Productiv, Inc.

System and Organization Controls (SOC) 2 Type 2

Report on Productiv, Inc.'s Description of Its SaaS Management Platform and on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality

Throughout the Period
September 1, 2019 to August 31, 2020

Productiv

Contents

I. Independent Service Auditor's Report

Tel: 415-397-7900
Fax: 415-397-2161
www.bdo.com

One Bush Street, Suite 1800
San Francisco, CA 94104

Independent Service Auditor's Report

To the Management of
Productiv, Inc.
Palo Alto, California

Scope

We have examined Productiv, Inc.'s (Productiv or the Company) accompanying description of its SaaS Management Platform system titled *Productiv, Inc.'s Description of Its SaaS Management Platform System* throughout the period September 1, 2019 to August 31, 2020 (description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, Description Criteria), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period September 1, 2019 to August 31, 2020, to provide reasonable assurance that Productiv'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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

The information included in Section V, *Other Information Provided by Productiv, Inc. That Is Not Covered by the Independent Service Auditor's Report*, is presented by Productiv's management to provide additional information and is not part of Productiv's description. Information about Productiv's management's response to exceptions identified in the report has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve Productiv's service commitments and system requirements based on the applicable trust services criteria and, accordingly, we express no opinion on it.

Productiv uses Amazon Web Services (AWS), a subservice organization, to provide cloud computing services; and GitHub, a subservice organization, to provide cloud-based source code management and version control services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Productiv, to achieve Productiv's service commitments and system requirements based on the applicable trust services criteria. The description presents Productiv's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Productiv's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Productiv, to achieve Productiv's service commitments and system requirements based on the applicable trust services criteria. The description presents Productiv's controls, the applicable trust services criteria and the complementary user entity controls assumed in the design of Productiv's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Productiv 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 Productiv's service commitments and system requirements were achieved. Productiv has provided the accompanying assertion, titled *Assertion of Productiv, Inc. Management* (assertion), about the description and the suitability of design and operating effectiveness of controls stated therein. Productiv 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 that 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 the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risks 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, the tests we performed and the results of our tests are listed in Section IV of this report.

Opinion

In our opinion, in all material respects:

a. the description presents the SaaS Management Platform system that was designed and implemented throughout the period September 1, 2019 to August 31, 2020, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period September 1, 2019 to August 31, 2020 to provide reasonable assurance that Productiv'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 organizations and user entities applied the complementary controls assumed in the design of Productiv's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period September 1, 2019 to August 31, 2020 to provide reasonable assurance that Productiv'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 Productiv's controls operated effectively throughout that period.

Emphasis-of-Matter

The World Health Organization classified the COVID-19 outbreak as a pandemic in March 2020. Based on the rapid increase in exposure globally, the gravity or length of the impact of the COVID-19 outbreak cannot be estimated at this time.

Restricted Use

This report is intended solely for the information and use of Productiv; user entities of Productiv's SaaS Management Platform system during some or all of the period September 1, 2019 to August 31, 2020; business partners of Productiv subject to risks arising from interactions with the SaaS Management 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 user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

BDO USA, LLP

October 6, 2020

II. Assertion of Productiv, Inc. Management

Assertion of Productiv, Inc. Management

We have prepared the accompanying description of Productiv, Inc.'s (Productiv or service organization) SaaS Management Platform system titled *Productiv, Inc.'s Description of Its SaaS Management Platform System* throughout the period September 1, 2019 to August 31, 2020 (description), based on the criteria for a description of a service organization's system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, Description Criteria), (description criteria). The description is intended to provide report users with information about the SaaS Management Platform that may be useful when assessing the risks arising from interactions with Productiv's system, particularly information about system controls that Productiv 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, confidentiality and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Productiv uses subservice organizations to provide cloud computing services and cloud-based source code management and version control services. A list of these subservice organizations and the activities performed is provided in Section III. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Productiv, to achieve Productiv's service commitments and system requirements based on the applicable trust services criteria. The description presents Productiv's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Productiv'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 Productiv, to achieve Productiv's service commitments and system requirements based on the applicable trust services criteria. The description presents Productiv's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Productiv's controls. The description does not extend to controls of the user entities.

