MFA COMPANIES

SOC 3 REPORT SOFTWARE AS A SERVICE REPORT ON SECURITY PRINCIPLE PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS FOR THE PERIOD JUNE 1, 2018 THROUGH MAY 31, 2019

PREPARED PURSUANT TO SYSTEM AND ORGANIZATION CONTROLS (SOC 2) TYPE 2 EXAMINATION PERFORMED UNDER AT-C 105 AND AT-C 205 RELEVANT TO SECURITY

TABLE OF CONTENTS

Recorded Future Inc.
Somerville, Massachusetts

Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security

To: Recorded Future

Scope

We have examined Recorded Future's accompanying description of its software-as-a-service (SaaS) platform system found in Section III, iii titled Recorded Future's SaaS Platform System Description throughout the period June 1, 2018 to May 31, 2019 based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 1, 2018 to May 31, 2019, to provide reasonable assurance that Recorded Future's service commitments and system requirements were achieved based on the trust services criteria relevant to Security as forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Recorded Future uses subservice organizations, identified in Section IV. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Recorded Future, to achieve Recorded Future's service commitments and system requirements based on the applicable trust services criteria. The description presents Recorded Future's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Recorded Future's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls assumed in the design of Recorded Future'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.

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. In Section II, Recorded Future has provided the accompanying assertion titled Assertion of the Management of Recorded Future about the description and the suitability of design and operating effectiveness of controls stated therein. Recorded Future is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

An examination of 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;
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in section VII of this report.

Opinion

In our opinion, in all material respects—

a. the description presents Recorded Future's SaaS Platform system that was designed and implemented throughout the period June 1, 2018 to May 31, 2019 in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period June 1, 2018 to May 31, 2019 to provide reasonable assurance that Recorded Future's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of Recorded Future's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period June 1, 2018 to May 31, 2019 to provide reasonable assurance that Recorded Future's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Recorded Future's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section VII is intended solely for the information and use of Recorded Future; user entities of Recorded Future's SaaS Platform system during some or all of the period June 1, 2018 to May 31, 2019, business partners of Recorded Future subject to risks arising from interactions with the SaaS Platform system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria; and
- 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 the specified parties.

Moody, Famiglietti & Andronico, LLP

Moody, Famiglietti & Andronico, LLP
Tewksbury, Massachusetts
October 18, 2019

Recorded Future

Assertion of the Management of Recorded Future

We have prepared the accompanying description of Recorded Future's SaaS Platform system titled Recorded Future SaaS Platform Description in Section III, iii throughout the period June 1, 2018 to May 31, 2019 based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*. The description is intended to provide report users with information about the SaaS Platform system that may be useful when assessing the risks arising from interactions with Recorded Future's system, particularly information about system controls that Recorded Future has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

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

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

1) The description presents Recorded Future's SaaS Platform system that was designed and implemented throughout the period June 1, 2018 to May 31, 2019 in accordance with the description criteria.
2) The controls stated in the description were suitably designed throughout the period June 1, 2018 to May 31, 2019 to provide reasonable assurance that Recorded Future's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Recorded Future's controls throughout that period.
3) The controls stated in the description operated effectively throughout the period June 1, 2018 to May 31, 2019 to provide reasonable assurance that Recorded Future's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Recorded Future's controls operated effectively throughout that period.

DocuSigned by:
Scott Almeida
A7D644BE7C84492...

Scott Almeida

Chief Financial Officer

October 18th 2019

III. Overview of Operations

i. Company Overview

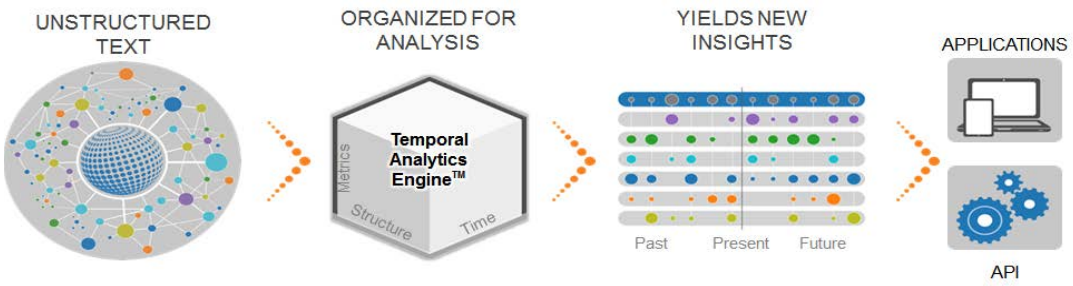
Recorded Future is a real-time cyber threat intelligence companies that analyzes the web and enables customers to forecast cyber threats, conduct intelligence research, increase business competitiveness, and monitor the horizon for situational awareness. Recorded Future provides products built upon an all-in-one Web intelligence platform, and the platform consists of processes ranging from source collection and processing to analysis and reporting. The platform involves many technology 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 Web Intelligence Engine. This is the data-mining innovation that lets Recorded Future's products understand what events have been reported on the Web, and place them in time and space.

The Web 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 actually 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 Web Intelligence Engine and core expertise. Following is a pictorial description of the process.

