



System and Organization Controls 3 Report

Management's Report of its Assertions on the Effectiveness of Its Controls over the Recorded Future Intelligence Platform System Based on the Trust Service Criteria for Security

For the period June 1, 2021 to May 31, 2022



Contents

1. INDEPENDENT SERVICE AUDITOR'S REPORT	1
2. ASSERTION OF RECORDED FUTURE, INC.'S MANAGEMENT ..	3
ATTACHMENT A	4
Description of the Boundaries of Recorded Future's Intelligence Platform System	4
Company Overview	4
Platform Overview	4
Components of the System Used to Provide the Services	5
Infrastructure and Software	6
Data	6
People	6
Procedures	9
Complementary Subservice Organization Controls	10
ATTACHMENT B	11
The Principal Service Commitments and System Requirements ..	11

1. Independent Service Auditor's Report

To the management of Recorded Future, Inc.:

Scope

We have examined Recorded Future, Inc.'s (Recorded Future) accompanying assertion titled "Assertion of Recorded Future, Inc.'s Management" (assertion) that the controls within Recorded Future's Intelligence Platform System (system) were effective throughout the period June 1, 2021, to May 31, 2022 to provide reasonable assurance that Recorded Future's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

For Recorded Future's core offerings, Recorded Future uses Amazon Web Services (AWS) (subservice organization) to provide data center hosting, customer support, developer support and data curation services. The description of the boundaries of the system (Attachment A) indicates that Recorded Future's controls can provide reasonable assurance that certain service commitments and system requirements, based on the applicable trust services criteria, can be achieved only if AWS's controls, assumed in the design of Recorded Future's controls, are suitably designed and operating effectively along with related controls at the service organization. The description of the boundaries of the system presents Recorded Future's system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS. Our examination does not extend to the services provided by AWS and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period June 1, 2021, to May 31, 2022.

Service Organization's Responsibilities

Recorded Future 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 Recorded Future's service commitments and system requirements were achieved. Recorded Future has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Recorded Future is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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 management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Recorded Future's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether the controls within the system were effective to achieve Recorded Future's service commitments and system requirements based on the applicable trust services criteria.

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

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

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

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

Opinion

In our opinion, management's assertion that the controls within Recorded Future's Intelligence Platform System were effective throughout the period June 1, 2021, to May 31, 2022, to provide reasonable assurance that Recorded Future's service commitments and system requirements were achieved based on the applicable trust services is fairly stated, in all material respects.

Restricted Use

This report is intended solely for the information and use of Recorded Future, user entities of Recorded Future's Intelligence Platform System during some or all of the period June 1, 2021, to May 31, 2022, and prospective user entities and is not intended to be, and should not be, used by anyone other than these specified parties.



September 16, 2022



2. Assertion of Recorded Future, Inc's Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Recorded Future's Intelligence Platform System (system) throughout the period June 1, 2021, to May 31, 2022, to provide reasonable assurance that Recorded Future's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.


For Recorded Future's core offerings, Recorded Future uses Amazon Web Services (AWS) to provide data center hosting, customer support, developer support and data curation services. The boundaries of the System presented in Attachment A includes only the controls of Recorded Future and excludes controls of AWS. However, the description of the boundaries of the system does present the types of controls Recorded Future assumes have been implemented, suitability designed, and operating effectively at AWS. Certain trust services criteria can be met only if AWS's controls assumed in the design of Recorded Future's controls are suitability designed and operating effectively along the related controls at Recorded Future. However, we perform annual due diligence procedures for third-party subservice providers and based on the procedures performed, nothing has been identified that prevents us from achieving our specified service commitments and system requirements.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2021, to May 31, 2022, to provide reasonable assurance that Recorded Future's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Recorded Future's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

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

We assert that the controls within the system were effective throughout the period June 1, 2021, to May 31, 2022, to provide reasonable assurance Recorded Future's service commitments and system requirements were achieved based on the applicable trust services criteria.

Recorded Future, Inc.

