production environment through the use of an orchestrator coverage tool.	No deviations noted.
56	Notifications of test failures are sent to key JFrog personnel. Each is documented in the change management tool.	Inspected the evidence and determined that notifications of test failures were sent to key JFrog personnel. Each was documented in the change management tool.	No deviations noted.
57	Appropriate JFrog personnel are notified when new versions are deployed to production.	Inspected the evidence and determined that appropriate JFrog personnel were notified when new versions were deployed to production.	No deviations noted.

Risk Mitigation

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
2	The Board's Committees (Audit, Compensation and Nominating Governance) meet quarterly to discuss a preset agenda and to evaluate threats and risks during risk assessment meetings according to each respective committee's charter.	Inspected an agenda example and invitations and determined that the Board's Committees met on a quarterly basis. The Board's Committees meeting had a fixed agenda.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The Board meets on a quarterly basis. The Board meeting has a fixed agenda that includes, as applicable (1) financial (2) HR (3) security (4) business update (5) Marketing and Sales (6) other matters (management discussion) (7) updates from the Board's committees	Inspected an agenda example and invitations and determined that the board met on a quarterly basis. The board meeting had a fixed agenda.	No deviations noted.
2	The Board's Committees (Audit, Compensation and Nominating Governance) meet quarterly to discuss a preset agenda and to evaluate threats and risks during risk assessment meetings according to each respective committee's charter.	Inspected an agenda example and invitations and determined that the Board's Committees met on a quarterly basis. The Board's Committees meeting had a fixed agenda.	No deviations noted.
3	The executive team meets at least on a monthly basis, in order to evaluate risks and threats and discuss, inter alia, security and non-compliance issues and address them.	Inspected an agenda example and invitations and determined that the management team met on a weekly basis. The management meeting had a fixed agenda.	No deviations noted.
9	New employees are required to sign a standard employment agreement and an NDA addressing business practices, conflicts of interest, confidentiality, and intellectual property.	For the selected employees, inspected the NDA's signed and determined that they addressed the business practices, conflicts of interest, security and confidentiality clauses.	No deviations noted.
15	A comprehensive risk assessment is periodically performed to identify and evaluate changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives. As part of this process, threats to system security are identified and evaluated, and the risk(s) from these threats are formally assessed. The process is documented and maintained.	Obtained and reviewed the risk assessment evidence and determined that a risk assessment process was carried out.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
16	Key JFrog stakeholders evaluate threats and risks, also through internal audit, internal controls and risk review, which is presented to the audit committee, which takes place on a semiannual basis. The audit committee minutes and actions are documented in written form.	Inspected the risk assessment meeting minutes and an invitation and determined that Key JFrog stakeholders evaluated threats and risks during risk assessment meetings, which took place on a semiannual basis.	No deviations noted.
17	On an annual basis, JFrog assesses the risks that vendors and business partners (as well as the vendors and business partners of said) represent to the achievement of the Company's objectives.	Inspected the evidence and determined that on an annual basis, JFrog assessed the risks that vendors and business partners represented to the achievement of the Company's objectives.	No deviations noted.
69	Related party and vendor systems are subject to review as part of the vendor risk management process. When available and applicable, attestation (i.e., SOC 2) reports are obtained and evaluated.	Inspected the evidence and determined that related party and vendor systems were subject to review as part of the vendor risk management process. When available and applicable, attestation (i.e., SOC 2) reports were obtained.	No deviations noted.
77	New vendors, business partners, and subcontractors are required to sign a standard NDA agreement, which contains clauses regarding confidentiality and the use of intellectual property.	Inspected samples of signed confidentiality agreements and determined that new vendors, business partners, and subcontractors were required to sign a standard NDA agreement, which contains clauses regarding confidentiality and the use of intellectual property. on internal SLA.	No deviations noted.