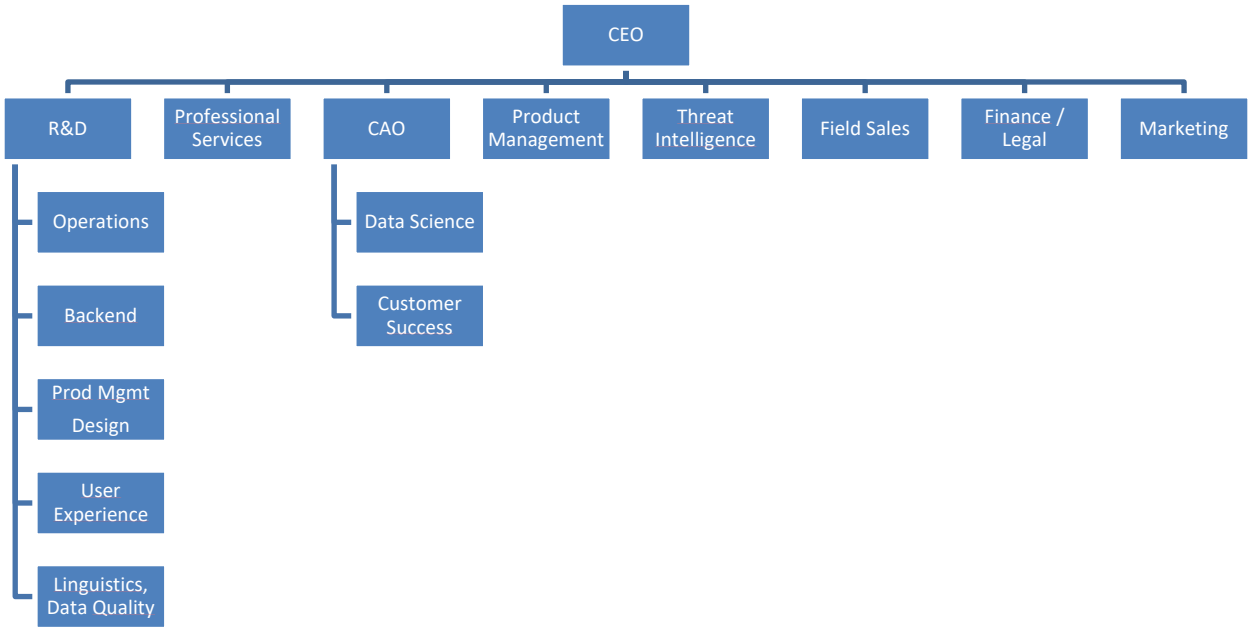


Recorded Future is headquartered in Somerville, MA, USA with two additional hubs in Arlington, Virginia, USA and Gothenburg, Sweden. Recorded Future has additional offices in London, UK, Singapore and Tokyo.

The primary target groups for Recorded Future are the Threat Intelligence team and the Security Operations Center (SOC). Recorded Future works with clients from all sectors, both private and government. Direct clients typically fall in the Fortune 2000 sector. The Company 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) and IT systems.

ii. Organization Chart



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

R&D/Engineering: R&D/Engineering is 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:** The Operations Team is 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.
- **Backend:** Backend builds the underlying framework including databases, indexing operations and optimization as well as API support.
- **Product Management/Design:** The Product Management / Design Team breaks down the bigger product goals to actual R&D deliverables and designs.
- **User Experience:** User Experience focuses on the development and maintenance of the end user interface.
- **Linguistics and Data Quality**: The Linguistics and Data Quality Team is responsible for the framework for harvesting sources and breaking down text to Recorded Future's patented data model.

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

CAO: The Chief Analytics Officer is responsible for driving key analysis projects, both internal and external.

- **Data Science:** 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.
- **Customer Success:** The primary focus for Customer Success is ensuring that Recorded Future's customers can successfully deploy and use the product within their organization. Customer Success responds to customer issues, trains customers on using the product and collects customer

feedback that is used for Product Management to shape future releases. Customer Success also provides analysis services.

Product Management: 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: Threat Intelligence defines our Threat Intelligence strategy influencing both business and product directions.

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

Finance/Legal: The Finance / Legal Team is responsible for the planning, organizing, auditing, accounting for and controlling of finances and maintaining contracts. This department also produces financial statements.

Marketing: Marketing is responsible for 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.

iii. Recorded Future SaaS Platform System Description

Services Provided:

Recorded Future is a universal threat intelligence solution that centralizes information from across the web, our proprietary data sources, and industry-leading research from our Insikt Group, enabling your organization 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 threat 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:

- Threat Analysis and Security Operations: Identify cybersecurity trends, research malware, and monitor your brand;
- Incident Response: Identify data exposure incidents for remediation;
- Vulnerability Management: Identify vulnerabilities and prioritize remediation;
- Risk Analysis: Assess third party's information security posture and identify third parties that have elevated risk to your organization; or
- Fraud: Monitor the dark web and criminal communities for direct mentions of your organization and assets

Recorded Future's solution can be delivered via:

i) The Recorded Future Portal, our graphical user-interface that is accessible via any supported internet browser (incl. Google Chrome, Mozilla Firefox, Edge and Safari). The web interface gives your organization direct access to all of our data, including Intelligence Cards that summarize information and risk on 300 million threat-related entities;