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

a. the description presents Productiv's SaaS Management Platform system that was designed and implemented throughout the period September 1, 2019 to August 31, 2020, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period September 1, 2019 to August 31, 2020 to provide reasonable assurance that Productiv'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 organizations and user entities applied the complementary controls assumed in the design of Productiv's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period September 1, 2019 to August 31, 2020 to provide reasonable assurance that Productiv'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 Productiv's controls operated effectively throughout that period.

Productiv, Inc.

October 6, 2020

III. Productiv, Inc.'s Description of Its SaaS Management Platform System

Productiv, Inc.'s Description of Its SaaS Management Platform System

Scope and Boundaries of the System

This is a System and Organization Controls (SOC) 2 Type 2 report and includes a description of Productiv, Inc.'s (Productiv, service organization or the Company) SaaS Management Platform system (the Platform), and the controls in place to provide reasonable assurance that Productiv's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria) (applicable trust services criteria), throughout the period September 1, 2019 to August 31, 2020, which may be relevant to users of the SaaS Management Platform system. It does not encompass all aspects of the services provided or procedures followed for other activities performed by Productiv.

Company Background

Productiv was founded in 2018 in Palo Alto, California by veterans from Amazon, Google, and LinkedIn who came together to help IT leaders rethink software as a service (SaaS) management. Backed by Accel, Norwest, and Okta Ventures, Productiv helps companies maximize application value in a way that is right for their people, their budget and their business.

Services Provided

Productiv provides a SaaS Management Platform that helps information technology (IT) leaders make better decisions about their SaaS applications. IT, finance, and business leaders collaborate when using the SaaS Management Platform to understand application adoption, increase company productivity, and reduce SaaS costs by providing insights about actual application use.

Productiv does this by analyzing how people engage with applications instead of just reviewing whether they logged in. Enterprises use Productiv to tighten-up application footprints and focus their teams' efforts on driving application adoption and engagement.

Productiv's SaaS Management Platform enables customers to:

1. *Manage SaaS Costs* - Visualize all applications and intelligently allocate licenses
    - Discover applications
    - Find wasteful spend
    - Analyze adoption and engagement
    - Forecast future use
2. *Reduce SaaS Costs* – Continuously evaluate and rationalize your application spend
    - Improve renewals and licensing tier decisions
    - Manage spend based on actual application use

- Make informed decisions about redundancy
- Drive adoption and engagement

3. *Drive SaaS Value* – Get data and insights to maximize the business value of applications
   - Drive application adoption
   - Enable stronger collaboration
   - Forecast and benchmark accurately
4. Plan SaaS Renewals – Never miss another renewal again
   - See all renewals in a calendar view
   - Choose the right license tier spend
   - Consider application overlap

System Incidents

Productiv did not identify any system incidents during the period September 1, 2019 to August 31, 2020, that resulted in significant failure in Productiv achieving its service commitments and system requirements as it relates to its SaaS Management Platform system based on the trust services relevant to security, confidentiality, and availability.

Impact of COVID-19

The World Health Organization classified the COVID-19 outbreak as a pandemic in March 2020. Based on the rapid increase in exposure globally, the gravity or length of the impact of the COVID-19 outbreak cannot be estimated at this time. In response, the Company moved its employees to work remotely and removed general access to the office headquarters. Operations continued unchanged otherwise.

Components of the System used to Provide the Services

The purpose of this description is to delineate the boundaries of the system, which includes the products and services listed above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure

The Platform includes the following infrastructure elements:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS Elastic Compute Cloud (EC2)	Computing Instances	The Platform is hosted on Amazon's core cloud server offering to provide operational speed, scalability and redundancy, and to utilize a variety of computing instances in multiple availability zones.

