hackerone

HackerOne Inc.

Independent Service Auditor's SOC 3 Report

For the

HackerOne Continuous Security Testing Platform System

For the Period of July 1, 2020, to June 30, 2021

Attestation and Compliance Services

schellman

Quality, above all.

INDEPENDENT SERVICE AUDITOR'S REPORT

To HackerOne Inc.:

Scope

We have examined HackerOne Inc.'s ("HackerOne") accompanying assertion titled "Assertion of HackerOne Service Organization Management" ("assertion") that the controls within its HackerOne Continuous Security Testing Platform system ("system") were effective throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that HackerOne's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

HackerOne uses a subservice organization for cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HackerOne, to achieve HackerOne's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system 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.

Service Organization's Responsibilities

HackerOne 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 HackerOne's service commitments and system requirements were achieved. HackerOne has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, HackerOne is responsible for selecting, and identifying in its assertion, the applicable trust services 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 systems requirements were achieved based on the applicable trust services criteria. 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 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 HackerOne's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve HackerOne'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.

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 HackerOne'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 HackerOne's Continuous Security Testing Platform system were effective throughout the period July 1, 2020, through June 30, 2021, to provide reasonable assurance that HackerOne's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

SCHELLMAN & COMPANY, LLC

Tampa, Florida
July 27, 2021

ASSERTION OF HACKERONE SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within HackerOne Inc.'s ("HackerOne") Continuous Security Testing Platform system ("system") throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that HackerOne's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that HackerOne's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. HackerOne's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 July 1, 2020, to June 30, 2021, to provide reasonable assurance that HackerOne's service commitments and systems requirements were achieved based on the applicable trust services criteria.

Description of the Boundaries of the HackerOne Continuous Security Testing Platform System

Company Background

HackerOne was founded in 2012 and is headquartered in San Francisco with offices in London and the Netherlands. HackerOne is a provider of bug bounty, vulnerability coordination solutions and penetration testing services, helping organizations find and fix critical vulnerabilities before they can be exploited.

Description of Services Provided

The HackerOne Continuous Security Testing Platform (HackerOne Platform) enables crowdsourced vulnerability discovery and disclosure activities. Customers are given access to a large and diverse number of crowdsourced security researchers, also called finders or hackers. This enables researchers to conduct remote, internet-based, crowdsourced vulnerability discovery and disclosure services against internet-accessible assets, including public-facing and private-facing websites, networks, systems, and applications.

The HackerOne Platform facilitates communication between the customer, triage personnel, and security researchers through the creation of customized vulnerability management workflows to track vulnerabilities throughout the remediation lifecycle. In addition, the coordination of vulnerability disclosures that impact third-party organizations or vendors is managed within the HackerOne Platform to maintain secure transmission and storage throughout the disclosure lifecycle.

Help Desk and Support

HackerOne provides customer support for its HackerOne Platform through a dedicated support team via e-mail at support@hackerone.com. A documentation center (https://docs.hackerone.com/) is provided for customers and external users, and a support ticketing system is maintained.

The system description in this section of the report details the HackerOne Platform. Any other HackerOne services are not included within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at HackerOne and does not include the policies, procedures, and control activities at Amazon Web Services, Inc. (AWS).

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

HackerOne has in place operational procedures to help ensure that customer security, availability, and confidentiality commitments can be met. HackerOne's commitments to user entities are documented and communicated to customers via the master service agreements (MSA), data processing agreements (DPA), service-level agreements (SLA), and through the terms and conditions, data and information security policy, and technical and organizational measures available to customers on the company website. Security management policies and procedures define an organization-wide approach to how information systems and customer confidential data are protected. These include policies and procedures around how the services are designed and developed, how the systems operate, how the internal business systems and networks are managed, and how employees are hired, trained, and managed.