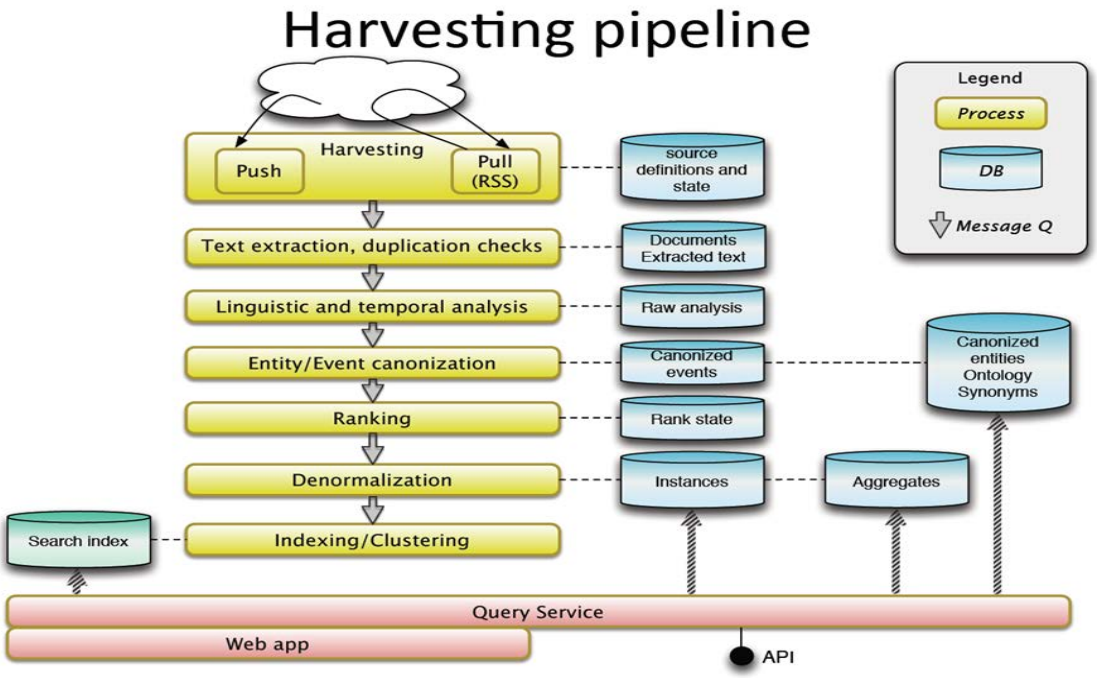
ii) The Recorded Future API, which allows your organization to integrate Recorded Future's data directly into your existing security technologies and workflows; or

iii) The Recorded Future Browser Extension, the browser extension works by scanning the current page for CVEs, Hashes, Domains and IP Addresses and listing them in the extension popup when the user clicks the browser extension icon (located towards the top in the browser menu bar).

iv) The Recorded Future Mobile App, provides access to our Home Screen (incl research from Insikt Group, cyber news, malware trends, and alerts), access to Recorded Future's Intelligence Cards (covering threat actor profiles, IP addresses, hashes, CVEs, domains, and more), and searching for entities with risk scores.

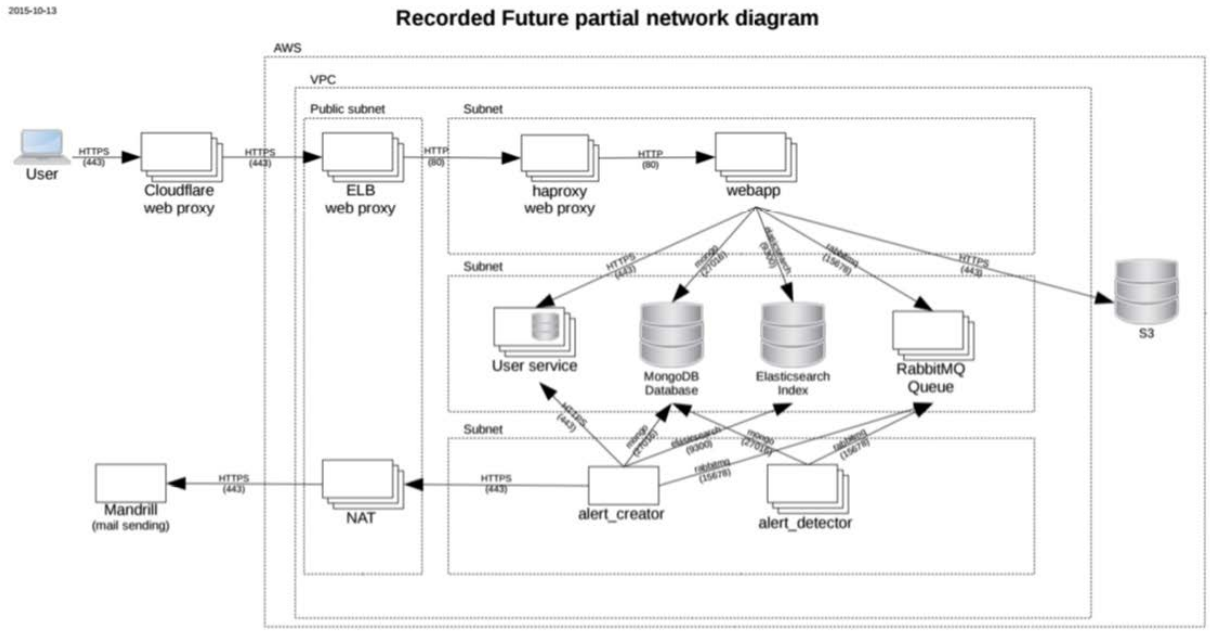
Network Overview:

Recorded Future is a web application that is hosted on AWS (Amazon Web Services). Recorded Future hosts its entire infrastructure in a Virtual Private Cloud (VPC) on Amazon. The network is divided into a number of subnets and everything is replicated across multiple availability zones. Only the nodes in the public subnet can be accessed from the Internet. All outbound traffic from the other subnets must pass through machines in this zone.



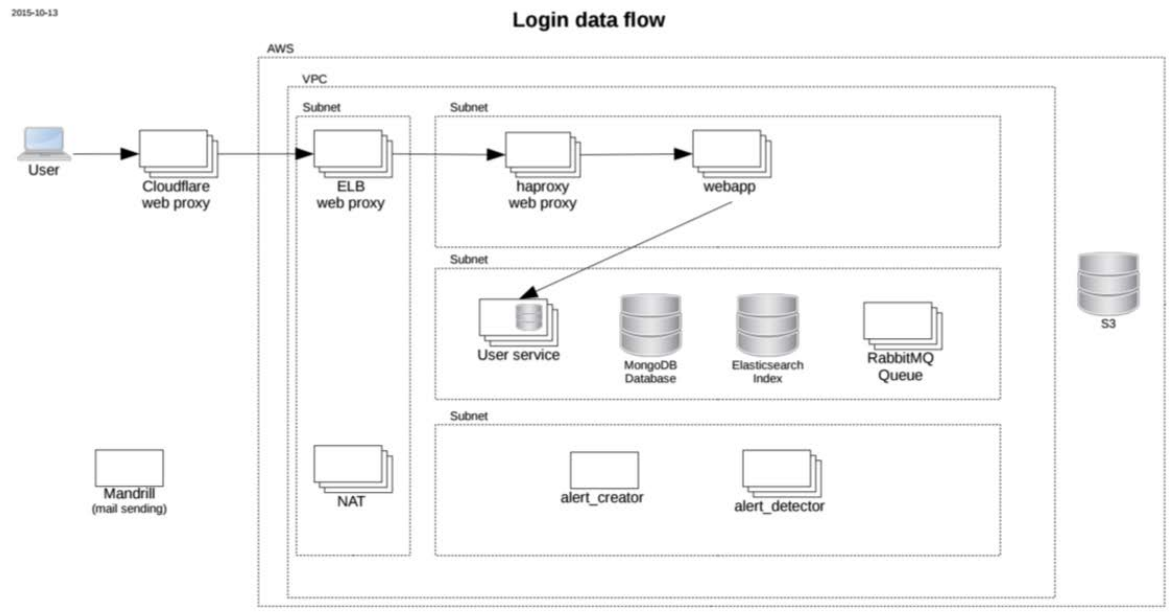
Recorded Future Partial Network Diagram:

The diagram below shows the parts of the system which are directly involved with responding to web requests and generating alerts.



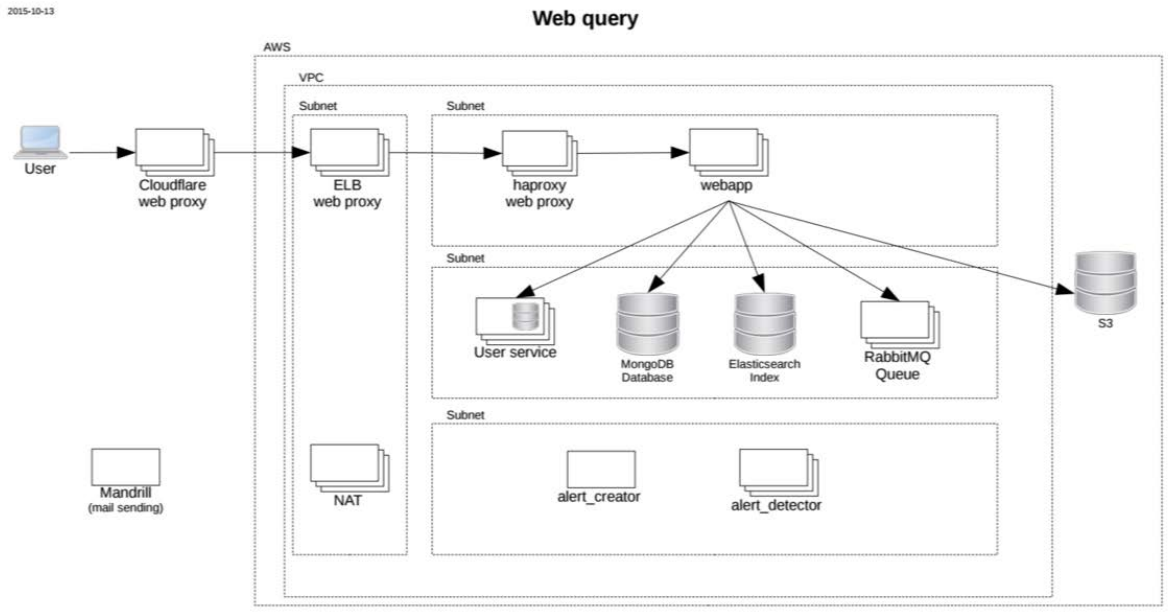
Login Data Flow:

The user's login request is sent to the web application which sends it to the user service for validation. The user service validates the provided credentials. If the authentication is successful, the web application then generates a session cookie which is used for the rest of the session.



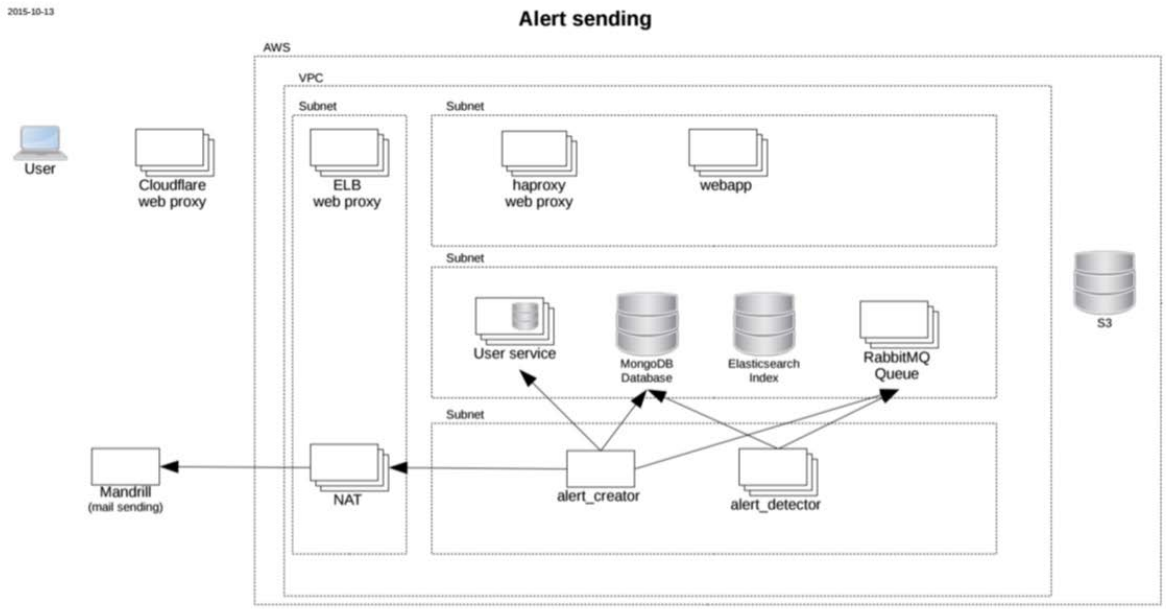
Web Query Flow:

The user browser will include the session cookie in the web request. If needed the web application contacts the user service to check which access rights the user has. The web application will query the database, index and possible S3 to fetch the required data. The web application may also setup a listener on RabbitMQ to listen for new references and other changes.



Alerts:

All configured alerts are stored in an alert collection in the Mongo databases. The alert definition contains an encrypted reference to the user. The alert detector receives all new references via a RabbitMQ queue and checks them against the configured alerts. If it detects a matching reference it sends a message via RabbitMQ, to the alert creator. The alert creator sends the encrypted user reference to the user service in order to get the email addresses the alert should be sent to. The email is generated and sent via Mandrill, an external email sending service.



Amazon Web Services (AWS):

Recorded Future uses Amazon Web Services for hosting its virtual servers and for other key infrastructure services. AWS is a cloud computing platform providing *Infrastructure as a Service* (IaaS) and has been operating since 2006. The primary services used by Recorded Future are:

- Compute
  - Amazon EC2 - provides virtual servers used by Recorded Future for its application servers
  - Auto Scaling - helps you maintain application availability and allows you to scale your Amazon EC2 capacity up or down automatically according to conditions you define.

- Compute (continued)
  - Amazon VPC - lets you provision a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define.
  - Elastic Load balancing -provides load balancing across the application servers
- Storage and Content Delivery
  - Amazon S3 - provides highly reliable and available long-term storage of backups and application server images
  - Amazon EBS - provides persistent block level storage volumes for use with Amazon EC2 instances in the AWS Cloud.
  - Amazon Cloud Front - is a content delivery web service.
- Networking
  - Amazon VPC
  - Amazon Route 53 - is a cloud Domain Name System (DNS) web service.
  - Elastic Load Balancing - provides load balancing across the application servers
- Administration and Security
  - Amazon Identity and Access Management (IAM) - is a web service that helps you securely control access to AWS resources for your users.
  - AWS CloudTrail - is a web service that records AWS API calls for your account and delivers log files to you.
- AWS Support
  - AWS Support

AWS successfully completes annual Service Organization Controls (SOC 2), Type 2 audits. Recorded Future reviews AWS's SOC reports after each audit to ensure it can meet its own Security objectives.