DocuSigned by:

A7D644BE7C84492...
Scott Almeida | CFO
9/16/2022

Attachment A

Description of the Boundaries of Recorded Future's Intelligence Platform System

Company Overview

Recorded Future, Inc. (Recorded Future) delivers security intelligence to amplify the effectiveness of security and IT teams in reducing exposure by uncovering unknown threats and informing better, faster decisions. Working to provide a singular view of digital, brand, and third-party risk, the Recorded Future Intelligence Platform system (the "Platform") provides proactive and predictive intelligence, analyzing data from open, proprietary, and aggregated customer-provided sources. Recorded Future arms threat analysts, vulnerability management teams, security operations centers, and incident responders with context-rich, actionable intelligence in real time that is ready for integration across the security ecosystem.

Platform Overview

Recorded Future provides offerings built upon an all-in-one Intelligence Platform, and the Platform consists of processes ranging from source collection and processing to analysis and reporting. The Platform involves many technologies building blocks, e.g., text search, data visualization, natural language processing, and entity extraction, to name a few.

At the core of this technology is the patented Intelligence Engine. This is the data-mining innovation that lets the Platform understand what events have been reported on and place them in time and space.

The Intelligence Engine works by separating collected, analyzed online media and documents, and their content from their subject – the "canonical" entities and events. Documents contain references to these entities and events, and these references are used to rank entities and events based on; 1) the number of references to them, 2) the credibility of the documents or document sources containing these references, and 3) several other factors (e.g., co-occurrence of different events and entities in the same or in related documents is also used for ranking).

Recorded Future also conducts analysis on the "time and space" dimension of documents – references to when and where an event has taken place, or even when and where it will take place – since many documents refer to events expected to take place in the future.

The combination of automatic event/entity/time/location extraction, implicit link analysis for novel ranking algorithms, and statistical prediction models forms the basis for Recorded Future's Intelligence Engine and core expertise.

Recorded Future is headquartered in Somerville, Massachusetts, USA with an additional hub in Gothenburg, Sweden. Recorded Future has additional offices in Virginia, London, United Kingdom, Singapore, Dubai and Tokyo.

Recorded Future is focused on providing security intelligence to allow organizations to quickly identify, prioritize, and action threats with confidence. This approach empowers organizations to prioritize workflows based on risk, make confident decisions using external context, alert proactively on relevant threats, implement targeted blocking at security controls, and maximize value of existing security investments.

The primary target groups for the Platform are the Threat Intelligence, Security Operations Center (SOC) and Incident Response, Brand Protection, Vulnerability Management, Third-Party Risk and Geopolitical Risk. Recorded Future works with clients from all sectors, both private and government. Direct clients typically fall in the Fortune 2000 sector. Recorded Future also works with partners or Managed Security Service Providers (MSSPs) who in turn work with smaller clients not hosting their own threat analysis teams or SOC's.

The product is either used as a standalone product or integrated to Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Governance Risk and Compliance (GRC), or other IT and security systems.

Components of the System Used to Provide the Services

Recorded Future is a universal security intelligence solution that centralizes information from across our proprietary data sources, and industry-leading research from our Insikt Group, enabling organizations to use intelligence-driven security to proactively defend itself against cyberattacks.

Recorded Future provides analysts deep visibility into their threat landscape by analyzing and visualizing cyber threats, even across numerous foreign languages (NLP capabilities), with our vast open-source intelligence (OSINT) and proprietary data repository. Analysts receive real-time alerts when relevant cyber threats to their organization appear.

Recorded Future believes that machine learning combined with human expertise is the superior approach for creating real-time, relevant security intelligence to effectively reduce risk at scale. Our vast data is sourced from across the open, deep, and dark web to produce insightful and actionable intelligence data to act as a force multiplier. By reducing the manual collection and processing of intelligence data, Recorded Future frees up precious security analyst and engineering manpower, allowing them to be making decisions where they are most needed instead of curating data.