HackerOne’s principal security, availability, and confidentiality commitments are standardized and include, but are not limited to, the following:

Principal Service Commitments and System Requirements		
Trust Services Category	**Service Commitments**	**System Requirements**
Security	• HackerOne will provide the services and the HackerOne Platform in accordance with HackerOne’s data and information security terms. HackerOne's workforce is sufficiently trustworthy to work in an environment which contains HackerOne information systems and customer's confidential information. • HackerOne shall engage one or more third parties no less than annually to evaluate its processes and systems to ensure continued compliance with obligations imposed by law, regulation, or contract with respect to the security, availability, and confidentiality of customer's confidential information. • HackerOne personnel, who access systems that store, transmit or process customer's confidential Information shall be assigned individual system accounts to ensure accountability for access granted. • HackerOne shall implement appropriate password parameters for systems that access, transmit or store customer's confidential information. HackerOne shall implement strong authentication services, complex passwords, and multi-factor authentication (MFA), where applicable, for all network and systems access to related systems. • HackerOne shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges for HackerOne information systems and customer's confidential information. • HackerOne shall maintain reasonable network perimeter controls such as firewalls at all perimeter connections. HackerOne shall no less than annually evaluate its network perimeter controls.	• Maintain information security and data handling policies and procedures. • Employees undergo a criminal background check prior to hiring. • Employees undergo performance reviews on an annual basis. • HackerOne employees are required to sign a confidentiality agreement upon hire. • HackerOne undergoes a third-party controls attestation on an annual basis. • External penetration testing is performed by third-party specialists on an annual basis. • Minimum password requirements and/or secure shell (SSH) public key authentication, including MFA as applicable, are enforced on production systems. • Maintain policies and procedures for requesting, approving, and administering access to production systems. • Users are assigned unique user accounts. • Privileged access to production systems and data is restricted to authorized personnel. • Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, resource utilization. • AWS security groups are configured as virtual firewalls. • AWS security group configurations are reviewed on a quarterly basis. • Internal vulnerability assessments are performed on a weekly basis.

Principal Service Commitments and System Requirements		
Trust Services Category	**Service Commitments**	**System Requirements**
Security (cont.'d)	• System configuration parameters shall include procedures to disable all unnecessary services on devices and servers. This practice shall at a minimum be applied to all systems that access, transmit, or store customer's confidential information. • HackerOne shall establish and adhere to policies and procedures for patching systems. Systems and applications used to access, process or store customer's confidential information shall be maintained at current stable patch level. • HackerOne shall install commercially reasonable anomaly detection software, to include anomaly / intrusion detections and deviations from standard system configuration, on all systems used to access, process or store customer's confidential information as well as other information that HackerOne hosts. • HackerOne shall maintain formal processes to detect, identify, report, respond to, and resolve any event that compromises the security, availability, and confidentiality of customer's data or service provider's systems in a timely manner. • For all systems that access, transmit or store customer's confidential information, system logs shall be in place to uniquely identify individual users and their access to associated systems and to identify the attempted or executed activities of such users. • HackerOne shall maintain reasonable change control processes to approve and track all changes within HackerOne's computing environment.	• Remediation plans are formally documented and tracked through resolution for vulnerabilities identified as part of penetration testing and vulnerability scanning activities. • Confirmed and resolved vulnerabilities and hacker-powered penetration test results are publicly available. • Maintain standard build procedures that include the requirement that unnecessary service accounts on devices and servers are disabled. • A patch management utility is in place to monitor for patches, upgrades, and fixes to production server operating systems. • An intrusion prevention system (IPS) is utilized to analyze and report network events and to block suspected or actual network security breaches. • A host-based intrusion detection system (HIDS) is in place to detect threats and is configured to send to security personnel when threats are detected. • Maintain security management policies and procedures to prevent, detect, contain, and correct violations of measures taken to protect the security, availability, and confidentiality of HackerOne information systems and/or customer's confidential information. • Maintain change management policies and procedures, requiring authorization and approval for any system changes impacting production systems. • Network communications are encrypted with secure transport layer security (TLS), perfect forward secrecy (PFS), and HTTP strict transport Security (HSTS). • An advanced encryption standard (AES)-256 encrypted VPN is utilized for remote access to production systems.