Data:

Recorded Future implements and maintains backup, security and business continuity measures that are designed to maintain the security and integrity of customer data. Recorded Future customer data consists of the following, which is all protected and secured via encryption:

- User info - email and password;
- Analyst Notes
- Queries - both saved and real time; and
- Alerts and reports

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

Operations:

To maintain the operation of the Recorded Future service the Company provides the following main services 24 by 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.

People:

Recorded Future has a staff of approximately 500 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 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.

Recorded Future obtains references on candidates.

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 and are updated as necessary.

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

IV. Relevant Aspects of the Control Environment, Control Activities, Risk Assessment Process, Monitoring Controls, Information and Communication, and Sub-Service Organizations

Control Environment:

The control environment at Recorded Future begins at the highest level. Executive leadership plays an important role in establishing Recorded Future's core values and principles. The organizational structure at Recorded Future produces a framework for planning, executing and controlling business operations. Roles and responsibilities are clearly defined to ensure adequate staffing, efficient operation and segregation of duties. Recorded Future employees are subject to annual reviews and new employees follow a structured on-boarding process to ensure knowledge of processes, systems policies and procedures.

Recorded Future has a Security Management team to review and revise security and privacy related technology and organizational issues.

Control Activities:

Recorded Future management meets regularly to review business plans and results. The Board of Directors meets at least quarterly for a similar in-depth review. Annual goals and objectives guide the review of plans with a focus on financial results. Policies, procedures, and practices exist that ensure business plan directives are carried out across Recorded Future.

Project and service management tools are used across Recorded Future. An online help desk service is used to track client support tickets and requests. All product development activities and release planning is done in accordance with Recorded Future's Release Management processes. This process uses Jira to track development activities, such as scoping, development, testing, acceptance and releases. Internal reviews take place prior to any release is moved to production. Final approval of release functionality is given by the Product Manager. All releases are tested in a staging environment that is an exact replica of the production system. Final approval to go live is given by the Product Manager.

Maintaining Data Security is crucial to Recorded Future. The Information Security Program is reviewed quarterly by the Information Security Team and changes are approved by management. This policy is reviewed and acknowledged annually by all employees. The Information Security Program ensures that access to Recorded Future's systems are restricted only to authorized users, covers the approval process for creating new, modifying and removing existing users, and the communication of security breaches. It also ensures that access to client data is restricted only to authorized persons and details specific steps to

deal with destruction of data and documents, and the roles and responsibilities of Recorded Future's employees and contractors. The Recorded Future employee on-boarding process ensures that all employees and contractors get access to the required systems in accordance with the Information Security Program.

Risk Assessment:

Recorded Future sets annual goals and objectives reviewed and approved by the Board of Directors. Individual and group objectives are set and approved by management. Performance against goals and objectives are regularly reviewed by the Board of Directors and management. Recorded Future undertakes a risk assessment of the following key areas of its software; security and availability. Management re-evaluates this risk assessment at least twice annually, identifying potential areas of risk within business practices and procedures by area of responsibility. Any changes to existing or new controls that are needed to address these risks are then implemented, documented and communicated to all employees.

Operational risks are monitored through regular meeting. Any potential changes to the software or infrastructure that could have an impact upon the key areas of risk are reviewed and extensively tested. Automated tests are used to help identify such risks. All changes to the software and infrastructure are tracked to ensure adequate testing to mitigate risk.

Monitoring:

Recorded Future utilizes automated monitoring systems to provide a high level of service performance and availability. Key operational metrics are monitored, and alarms are configured to notify operational personnel when warning thresholds are crossed on such metrics.

Recorded Future management monitors the quality of the day-to-day service and operational activities including the internal control environment. Continuous team meetings are held within the Engineering department where issues are discussed and reviewed and the Vice President, Engineering ensures that issue resolution is moving adequately.

Servers used by Recorded Future have extensive logging capabilities and are periodically reviewed to check for security breaches. Additionally, server user account lists are regularly reviewed to check that access is only available to those that have business need for such privileges.

Vice President, Engineering ensures that bi-annual risk assessments are conducted and that employee on-boarding procedures are followed.

Recorded Future has a dedicated Information Security Team that monitors the information security program.

Information and Communication:

Recorded Future has documented internal communication policies and procedures to ensure that all employees understand their individual roles and responsibilities concerning controls and to ensure that significant events are communicated in a timely manner. This is all located on the intranet, readily available to all employees for review and readily available to all employees of the Company.

Subservice Organizations The following subservice organizations are used by Recorded Future in the delivery of their application services. *This report does not extend to the controls of the subservice organizations listed below.*	**Description of Services Provided**
Amazon Web Services (AWS)	Recorded Future contracts with AWS for data center hosting (SaaS).
Infinit-O	Recorded Future contracts with Infinit-O for Tier 1 customer support and data curation.
Cloudflare	Recorded Future contracts with Cloudflare for DDoS mitigation and other related security measures.
Atlassian (JIRA & Confluence)	Recorded Future contracts with Atlassian for Project Management and internal corporate communications.
Salesforce	Recorded Future contracts with Salesforce to manage customer and prospect contact and sales information.
Google G-Suite	Recorded Future contracts with G-Suite for internal corporate communication.