Recorded Future's use cases include:

- Security Operations and Incident Response
- Threat Intelligence
- Brand Protection
- Vulnerability Management
- Third-Party Risk
- Business Continuity and Geopolitical Risk

Recorded Future's solution can be delivered via:

- i. The Recorded Future Portal
- ii. The Recorded Future Browser Extension
- iii. Recorded Future Connect Technology
- iv. The Recorded Future Mobile App

Infrastructure and Software

Recorded Future is a web application that is hosted at Amazon Web Services (AWS). Recorded Future hosts its entire infrastructure in a Virtual Private Cloud (VPC) on AWS. The network is divided into several subnets, and everything is replicated across multiple availability zones. Only the nodes in the public subnet can be directly accessed from the Internet. All outgoing traffic must pass through NAT-gateways which are placed in the public subnets. The boundaries of the system includes only the controls of Recorded Future and excludes controls at AWS. Controls operated by AWS are not included in the scope of this report. Due diligence procedures are performed on AWS's control environment on an annual basis.

Data

Recorded Future implements and maintains backup, security and business continuity measures that are designed to maintain the security and integrity of customer data. Beyond customer financial information that is securely kept for billing purposes, and user passwords to allow access to the service (for those organizations that are not using single sign on), Recorded Future stores the following customer data:

- Saved queries
- User-generated analyst notes
- Alerts
- Reports
- Lists, including watch lists
- Information collected via our free browser extension (Recorded Future Express)

Recorded Future encrypts and stores this data securely. Recorded Future logs certain user actions. Logs that contain user-provided query data are automatically anonymized and then deleted after 14 days, and all other customer data (including analyst notes) are deleted, or anonymized, as applicable, after the subscription is terminated.

Recorded Future also stores error and event logs and documents from open-source data.