Principal Service Commitments and System Requirements		
Trust Services Category	**Service Commitments**	**System Requirements**
Security (cont.'d)		- User-submitted content, such as attachments and images, is stored in an encrypted format at rest using AES-256. - Databases, customer files, and data backups are encrypted at rest using AES-256.
Availability	- The HackerOne Platform will be operational and available to customers 24 hours per day, 7 days per week at least 99.5% of the time in any calendar month, except for scheduled maintenance and upgrades, and excluding API interruptions or third-party system interruptions. - HackerOne shall provide at least 24 hours' advance notice to customers on scheduled maintenance in excess of 30 minutes. - HackerOne will respond to customers and provide a first response in accordance with the time requirements defined in the SLA.	- Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, resource utilization, and to alert engineering personnel upon detection of unusual system activity or service requests. - Platform uptime, incidents, and SLAs are made available to external users via the HackerOne status page. - An automated ticketing system is utilized to document system availability and capacity incidents, responses, and resolution. - Maintain security management policies and procedures to prevent, detect, contain, and correct violations of measures taken to protect the security, availability, and confidentiality of HackerOne information systems and/or customer's confidential information. - Production data is replicated across geographically separate availability zones. - Engineering personnel perform backup data restores on an annual basis - Disaster recovery plans are tested on an annual basis to help ensure the production environment can be recovered in the event of a disaster.

Principal Service Commitments and System Requirements

Trust Services Category	Service Commitments	System Requirements
Confidentiality	• HackerOne shall maintain reasonable and appropriate processes and mechanisms to maintain accountability and tracking of the receipt, removal, and transfer of storage media used for HackerOne information systems or on which customer's confidential information is stored. • Except as expressly provided in the MSA, HackerOne agrees not to divulge to any third person any confidential information of the disclosing party and not to use any confidential information of the disclosing party for any purpose not contemplated by the MSA, provided the parties acknowledge and agree that the HackerOne aggregate data is not confidential information. • HackerOne shall ensure that any agent, including without limitation any third-party sub processor or subcontractor, to whom HackerOne provides customer's confidential information agrees to maintain reasonable and appropriate safeguards to protect such customer's confidential information. • HackerOne will ensure that any sub-processor it engages to provide an aspect of the services on its behalf in connection with the DPA does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of confidential data than those imposed on HackerOne in the DPA. • HackerOne personnel, who access systems that store, transmit or process customer's confidential Information shall be assigned individual system accounts to ensure accountability for access granted. • As soon as reasonably practicable following termination or expiry of the agreement or completion of the services, and in any event within 60 days of, upon customer's written request, HackerOne will delete or return to the customer all confidential data for which HackerOne is the processor and that is processed pursuit to the DPA.	• Maintain data and media handling policies and procedures. • Maintain data classification, retention, and disposal policies and procedures. • HackerOne employees are required to sign a confidentiality agreement upon hire. • HackerOne requires that vendors sign a confidentiality agreement before sharing any data or information designated as confidential. • Users are assigned unique user accounts. • Privileged access to production systems and data is restricted to authorized personnel. • Network communications are encrypted with TLS, PFS, and HSTS. • An AES-256 encrypted VPN is utilized for remote access to production systems. • User-submitted content, such as attachments and images, is stored in an encrypted format at rest using AES-256. • Databases, customer files, and data backups are encrypted at rest using AES-256. • The security team reviews changes to vendors along with their completed audit reports on an annual basis and determines the impact of any changes in relation to the organization's objectives and the impact on confidentiality of customer data.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

The HackerOne Platform is hosted within AWS in the AWS US East/West regions of us-west-2 (Oregon), us-east-1 (Virginia), us-east-2 (Ohio), and in the AWS ap-south-1 (Mumbai, India) region. The HackerOne Platform consists of a multi-tier virtualized architecture comprised of Linux-based application and database servers, storage and content delivery systems, and server and application monitoring and logging tools. HackerOne does not own or maintain hardware located in the AWS data centers, and operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure (e.g., physical infrastructure, geographical regions, availability zones, edge locations) and HackerOne is responsible for securing the platform deployed in AWS (e.g., customer data, applications, identity access management, network traffic).