Recorded Future has determined that these services operate within acceptable levels of risk. For this report, Recorded Future name has carved out services in the management, service, compute, storage, and infrastructure layers.

Third party access to data:

Recorded Future offers APIs that allow a third-party tool to access data in the system. The customer is responsible for approving these connections. Recorded Future only exposes the API, and access to Recorded Future's systems via an API require authentication.

V. Security Principle

Recorded Future operations are constructed to meet the service requirements for its clients. Internal controls have been established to safeguard these services and are present in the form of the security principle.

Recorded Future has an Information Security Program that is reviewed and updated quarterly by the Security Information Team. The Vice President, Engineering is ultimately responsible for this program. The program is published on the intranet to be available to all employees.

As part of the security review process, the Information Security Team conducts a risk assessment covering new and existing risks and their potential impact upon security. From this risk assessment the Information Security Team communicates any policy updates and activities that need to be undertaken. The Vice President, Engineering is responsible for making these updates and the communication of such updates and activities.

The program contains practices on classifying sensitive data. For such data, the program defines how it should be protected, how access is controlled, and the requirements for destruction and retention. The program also includes procedures on sharing information with third parties.

All employees sign a Non-Disclosure Agreement (NDA) which prescribes the way that confidential information is used, shared and destroyed. This agreement prohibits any disclosures of information and other data to which the employee has access. Business partners are subject to similar NDA's and / or other contractual confidentiality provisions.

Recorded Future has procedures in place to identify, assess and respond to security issues. Weekly meetings are held to discuss any potential issues that arise, to assess the risks posed by these issues and take corrective actions. To ensure that customers understand the system and the security requirements of their users, Recorded Future provides a system description and user control considerations to all its customers upon request to the Customer Success (Intelligence Services) team. Customers can also request support on Recorded Future's third-party hosting service, Amazon Web Services (AWS). The system description outlines the infrastructure, software, people, procedures, data and third-party providers that constitute the "system." The user control considerations describe the controls that must be employed at customer organizations. The information relative to AWS within the Subscription Agreement prescribes

that Recorded Future relies on the AWS's confidentiality practices and controls and that these controls must meet or exceed those of Recorded Future. The necessary steps to report any security issues or breaches follow the support guidelines provided by Recorded Future Customer Success team via the Support site. If any incidents are reported, a ticketing system is used to track the issue through resolution including any actions taken. If at any time Recorded Future makes changes that may affect overall system security, these changes are communicated to the customer.

To ensure access to all systems and infrastructure is restricted only to authorized users, Recorded Future has an on-boarding process that requires approval from line-of-business managers to grant user access and to change user access rights to systems. Thus, to obtain access to customer data, approval is needed from the line-of-business manager. To obtain system administrator privileges, including access to server operating systems, databases, backups and firewalls, approval is needed from Vice President, Engineering. Similarly, Recorded Future has departure procedures that ensure user account terminations occur within 1 business day of notification.

Application and access to operating systems, requires a unique user ID and password combination. Additional security includes the encryption of all user data. Users trying to access the application are locked-out after a number of failed password attempts. Two factor authentications are enforced where applicable. Private/public key pairs are used for application server operating system access. Anti-virus is installed on all application servers where applicable and is configured to run and update daily. Recorded Future maintains and updates a Key Management Policy.

Access to Recorded Future's suite is controlled by encryption keys. As all servers are hosted at AWS, no employee has physical access to any of the infrastructure of the system. To ensure that the controls at AWS are consistent with the security policies, the AWS third-party assurance report is reviewed by Vice President, Engineering as available, but at least annually.

Any security issues are tracked within an ongoing incident system that includes the response and final resolution to the issue. R&D keeps pace with technological changes that may affect system security through a variety of means, including subscriptions, seminars, webinars and regular interactions with other professionals. Any potential policy impairments are discussed at quarterly Information Security Team meetings. The Team also works with legal counsel to keep abreast of practices needed to comply with applicable laws and regulations addressing confidentiality that may affect Recorded Future.

Recorded Future has a Change Management Policy that is reviewed annually. It ensures that only authorized, tested and documented changes are made to the system. It also includes procedures on the authorization and deployment of emergency changes. New versions of the application are thoroughly tested before release, by unit tests, by automated and manual testing.

Recorded Future ensures that personnel responsible for design, development, implementation and operation of its systems are qualified to fulfill their responsibilities. Employee performance is monitored with annual performance reviews. Annual security training is provided to all employees.

VI. User Control Considerations

The security controls and practices of Recorded Future, Inc. are designed with the assumption that complimentary administrative, physical, and technical controls are implemented by client organizations. The application of these specific controls at client organizations is necessary to provide reasonable assurance that the control objectives included in this report are achieved. Clients of Recorded Future need to implement and maintain an internal control structure that provides reasonable assurance that services are performed by Recorded Future in accordance with client instructions.