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS Lambda	Serverless Compute Platform	Productiv leverages AWS Lambda to perform compute services to run code without provisioning or managing servers.
AWS Simple Storage Service (S3)	File Storage	Productiv uses AWS S3, a secure, durable, highly-available object storage service to store customer data.
AWS Dynamo Database Service	Databases	Productiv uses DynamoDB as the databases that store customer data.
AWS Identity and Access Management (IAM)	Access Management	Productiv controls the provisioning, maintenance and deprovisioning of AWS access through this service.
AWS API Gateway	API Routing	Productiv uses the Application Programming Interface (API) gateway to manage the load balancing and API routing for the user interface (UI) and backend services.
AWS Elastic Beanstalk	Web Application Orchestration Service	Productiv implements Beanstalk environments to orchestrate and configure each of its production services.

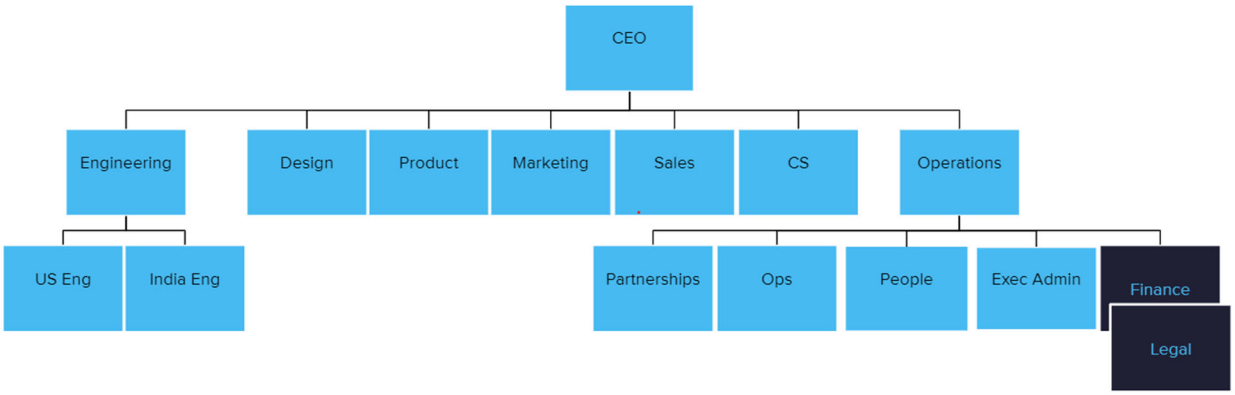
Software

Productiv leverages industry-standard third-party software tools to support the system. There are three key categories of software tools used: 1) system configuration and provisioning software, 2) source code management software and 3) monitoring software.

Primary Software		
Software	**System Components**	**Purpose**
AWS Linux	Operating System	Productiv uses Linux images for AWS EC2 servers
GitHub	Source Code Management and Version Control	Productiv uses GitHub for source code management and version control services
AWS CodeBuild & CodePipeline	Continuous Integration and Delivery Tools	Productiv uses CodeBuild and CodePipeline to automate the code build and deploy processes
GuardDuty	Intrusion Detection System	GuardDuty is used for monitoring for cloud and host intrusions
AWS CloudTrail	Cloud Monitoring	Productiv uses AWS CloudTrail to log operational/change events for the AWS Infrastructure.

Primary Software		
Software	**System Components**	**Purpose**
AWS CloudWatch	Cloud Monitoring	Productiv uses the AWS CloudWatch performance and capacity monitoring and management tools for the AWS Infrastructure.

People



Productiv personnel provide support and services in each of the core functional areas listed below:

Senior Management – Key executives that perform daily supervision, planning and administrative processes required by the Company

Engineering – Development and management of system features and services and troubleshoot complex problems. Also, to prevent unauthorized access and the protection of confidential and sensitive data

Product – Designing and formulating new features and services

Customer Success – Manages the relationship between customers and the Company

People – Critical functional area that has the responsibility of supporting employee well-being of the Company

Legal – Outsourced and manages the legal aspects of the Company

Processes and Procedures

Formal security, availability and confidentiality policies have been implemented and are reviewed annually, at minimum. Productiv personnel and contractors must adhere to Productiv policies and procedures that address services to be delivered. These documents are communicated to internal personnel and are made available on the internal collaborative workspace.