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
HackerOne Platform	Facilitates communication between the customer, triage personnel, and security researchers through the creation of customized vulnerability management workflow to track vulnerabilities throughout the remediation lifecycle	Amazon Linux	Multiple AWS regions
AWS Elastic Compute Cloud (EC2)	Provides virtualized infrastructure security group control over applications and services provided by HackerOne		
AWS Relational Database Service (RDS)	Database solution for storage of operational data	PostgreSQL	
Snowflake	Data warehouse utilized for exacting, transforming, and loading (ETL) data to systems	Amazon AWS	
Okta	Vendor provided secure identity management and single sign-on (SSO)	Proprietary	Okta

In addition, HackerOne utilizes the following applications and services to support the HackerOne Platform:

- Amazon CloudFront – content delivery network
- Amazon CloudWatch – metrics and performance monitoring
- Amazon DynamoDB – key/value store
- Amazon Elasticache for Redis – caching
- Amazon GuardDuty – intrusion detection
- Amazon Inspector – vulnerability management
- Amazon Kinesis – logging
- Amazon Route 53 – domain name system (DNS)
- Amazon Simple E-mail Service (Amazon SES) – e-mail delivery

- Amazon Simple Notification Service (Amazon SNS) – publish/subscribe messaging
- Amazon Simple Queue Service (SQS) utilizing Sidekiq and Shoryuken – queueing and asynchronous processing
- Amazon Simple Storage Service (Amazon S3), Amazon S3 Glacier – object storage and logging
- Amazon Virtual Private Cloud (VPC) – private cloud services
- Ansible – operating system configuration management (Linux)
- AWS CloudTrail – security monitoring and auditing
- AWS Identity and Access Management (IAM) – access management
- AWS Key Management Service (KMS) – key management
- AWS Lambda – serverless infrastructure
- AWS Security Hub – security monitoring and management
- AWS Shield – distributed denial of service (DDoS) prevention
- Cloudflare – content delivery network, DDoS prevention, and DNS services
- Datadog – metrics and performance monitoring
- Fivetran – data pipeline services
- Git – source control management
- GitLab – development collaboration, code review, task management, continuous integration, and deployment
- New Relic – metrics and performance monitoring
- Osquery – endpoint visibility, file integrity monitoring, process auditing, baseline compliance, HIDS, vulnerability management, and malware detection
- PagerDuty – on-call rotation, escalation, and incident tracking
- Pingdom – edge monitoring and uptime statistics
- Slack – internal communication and notification system
- StatusPage – customer incident and uptime communications
- Sumo Logic – log analysis and monitoring, anomaly detection
- Terraform – infrastructure configuration management
- Twilio – short message service (SMS) notification
- Vault – secrets management
- Zapier – workflow automation
- Zendesk – helpdesk and ticketing system

People

HackerOne develops, manages, and secures the HackerOne Platform via separate functional departments. The responsibilities of these departments are defined below.

- Executive Management – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
- Employee Success (Human Resources (HR)) Department – responsible for onboarding new personnel, defining roles and positions of new hires, performing background checks, and facilitating the employee termination process.

- Customer Success Department – responsible for the support of the company’s customers in their use of the service, including both managing customer programs and triaging incoming security vulnerabilities.
- Product Department – responsible for the product lifecycle, including project management for development, design of user interfaces and experiences, and external documentation.
- Engineering Department – responsible for development, testing, deployment, and maintenance of new code for the HackerOne Platform, access controls and security of the production environment, providing management of technical resource activities, and providing technical resources to the Customer Success Department.
- Finance Department – responsible for oversight of corporate information technology (IT).
- Compliance Department – responsible for security and privacy compliance activities.

Procedures

Access, Authentication and Authorization

Documented standard build procedures and build automation tools are utilized for deployment of production servers. Access to the production systems is governed by IT policies and procedures. Authentication to the HackerOne production environment is restricted via multiple layered security mechanisms. HackerOne employees accessing production systems are required to authenticate utilizing a unique user account, MFA token, and predefined minimum password requirements, including SSH keys when entering through the Linux host. System and service account passwords are stored within a password management tool. Predefined security groups are utilized to assign role-based access privileges and segregate access to data within the in-scope systems. Additionally, a user must be connected to the encrypted virtual private network (VPN) before any type of connection to production services can be made.

Further, AWS security groups are in place to filter unauthorized inbound network traffic from the Internet and are configured to deny any type of network connection that is not explicitly authorized by a rule. Access to administer the production systems is restricted to authorized personnel. User activity is logged within each system layer and access is reviewed on an as-needed basis by security engineers.