This section describes controls that should be in operation at client organizations to complement the controls at Recorded Future. The client control considerations presented should not be regarded as a comprehensive list of all controls which should be employed by client organizations. There may be additional controls that would be appropriate which are not identified in this report.

Recorded Future expects clients to implement a certain level of control to ensure a reliable and secure operating environment. These controls include:

General:

- Client is responsible for controlling all output from Recorded Future that is delivered to them.
- Client must inform Recorded Future by emailing support@recordedfuture.com if client primary contact changes.

System Environment:

- Client shall maintain in good working order: equipment, hardware, dedicated access and all software, inclusive of licenses and support services as described within their individual contracts.
- Client is responsible for the acquisition, configuration, monitoring, maintenance and management of all hardware, software, and interfaces at client's location(s), including LAN, computers, software, telecommunications and devices.
- Client is responsible for managing all user accounts and security authorizations they are given to ensure appropriate use of the system.
- Client will appropriately manage all third-party relationships including, but not limited to, any tools interacting with Recorded Future.

System Implementations and Ongoing Support Interactions:

- Client will request and approve all Statements of Work (SOW) prior to a task being executed as applicable for projects and customizations.
- Client is responsible for ensuring the accuracy of all issues and request tickets.
- Client is responsible for notifying Recorded Future of any unauthorized use of any account or any other known suspected breach of security issue.
- Client is responsible for defining business requirements and approval of detailed specifications for all requested changes to their respective systems.
- Client is responsible for ensuring the confidentiality of Recorded Future's intellectual property and sensitive information, including pricing, methodologies and practices
- Recorded Future offers APIs that allow a third-party tool to access data in the system. The customer is responsible for approving these connections. Recorded Future only exposes the API, and access to Recorded Future's systems via an API require authentication.

VII. Information Provided by Service Auditor

This report on policies and procedures placed in operation is intended to provide interested parties with information sufficient to obtain an understanding of those aspects of Recorded Future's control structure policies and procedures that may be relevant to its customers' internal control structure as it relates to their financial statements. This report, when coupled with an understanding of the internal control structure policies and procedures in place at the customers' site, is intended to assist in the assessment of the internal control structure surrounding the information technology and transaction processing functions performed by the Company.

Our examination covered the controls related to the criteria for the security principle set forth in TSP section 100 (2017 *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy*) designed and implemented by Recorded Future to meet the control objectives and did not extend to controls in effect at a client site (i.e., user control considerations), or subservice organizations. The audit was conducted in accordance with assertion standards under Section 101 and the Guide to SOC 2 "*Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy*" of the American Institute of Certified Public Accountants. It is the responsibility of each interested party to evaluate this information in relation to internal control structure policies and procedures in place at the customer site to obtain an understanding of the internal control structure policies and procedures and to assess control risk. Recorded Future and its customers' portions of the internal control structure must be evaluated together. If effective user internal control structure policies and procedures are not in place, the Recorded Future control structure policies and procedures may not compensate for such weaknesses.

Our examination included: (a) inquiry of appropriate management, supervisory, and staff personnel; (b) inspection of documents and records on a sample basis; (c) observation of activities and operations; and (d) attribute testing for a sample of transactions or records. Our tests of controls were performed for the period of June 1, 2018 through May 31, 2019 and were applied to those control activities relating to trust criteria specified by Recorded Future's management.

The description of the trust criteria designed and placed in operation to meet the criteria is the responsibility of Recorded Future's management. Our responsibility is to express an opinion on whether the controls are operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the trust criteria, as specified by Recorded Future, was achieved throughout the period of June 1, 2018 through May 31, 2019.

Control Environment Elements:

The control environment represents the collective effect of various factors on establishing, enhancing, or mitigating the effectiveness of specific policies and procedures. In addition to the tests of control design described below, our procedures included tests of relevant elements of the control environment. Such tests included inquiry of appropriate management, supervisory, and staff personnel, and inspection of documents and records.

Testing of Operating Effectiveness:

Our tests of the effectiveness of control structure policies and procedures included such tests as we considered necessary in the circumstances to evaluate whether those policies and procedures, and the extent of compliance with them, is sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period June 1, 2018 through May 31, 2019. Our tests of the operational effectiveness of control structure policies and procedures were designed to cover the period June 1, 2018 through May 31, 2019, for each of the control policies and procedures listed below, which are designed to achieve the specific control objectives listed therein. In selecting particular tests of the operational effectiveness of control structure policies and procedures, we considered: (a) the nature of the items being tested, (b) the types and competence of available evidential matter, (c) the nature of the audit objectives to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test. The information included in Recorded Future's Relevant Aspects of the Control Environment, Control Activities, Risk Assessment Process, Monitoring Controls, Information and Communication and Subservice Organizations was not used in planning our examination, although an understanding of the environment and operations was obtained using alternate methods prior to initiating fieldwork.

Description of Testing Procedures Performed:

As part of the examination of the Company's internal controls, MFA performed a variety of procedures that provided the basis for understanding the framework for controls. The tests were to determine whether the presented controls supporting the operations were in place and operating effectively for the period of June 1, 2018 through May 31, 2019.

1 Highwood Drive, Tewksbury, MA 01876

www.themfacompanies.com