Policies and plans reviewed and made available include:

- Operational Information Security Policy
- Data Retention and Destruction Policy
- Internal Risk Management Policy
- Disaster Recovery and Resiliency Plan
- Incident Management and Breach Response Policy
- Vendor Management Checklist
- Employee Hiring, Onboarding and Termination Policy

Data

Productiv collects, processes and stores the following data from customers:

- Customer credentials used to access the data from the applications. Stored in AWS secret store.
- Contract and organization data. The data is stored in AWS S3.
- Usage data from the SaaS applications. Stored in AWS DynamoDB.

Data security:

- Data is encrypted in transit and at rest using AES-256 encryption.
- DynamoDB data is backed-up on an ongoing basis and controlled by the same access control rules as the primary data.
- Access to data is strictly controlled. Customers are only provided access to their own data, and can request different access levels for their users/admins.
- Productiv does not share our customers' data with any third-party.
- Ingested customer data (e.g., SaaS-app usage metrics) is retained for a timeframe per requirements/agreements per customer. All such data is retained or disposed as required per customer agreements, according to the Data Retention and Destruction Policy.

Description of the Controls Relevant to the Security (Common Criteria), Availability, and Confidentiality Trust Services Categories

Control Environment

The control environment at Productiv is the foundation for each of the other areas of internal control. Management emphasizes the implementation and adherence to controls and ethical behavior throughout the organization by providing a clear tone-at-the-top and helps establish the internal control mindset for the whole organization.

The Board of Directors operates independently from management to provide guidance and works with management to ensure business and internal control objectives are met. To help ensure the competency of personnel to fulfill control responsibilities, Productiv management and the Board of Directors have established an organizational structure supporting the Platform and reviews the structure on an annual basis. Further, roles, responsibilities, professional requirements and key competencies are documented in job descriptions.

The People team follows the structure established in the organizational chart to perform annual employee performance reviews over internal business and control requirements.

Hiring practices play a central role in Productiv's control environment as they facilitate the transfer and addition of control responsibilities, as well as trigger the change of access to sensitive systems. Prior to onboarding, background checks are performed on personnel who will have access to Productiv production systems and confidential information. Management and the People team have a formal process to address issues identified through background checks. As part of the hiring process, candidates are interviewed, and their skills and competencies are evaluated.

New hires are required to complete security awareness and e-learning courses during the first week of onboarding (and annually thereafter). They are also required to read and acknowledge the Employee Handbook during the first week of onboarding.

The Employee Handbook includes a code of conduct, the consequences of noncompliance with policies and procedures, and is available to employees on the Company's internal document repository. Management also communicates data handling expectations to internal personnel and requires them to sign Productiv's confidentiality policy upon hire.

Communication and Information

Management establishes formal security-related policies and standards to support the Platform, and policies are approved by the Chief Technology Officer (CTO). The CTO is further specifically responsible for adherence to and modification of the Platform security, availability and confidentiality policies. Productiv has established a Records Retention and Disposal Standard to define requirements for the secure storage and disposal of sensitive data.

Proper communication between Productiv, employees, third-parties and customers is key to ensuring control objectives are accomplished.

Productiv implements procedures to ensure that both the Company and its customers have the information needed to effectively operate the Platform. The Company communicates customer obligations, responsibilities and restrictions through Master Services Agreements (MSAs). The MSA

also includes services provided, requirements for handling confidential information and standard terms and conditions. Productiv maintains a support ticketing system to track, prioritize, and address inbound-customer communication and reporting of incidents, to help identify incidents in a timely manner.

Productiv has a formal onboarding process to help ensure that customers are familiar with the product and their security-related responsibilities. Additionally, changes that impact Platform security, availability, and confidentiality are communicated to customers by Customer Support prior to the change, or as a result of an outage/incident.

Risk Assessment

Management performs an annual risk assessment in which it identifies, addresses and documents risks. Identified risks are reviewed and actions are identified to mitigate risks to levels deemed acceptable by management. Productiv management actively identifies and assesses fraud risk as part of the risk assessment process. Reporting procedures are in place for employees to take appropriate action to report unacceptable behavior and fraud.