Production customer data is stored in an encrypted format at rest utilizing AES-256 encryption. Access to the encryption keys is restricted to authorized security personnel. Additionally, a mobile device management (MDM) software is configured to encrypt the hard drives of HackerOne-owned workstations utilizing XTS-AES-128 encryption.

Access Requests and Access Revocation

Management has established controls to ensure that access to data is restricted to those who require access. A formal process has been established for managing user accounts and controlling access to HackerOne’s resources within the production environment. When a new employee is hired and has accepted a position at HackerOne, user access provisioning and onboarding requirements are documented as part of a standardized process. New hire access request forms include relevant information related to the new employee such as full name, job title, start date, and employment eligibility requirements. Certain access approvals are implicit based upon the new hire’s job role. Other internal user access requests are documented on a standard access request form and require the approval of a manager.

Upon notification of employee termination, a member of the IT team revokes the terminated employee’s system access, as well as privileged system access to the production systems. Employee termination activities are documented within the offboarding checklist. On a quarterly basis, members of the compliance team perform a user access review, including a review of privileged user account access, to help ensure users with access to the production systems are authorized.

Change Management

HackerOne maintains documented policies and procedures to guide personnel in change control practices that include, but are not limited to, initiating change requests, change control requirements, roles and responsibilities, and change approvals. Software development practices are aligned with the systems development life cycle

(SDLC) methodology, which helps ensure that security control specifications are met during the design process. The engineering team meets on a monthly basis to discuss and communicate the ongoing and upcoming initiatives and architecture changes.

HackerOne utilizes GitLab version control software to control code versioning and security throughout the code development process. Write access privileges to source code libraries and administrative access privileges within GitLab are restricted to user accounts accessible by authorized engineering or development personnel and provide for appropriate segregation of duties.

Upon initiation of a pull request, GitLab is configured to require code reviews and approval from an individual independent of the individual who initiated the pull request, as well as the successful completion of quality assurance (QA) testing in a non-production environment prior to merging the code commits within the pull request to the master branch. Baseline tests and static code scanning are performed for each pull request as well as specific checks that are dependent on the nature of the code commits within the pull request. If a test fails, the process is required to start over again until successful completion of testing. Upon successful completion of QA testing, changes are authorized for implementation to the production environment via GitLab continuous integration (CI) pipelines.

Access privileges to promote changes into the production environment via the automated deployment tool are segregated from those users with development responsibilities and restricted to authorized engineering personnel. Additionally, a file integrity monitoring (FIM) tool is utilized to monitor for changes to the production environment and is configured to notify engineering personnel when changes to the production environment occur. Development and test environments are logically separated from the production environment to help ensure that unauthorized code is not deployed to production.

Operating System Patch and Upgrade Management

A patch management utility is in place to monitor for patches, upgrades, and fixes to production server operating systems. Security patches for production server operating systems are automatically installed within 24 hours. Patches for other production systems are implemented through the change management process.

Data Backup and Disaster Recovery

Processes have been implemented for the backup of critical system components and data. Backups are managed by the engineering team and scheduled on a regular frequency established by the respective system owners. Critical production data stores are backed up at least hourly, while supplemental production data stores are backed up at least daily. The backup process is monitored for failures, and any failures are resolved per documented procedures to meet required backup frequency and retention.

HackerOne utilizes AWS to provide data redundancy to minimize disruptions to the availability of customer data. The data redundancy is achieved through fragmentation of data into extents, which are copied onto multiple nodes within a region. This approach minimizes the impact of isolated storage node failures and loss of data.

HackerOne has established a business continuity program that includes a business continuity plan (BCP), disaster recovery plan (DRP), and procedures for monitoring and improving the program.

HackerOne has defined the BCP to serve as a guide to respond, recover, and resume operations during a serious adverse event. The BCP covers the key personnel, resources, services, and actions required to continue critical business processes and operations. This plan is intended to address extended business disruptions.