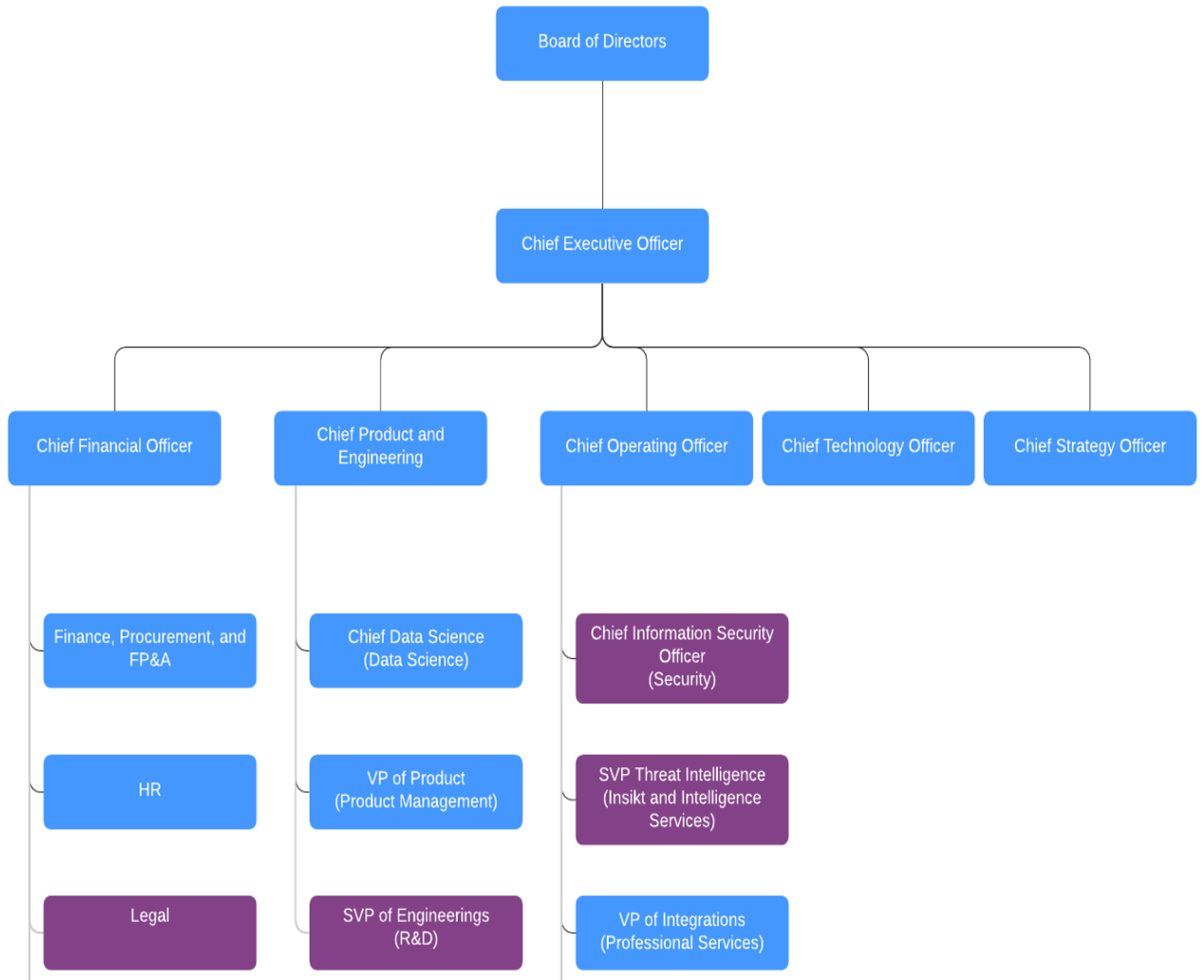
People

Recorded Future has a staff of approximately 850 employees organized in the functional areas described herein. The background of all employees varies, but most have a higher education within the technology field. Job descriptions are available for all roles. Depending on the job description, certifications may be required. Recorded Future obtains references on candidates.

All new hires and current employees are required by law and/or internal policy to complete several checks before they are eligible to begin employment. Depending on location and role, these checks may include identity verification, verifying eligibility to work, and background checks.

Currently, Recorded Future conducts background checks on all employees unless prohibited by local law and/or granted an exemption by the legal department. Recorded Future retains a third-party agency to conduct the screening process and maintaining the corresponding records. The types of screens that may be conducted include but are not limited to: education verification, employment verification for as many as seven years, identity verification, criminal record searches, and a sex offender registry search. Additionally, as appropriate for a position, credit, professional license, and/or state motor vehicle checks.

Recorded Future applies a three-tier interview process at a minimum, which includes prequalification for the job, assessment of the candidates' skills including potential tests when applicable and interviews with the candidates' direct colleagues



CEO: responsible for Recorded Future's strategic direction, finances, key relationships, and operations with a focus on growing the business.

R&D/Engineering: responsible for all aspects of building and maintaining Recorded Future's Platform, including architecting the application, developing new functionality, fixing bugs, testing of all releases, release deployment and monitoring of the live systems. The primary goal of the R&D/Engineering group is to rapidly develop new innovative functionality while ensuring that the application performs to the highest levels.

Operations Team: responsible for monitoring and deploying the system as well as creating and maintaining the Platform on which it is built. Operations also cover third line support for any critical issues as well as focuses on internal security.

Platform Team: builds the underlying framework including databases, indexing operations and optimization as well as API support.

Product Design Team: breaks down the bigger product goals to actual R&D deliverables and designs.

Applications Team: focuses on the development and maintenance of the end user interface.

Analytics Team: focuses on the linguistics and data quality and is responsible for the framework for harvesting sources and breaking down text to Recorded Future's patent-protected data model.

Integrations Team: responsible for the development, quality assurance and availability of Recorded Future's integrations.

Quality Assurance Team: responsible for assuring the quality of the offerings and solutions.

Delivery Management Team: manages new releases, and coordinate with internal stakeholders to ensure successful delivery of the company's offering. The team also oversees the planning and resource allocation necessary for new development.

Professional Services: offers customized services to customers including integration support and API solutions.

Chief of Data Science: responsible for the Data Science Team, and driving key analysis projects, both internal and external. The Data Science Team primarily works with ensuring good data quality for end customers through data cleaning as well as internal and external tools for data management.