Availability

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
58	The applications' database is backed up automatically on a daily basis. Weekly full-system and daily incremental backups are also performed.	Inspected the evidence and determined that the databases were backed up automatically on a daily basis and weekly full-system and daily incremental backups were also performed.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
60	Database servers have multi-availability zones where applicable. Full backups on these are performed weekly; incremental backups on a daily basis.	Inspected the evidence and determined that database servers had multizone availability, where applicable and that full backups on these were performed weekly; incremental backups on a daily basis.	No deviations noted.
64	JFrog's production environment is located in multi regions. To maintain high availability standards, the regions have replica in a different availability zone.	Inspected the evidence and determined that JFrog's production environment was located in multiple availability zones.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
58	The applications' database is backed up automatically on a daily basis. Weekly full-system and daily incremental backups are also performed.	Inspected the evidence and determined that the databases were backed up automatically on a daily basis and weekly full-system and daily incremental backups were also performed.	No deviations noted.
60	Database servers have multi-availability zones where applicable. Full backups on these are performed weekly; incremental backups on a daily basis.	Inspected the evidence and determined that database servers had multizone availability, where applicable and that full backups on these were performed weekly; incremental backups on a daily basis.	No deviations noted.
62	JFrog has developed a Disaster Recovery Plan (DRP) that sets forth the means and manner by which it can continue to provide critical services in the event of disaster.	Inspected the disaster recovery plan and determined that JFrog had developed a Disaster Recovery Plan (DRP) that set forth the means and manner by which it can continue to provide critical services in the event of disaster.	No deviations noted.
64	JFrog's production environment is located in multi regions. To maintain high availability standards, the regions have replica in a different availability zone.	Inspected the evidence and determined that JFrog's production environment was located in multiple availability zones.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
58	The applications' database is backed up automatically on a daily basis. Weekly full-system and daily incremental backups are also performed.	Inspected the evidence and determined that the databases were backed up automatically on a daily basis and weekly full-system and daily incremental backups were also performed.	No deviations noted.
62	JFrog has developed a Disaster Recovery Plan (DRP) that sets forth the means and manner by which it can continue to provide critical services in the event of disaster.	Inspected the disaster recovery plan and determined that JFrog had developed a Disaster Recovery Plan (DRP) that set forth the means and manner by which it can continue to provide critical services in the event of disaster.	No deviations noted.
63	DR restore tests are performed on an annual basis.	Inspected the evidence and determined that restore tests were performed on an annual basis.	No deviations noted.

Confidentiality

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
1	The Board meets on a quarterly basis. The Board meeting has a fixed agenda that includes, as applicable (1) financial (2) HR (3) security (4) business update (5) Marketing and Sales (6) other matters (management discussion) (7) updates from the Board's committees	Inspected an agenda example and invitations and determined that the board met on a quarterly basis. The board meeting had a fixed agenda.	No deviations noted.
3	The executive team meets at least on a monthly basis, in order to evaluate risks and threats and discuss, inter alia, security and non-compliance issues and address them.	Inspected an agenda example and invitations and determined that the management team met on a weekly basis. The management meeting had a fixed agenda.	No deviations noted.
12	Formal information security policies for the principles and processes within the organization are developed and communicated so that personnel understand JFrog's objectives and commitments.	Inspected the JFrog's security policy and determined that formal information security policies for the principles and processes within the organization were developed and communicated so that personnel	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	The policies are reviewed annually, updated as needed, and approved by JFrog Management team.	understand JFrog's objectives and commitments. The policies were reviewed annually, updated as needed and approved by the JFrog Management team.	
25	Users are identified through the use of a user ID/password combination using the Company's identity management system. Where applicable, strong password configuration settings are enabled to ensure (1) a minimum password length, (2) a limit on the number of attempts to enter a password before the user ID is suspended, and (3) password complexity.	Inspected the password configuration policy for the Active Directory and determined that users were identified through the use of a user ID/password combination using the Company's identity management system. Where applicable, strong password configuration settings were enabled to ensure (1) a minimum password length, (2) a limit on the number of attempts to enter a password before the user ID is suspended, and (3) password complexity.	No deviations noted.
30	Access to the production environment is restricted to authorized personnel. Access is accomplished via a unique account with one-time access token.	Inspected the list of users with access to the production environment and determined that access was restricted to authorized personnel using a time limited token.	No deviations noted.
33	Permission to access the version control, build, and change management tools is restricted to authorized personnel and is granted through personal identity permissions to the SSO via 2FA. After, the user accesses the production environment via a one-time unique token.	Inspected the list of users with access to the different tools and a screenshot of MFA configuration and determined that permission to access the version control, build, and change management tools was restricted to authorized personnel and was granted through a two-factor authentication process.	No deviations noted.
35	JFrog visitors are accompanied while on Company premises.	Inspected the Physical policy and determined that visitors were accompanied while on premises.	No deviations noted.
43	JFrog maintains employee training programs to promote awareness of JFrog's information security and privacy requirements as defined in JFrog's Security Awareness Training Policy.	Inspected the evidence and determined that JFrog maintained employee training programs to promote awareness of JFrog's information security and privacy requirements as defined in JFrog's Security Awareness Training policy.	No deviations noted.
65	Customers' sensitive data is encrypted within the JFrog application.	Inspected the evidence and determined that customers' password were encrypted within the JFrog application.	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
66	To maintain the levels of system confidentiality that conform with the Company's confidentiality commitments, third-party infrastructure providers sign confidentiality agreements with JFrog.	Inspected the evidence and determined that to maintain the levels of system confidentiality that conform with the Company's confidentiality commitments, third-party infrastructure providers signed confidentiality agreements with JFrog.	No deviations noted.
67	Logical access to stored data is restricted to application and database administrators. Data is stored in encrypted format using software supporting the advanced encryption standard (AES). Access permissions are reviewed on an annual basis.	Inspected the evidence and determined that logical access to stored data was restricted to application and database administrators. Data was stored in encrypted format using software supporting the advanced encryption standard. Access permissions were reviewed on an annual basis.	No deviations noted.
70	Confidentiality agreement is disclaimed as it relates to contracts with infrastructure third party providers in accordance with JFrog security policy.	Inspected the evidence and determined that the confidentiality agreement was disclaimed as it relates to contracts with infrastructure third-party providers in accordance with JFrog security policy.	No deviations noted.
72	The enterprise requires a minimum of AES 256-bit level encryption for data at rest and secures production data containers, using server-side encryption.	Inspected the evidence and determined that the enterprise required a minimum of AES 256-bit level encryption for data at rest and secures production data containers, using server-side encryption.	No deviations noted.
74	Encryption between JFrog customers and the JFrog application is enabled using best industry standards and practices.	Inspected a screenshot of the TLS certificate and determined that the encryption between JFrog customers and the JFrog application was enabled.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
4	Policies and procedures are documented, reviewed, and approved on an annual basis by the management team and made available to the Company's employees through JFrog's internal portal.	Inspected the policies and procedures of the company and a screenshot of the company internal portal and determined that policies and procedures were documented, reviewed and approved on an annual	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		basis by the management team and are made available to JFrog employees.	