Additionally, management presents a slide deck of security and compliance information and discusses Company risks with the Board on an annual basis. Productiv mitigates the potential risk of disruption to the business by purchasing cybersecurity insurance to help address cyber-related disruptions.

Monitoring Activities

Productiv has established procedures to adequately respond to and remediate Platform security, availability, or confidentiality incidents. An Incident Response Plan is in place and provides instructions for tracking, reporting, and resolving internal and external security incidents.

Confirmed security incidents impacting the Platform are escalated to the appropriate teams and management for resolution. If service issues are related to vendors and/or customers, they are notified. For high-severity incidents, a post-mortem analysis is performed, and remediating actions are assigned.

Application penetration tests are performed annually by an independent third-party; high, medium, and low-risk findings are assigned remediation actions as needed and mitigated. Productiv configures a tool to scan the production environment for vulnerabilities on a weekly basis. Engineering reviews the scan results and remediates high and medium-risk vulnerabilities identified by the scanning tool. Engineering configures Auto Scaling through AWS to ensure that deviations in server configurations do not occur and baseline standards are maintained.

The Company employs industry-standard monitoring tools over its system infrastructure to help ensure the security, availability, and confidentiality of the Platform. A threat detection solution is deployed over its production systems to monitor for unauthorized behavior, intrusions, and anomalies. These tools are configured to alert the Security team on a real-time basis.

Internally, Productiv's Security team communicates and tracks security-related internal control compliance activities using a security-compliance calendar.

Control Activities

Control activities are shaped by the control environment and assessment of risk, and form the day-to-day processes of the internal control structure.

Logical Access

The CTO provisions access to the production environment and the source code management and version control tool; access is restricted to appropriate personnel. Administrative access to the cloud provider management console is restricted to appropriate personnel and requires two-factor authentication. Productiv configures the Identity and Access Management (IAM) system such that engineers have read-only access and code can only be deployed to production through the key-restricted access of the continuous integration and delivery tool. Access to customer data is restricted to the Engineering team through AWS Identity and Access Management. The Platform is configured to restrict customer access to their own accounts.

Access to Productiv employee workstations requires a username and password.

Upon employee termination, a checklist is used to help ensure proper procedures are followed for terminated users. Members of the People team notify the Engineering team of employee or contractor terminations to ensure access to systems is terminated within one business day. On a quarterly basis, the CTO reviews internal user access to the source code repository and the production Platform to verify that permissions are valid.

Productiv configures security groups to restrict inbound traffic into the production environment. Additionally, A web application firewall (WAF) is in place to help prevent unauthorized access threats from outside of Company systems.

Productiv maintains a managed distributed denial of service (DDoS) protection service to help safeguard the applications running on the Platform.

Software Change Management

Productiv has a code release and rollback process to address standard changes, emergency/hotfix changes for infrastructure, releases for functionality, and bugfixes for the Productiv application. The process includes segregation of duties, approval by qualified personnel, logical process structure to help ensure that software changes maintain the security, confidentiality, and availability of the Platform.

Non-production and production environments are logically separated. Production data is configured to be anonymized when used in non-production environments. Builds are required to pass automated integration and performance tests through the continuous integration and delivery tool prior to production deployment.

Engineering enforces independent code peer-approval and the performance of automated unit tests (through configuration of the code management and version control tool) before code can be merged to the master branch. Additionally, software engineers independent of code development perform functional manual tests before code changes are deployed to production. For code that was developed by a third-party, the code is reviewed for security purposes before changes are pushed to production.

Note: the security review of code developed by a third-party was implemented and operating as of January 1, 2020.

The code repository is configured such that independent code approvals are required to be re-performed in the event a code-modifying commit is pushed to the branch after initial review.

System Operations

Data is encrypted at-rest and in-transit. Production databases are stored encrypted using AES-256 encryption at the cloud platform and employee laptop hard drives are required to be configured with full-disk encryption. Transmission of customer data is performed using standard encryption technology.

Employee workstations have anti-virus installed and the anti-virus software is configured to receive automatic virus signature definition updates and scheduled to run scans periodically. Workstations are also configured with automatic security updates.