Intelligence Services: customer success and ensuring that Recorded Future's customers can successfully deploy and use the product within their organization. Intelligence Services responds to customer issues, trains customers on using the product and collects customer feedback that is used for product management to shape future releases. Intelligence Services also provides analysis services.

Product Management: manages customer, partner and internal requirements and feedback used to shape future product releases. They send notifications on new features and releases and sets the product roadmap.

Threat Intelligence: defines our Threat Intelligence strategy influencing both business and product directions it includes Intelligence Services and Recorded Future's Insikt Group, the company's in-house research team that can provide subject-matter expertise to respond to Recorded Future (and customer) incidents upon request.

Sales: responsible for business development, direct sales, inside sales, pre-sales, partners, account management and sales management.

General & Administrative: includes Finance, Legal, and HR, and is responsible for the planning, organizing, auditing, accounting for and controlling of finances and maintaining contracts. This department also produces financial statements.

Marketing: driving customer subscriptions to Recorded Future. Its primary focus is on new customer acquisition and subscription expansion by refining and communicating Recorded Future's unique value proposition.

Procedures

Recorded Future has developed and documented formal policies and procedures. These policies and procedures have been developed to segregate duties, where possible, and enforce responsibilities based on job functionality. They also serve as guidelines and directions for day-to-day work. Policies and procedures are reviewed periodically, no less than annually, and are updated as necessary.

These procedures and policies are all found on Recorded Future's intranet (Lyra) and included in the Recorded Future Employee Handbook. New employees are trained on these procedures and policies. If any material changes are made, these changes are communicated to all employees. Training for changes is used when warranted.

To maintain the operation of the service, Recorded Future provides the following main services on a continuous basis (24/7):

1. Systems deployment and maintenance;
2. Security administration and auditing;
3. Intrusion detection and incident response;
4. Operations and performance monitoring;
5. Change controls; and
6. Business recovery planning.

Complementary Subservice Organization Controls

Recorded Future’s controls related to the Intelligence Platform system cover only a portion of overall internal controls for each user entity of Recorded Future. Certain service commitments and system requirements can only be achieved if the subservice organization’s controls contemplated in the design of Recorded Future’s controls are suitably designed and operating effectively along with the related controls at Recorded Future. The boundaries of the System presented includes only the controls of Recorded Future and excludes controls of AWS. Controls operated by AWS are not included in the scope of this report. Due diligence procedures are performed on AWS’s control environment on an annual basis.

Subservice Provider	Description of Services Provided	Applicable Trust Services Criteria	Types of controls expected to be in place at the third-party service provider in order to meet the security criteria
Amazon Web Services (AWS)	<ul style="list-style-type: none"> • Data center hosting • Customer support • Developer support • Data curation services 	CC 4.1 CC 5.1 CC 6.4 CC6.6 CC 6.8	Amazon Web Services is responsible for providing cloud infrastructure for hosted systems to reside in and physical security and environmental controls surrounding the physical data center.

Attachment B

The Principal Service Commitments and System Requirements

Recorded Future, designs its processes and procedures to meet its objectives for its Recorded Future, Intelligence Platform System. Those objectives are based on the service commitments that Recorded Future, makes to user entities, the laws and regulations that govern the provision of the Recorded Future, Intelligence Platform System, and the financial, system, operational and compliance requirements that Recorded Future, has established for the services.

Recorded Future, makes certain Security representations to its customers as detailed in the MSA, Service Level Agreements (SLAs) and other Customer agreements, as well as in the description of the service offering provided online and within this report. Security commitments include, but are not limited to, the following:

- Policies and mechanisms within the system to secure and separate Customer Data;
- Regular security assessments of the environment;
- Applicable security trainings and background checks for employees;
- Authorization, testing and approval of changes to the system;
- Environment monitoring and resolution of system incidents; and
- Encryption of certain sensitive information.

Recorded Future, establishes operational requirements that support the achievement of Security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Recorded Future, system policies and procedures, system design documentation and contracts with Customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of these system requirements as they relate to the Recorded Future, Intelligence Platform System.

There were no significant changes to the service organization's system during the period that are relevant to the service organization's service commitments and system requirements.