Privacy

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

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
78	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies. The names of such person or group and their responsibilities are defined.	Inspected the information security policies and internal company communications and determined that responsibility and accountability was assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the entity's privacy policies.	No deviations noted.
79	The Company's privacy policy, which fully discloses the type of personal information the Company may collect, as well as how the Company may use this information, is available on JFrog's website.	Inspected the company website and privacy policies and determined that JFrog's privacy policy was available on its website and fully disclosed the type of information the company may collect from the JFrog application, as well as how JFrog may use this information.	No deviations noted.
80	JFrog's privacy policy is reviewed and updated by management on at least an annual.	Inspected the company privacy policy and company communications and determined that the privacy policy was reviewed and updated by management on an annual basis.	No deviations noted.

P2.0: Privacy Criteria Related to Choice and Consent

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
81	Customers sign on contracts that address how their personal information will be handled.	Inspected signed customer contracts, the company's data processing addendum, and website, and determined that the contracts addressed how customer personal information is to be handled.	No deviations noted.
82	Personal information is collected consistent with JFrog's objectives related to privacy.	Inspected the company website, privacy policy, and contracts, and determined that personal information was collected consistent with JFrog's objectives related to privacy.	No deviations noted.

P3.0: Privacy Criteria Related to Collection

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
81	Customers sign on contracts that address how their personal information will be handled.	Inspected signed customer contracts, the company's data processing addendum, and website, and determined that the contracts addressed how customer personal information is to be handled.	No deviations noted.
82	Personal information is collected consistent with JFrog's objectives related to privacy.	Inspected the company website, privacy policy, and contracts, and determined that personal information was collected consistent with JFrog's objectives related to privacy.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
81	Customers sign on contracts that address how their personal information will be handled.	Inspected signed customer contracts, the company's data processing addendum, and website, and determined that the contracts addressed how customer personal information is to be handled.	No deviations noted.

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

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
83	Access to personal information in databases is restricted to authorized JFrog employees, including help desk personnel.	Inspected the access list to the company databases and determined that the access to personal information in databases was restricted to authorized JFrog personnel.	No deviations noted.
84	JFrog retains personal information consistent with the Company's objectives related to privacy.	Inspected contracts, data subject requests, and the privacy policy, and determined that personal information was retained for no longer than necessary to fulfill the entity's objectives related to privacy.	No deviations noted.
85	JFrog securely disposes of personal information in keeping with the Company's objectives related to privacy.	Inspected contracts, data subject requests, and the privacy policy, and determined that JFrog securely disposed of personal information to meet the entity's objectives related to privacy.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
81	Customers sign on contracts that address how their personal information will be handled.	Inspected signed customer contracts, the company's data processing addendum, and website, and determined that the contracts addressed how customer personal information is to be handled.	No deviations noted.
84	JFrog retains personal information consistent with the Company's objectives related to privacy.	Inspected contracts, data subject requests, and the privacy policy, and determined that personal	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		information was retained for no longer than necessary to fulfill the entity's objectives related to privacy.	

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
68	Upon customer request, at the conclusion of a contractual agreement, JFrog will dispose of customer confidential information.	Inspected the evidence and determined the upon customer request, at the conclusion of a contractual agreement, JFrog disposed of customer confidential information.	No deviations noted.