The DRP is intended for usage by HackerOne for the recovery from high severity incidents (disasters) for its critical processes. The BCP and/or DRP includes scope and applicable dependencies for the services, restoration procedures, and communications with appropriate teams (i.e., incident response). The BCP and DRP are reviewed at least annually by a designated user and made available to all applicable users.

On an annual basis, HackerOne performs testing of the BCP and DRP, which is used to assess the effectiveness and usability of the plans and to identify areas where risks can be eliminated or mitigated. The results of testing are documented, validated, and approved by appropriate personnel. This information is used to create and prioritize work items.

HackerOne continually monitors the network to ensure availability and addresses capacity issues in a timely manner. The process for capacity planning includes an analysis of the capacity based on various parameters. Automation is used to automatically provision extra capacity based on need. Actions identified from monitoring are assigned for appropriate resolution. Additionally, HackerOne projects future capacity requirements based on internal operational reports, revenue forecasts, and inputs from internal component teams.

Incident Response

HackerOne has implemented an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers.

HackerOne teams use the established incident classification, escalation, and notification process for assessing an incident's criticality and severity, and, accordingly, escalating to the appropriate groups for timely action. The security team documents, tracks, and coordinates responses to incidents, including following established forensic procedures where applicable. When required, security incidents are escalated to the compliance, privacy, legal, or executive management teams for any needed breach notification and/or potential legal action after an information security incident.

Post-mortem activities are conducted for customer impacting incidents or incidents with critical severity. Incident and security post-mortem trends are reviewed and evaluated periodically and, when necessary, the HackerOne Platform or security program may be updated to incorporate improvements identified as a result of incidents.

Additionally, HackerOne conducts semi-annual tests of the HackerOne incident response plan. Reports related to information security events are provided to management regularly.

System Monitoring

HackerOne has established incident response procedures and centralized tracking tools, which consist of different channels for reporting production system incidents and weaknesses. Log files are retained to provide immutable records of computer events about an operating system, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications, and are reviewed by security personnel on an as needed basis when alerting is set up, and weekly for logs without alerting. Automated mechanisms include system monitoring processes for alerting security teams per defined and configured events, thresholds, or metric triggers. Incidents may also be reported via defined communication mediums. Users are made aware of their responsibilities of reporting incidents that will be looked into without any negative consequences. HackerOne incident response provides 24x7 event and incident monitoring and response services. The teams assess the health of various components along with access to detailed information when issues are discovered.

Data

HackerOne has deployed secure methods and protocols for the transmission of confidential and/or sensitive information over public and private networks. Customer data is loaded into the production environment and accessed remotely from customer systems via the Internet. Customer initiated connections over the Internet are secured utilizing TLS 1.2 or 1.3. An AES-256 encrypted VPN that enforces MFA is required for remote access to production systems by HackerOne personnel.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts. Data stores housing customer data are encrypted at rest utilizing AES-256 encryption. Access to encryption keys is restricted to authorized security personnel.

[Intentionally Blank]

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer data	Data from customer accounts, including personal data	Confidential
Log, metrics, and analytics files	Data utilized for HackerOne's monitoring of performance and security of services provided, including Internet Protocol (IP) addresses, user activity, browser information, and performance metrics	
HackerOne internal data	Data utilized to manage and support the services provided	

Subservice Organizations

The cloud hosting services provided by AWS were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone or in combination with controls at HackerOne, and the types of controls expected to be implemented at AWS to meet those criteria.

Control Activities Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, operating system, and storage devices for its cloud hosting services where HackerOne systems reside.	CC6.1 – CC6.3, CC6.5 – CC6.6
AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4 – CC6.5 CC7.2
AWS is responsible for implementing controls to restrict and protect information during transmission, movement, and removal from the underlying storage devices for its cloud hosting services where HackerOne systems reside.	CC6.7
AWS is responsible for monitoring any changes to the logical access controls system for the underlying network, virtualization management, and storage devices where the HackerOne systems reside.	CC7.1
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for their cloud hosting services where HackerOne systems reside.	CC7.2
AWS is responsible for monitoring the capacity demand and ensuring capacity resources are available and functioning to meet HackerOne's availability commitments and requirements.	A1.1
AWS is responsible for ensuring the data center facility is equipped with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the HackerOne Continuous Security Testing Platform system.