P5.0: Privacy Criteria Related to Access

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
86	JFrog grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides electronic copies of that information, or erase it. If access is denied, data subjects are informed of the denial and, as required, the reason for such denial.	Inspected the company privacy policy, contracts, the customer account editing functionality, data subject requests, and the data subject request handling tool, and determined that JFrog granted identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provided physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy.	No deviations noted.
87	JFrog corrects, amends, or appends personal information based on information provided by data subjects. If a request for correction is denied, data subjects are informed of the denial and the reason for such denial.	Inspected the company privacy policy, contracts, the customer account editing functionality, data subject requests, the data subject request handling tool, and marketing communications, and determined that JFrog corrected or amended personal information based on	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		information provided by data subjects and communicated such information to third parties, as committed or required, to meet the entity's objectives related to privacy.	

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

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

P6.0: Privacy Criteria Related to Disclosure and Notification

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

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

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
89	JFrog creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to third parties.	Inspected the list of third-party sub processors and vendor risk management tool and determined that JFrog had practices in place for maintaining and documenting records of authorized disclosures of personal information to meet the entity's objectives related to privacy.	No deviations noted.
90	JFrog creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information.	Inspected JFrog's incident response plans and incident report, and determined that JFrog created and retained a complete, accurate, and timely record of detected or reported unauthorized disclosures of personal information.	No deviations noted.
91	Privacy commitments are obtained from vendors and other third parties who have access to personal information. On a periodic and as-needed basis, JFrog assesses compliance on the part of those parties and, if necessary, takes corrective action.	Inspected the company's data processing agreements and vendor risk management tool and determined that JFrog obtained privacy commitments from vendors and other third parties who had access to the company's personal information. JFrog assessed those parties' compliance on a periodic and as-needed basis and took corrective action, if necessary.	No deviations noted.
92	JFrog obtains commitments from vendors and other third parties with access to personal information to notify the Company in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures.	Inspected the company's data processing agreements with vendors and determined that JFrog obtained commitments from vendors and other third parties to notify the company in the event of actual or suspected unauthorized disclosures of information.	No deviations noted.
94	JFrog provides data subjects with an accounting of the personal information held and, upon their request, disclosure of their personal information held.	Inspected the JFrog privacy policy, website, and contracts, and determined that data subjects were provided with an accounting of personal information held and disclosure of the data subjects' personal	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
		information, upon the data subjects' request, to meet the company's objectives related to privacy.	

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

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

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
81	Customers sign on contracts that address how their personal information will be handled.	Inspected signed customer contracts, the company's data processing addendum, and website, and determined that the contracts addressed how customer personal information is to be handled.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
91	Privacy commitments are obtained from vendors and other third parties who have access to personal information. On a periodic and as-needed basis, JFrog assesses compliance on the part of those parties and, if necessary, takes corrective action.	Inspected the company's data processing agreements and vendor risk management tool and determined that JFrog obtained privacy commitments from vendors and other third parties who had access to the company's personal information. JFrog assessed those parties' compliance on a periodic and as-needed basis and took corrective action, if necessary.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
92	JFrog obtains commitments from vendors and other third parties with access to personal information to notify the Company in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures.	Inspected the company's data processing agreements with vendors and determined that JFrog obtained commitments from vendors and other third parties to notify the company in the event of actual or suspected unauthorized disclosures of information.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
93	JFrog provides notification of breaches and incidents to affected data subjects, regulators, and others.	Inspected JFrog's incident response plans and incident report and determined that JFrog provided notifications of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	No deviations noted.

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
83	Access to personal information in databases is restricted to authorized JFrog employees, including help desk personnel.	Inspected the access list to the company databases and determined that the access to personal information in databases was restricted to authorized JFrog personnel.	No deviations noted.
83	Access to personal information in databases is restricted to authorized JFrog employees, including help desk personnel.	Inspected the access list to the company databases and determined that the access to personal information in databases was restricted to authorized JFrog personnel.	No deviations noted.
94	JFrog provides data subjects with an accounting of the personal information held and, upon their	Inspected the JFrog privacy policy, website, and contracts, and determined that data subjects were	No deviations noted.

Description of Criteria, Controls, Tests and Results of Tests

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
	request, disclosure of their personal information held.	provided with an accounting of personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the company's objectives related to privacy.	

P7.0: Privacy Criteria Related to Quality

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
95	JFrog collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the Company's objectives related to privacy.	Inspected the company privacy policy, company communications, and data subject requests, and determined that JFrog had processes in place for maintaining accurate and complete personal information for the purposes for which it is to be used.	No deviations noted.

P8.0: Privacy Criteria Related to Monitoring and Enforcement

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

#	Controls specified by the Company	Testing performed by the auditor	Results of Testing
96	JFrog utilizes a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others, and periodically monitors compliance to satisfy the Company's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	Inspected the JFrog privacy policy, contracts, customer support communications, and data subject communications, and determined that the company had implemented a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy.	No deviations noted.