Productiv follows a documented Patch Management Policy to help ensure that servers in its environment are updated with current patches.

Risk Mitigation

Confidentiality agreements and/or non-disclosure agreements (NDAs) are required to be in place with third-parties prior to sharing information designated as confidential. Requirements for how Productiv handles confidential information are addressed within contractual agreements with customers.

Management completes a Vendor Management Checklist to evaluate vendor security controls prior to onboarding vendors. Management obtains third-party attestation reports for host data center and cloud service providers and other subservice organizations who are critical to supporting the delivery of Productiv services and the security of customer data. The reports are reviewed for issues or findings that might impact customer services, compliance, and access. Productiv management also performs a risk review on third-parties prior to access being granted to production systems that contain customer data, and annually thereafter.

Productiv has established a Disaster Recovery Plan to address operating procedures during events that significantly impact customer services. The plan is reviewed and tested on an annual basis.

To help ensure system availability despite loss or corruption of a single system instance, Productiv has developed processes for the backup and recovery of data. The Engineering team uses host-provider availability zones through AWS to provide Platform and service redundancy. Productiv configures its production databases to maintain continuous backups, which are stored for 35 days at the host-service provider.

Complementary Subservice Organization Controls (CSOCs)

Productiv's controls related to its SaaS Management Platform cover only a portion of the overall control environment required to provide reasonable assurance that the service commitments and system requirements were achieved. It is not feasible that the service commitments and system requirements can be achieved solely by Productiv's controls. The CSOCs in the table below are expected to be implemented and operating effectively:

Number	Complementary Subservice Organization Controls ("CSOC")	Applicable Criteria
Amazon Web Services		
1.	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CC6.1. CC6.6, CC6.7, C1.1, C1.2
2.	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	CC6.4, CC6.5, C1.2
3.	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC9.1
4.	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	CC8.1
5.	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	CC5.2
6.	Access to data and software is restricted to personnel authorized and provisioned with logical security controls.	CC5.2, CC6.1, CC6.2, CC6.4, CC6.6, C1.1
GitHub		
1.	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CC6.1. CC6.6, CC6.7, C1.1
2.	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC9.1
3.	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	CC8.1
4.	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	CC5.2

Number	Complementary Subservice Organization Controls ("CSOC")	Applicable Criteria
5.	Access to data and software is restricted to personnel authorized and provisioned with logical security controls.	CC5.2, CC6.1, CC6.2, CC6.4, CC6.6, C1.1

Complementary User Entity Controls (CUECs)

Productiv's controls related to its SaaS Management Platform cover only a portion of the overall control environment required to provide reasonable assurance that the service commitments and system requirements were achieved. It is not feasible that the service commitments and system requirements can be achieved solely by Productiv's controls. The CUECs in the table below are expected to be implemented and operating effectively:

Number	Complementary User Entity Controls (CUECs)	Applicable Criteria
1.	Maintaining the security of the client's account, passwords (including administrative and user passwords) and files, and for all uses of the client account.	CC2.3, CC5.2, CC6.1, CC6.2, CC6.6
2.	Reporting issues or security concerns related to the Productiv system to Productiv in a timely manner.	CC2.3, CC4.1, CC4.2, CC7.4

IV. Trust Services Categories, Criteria, Related Controls, Tests of Controls and Results of Tests

Trust Services Categories, Criteria, Related Controls, Tests of Controls and Results of Tests

This report is intended to provide information to the management of Productiv, user entities of the Productiv's SaaS Management Platform system, and prospective user entities, independent auditors and practitioners providing services to those entities, who have a sufficient understanding to consider it, along with other information, including information about the controls implemented by the user entity. This report is intended to provide information about the suitability of the design and operating effectiveness of the controls implemented to achieve the service commitments and system requirements based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria), throughout the period September 1, 2019 to August 31, 2020.

Although the applicable trust services criteria and related controls are presented in this section, they are an integral part of Productiv's description of its SaaS Management Platform system throughout the period September 1, 2019 to August 31, 2020.

The examination was performed in accordance with attestation standards established by the American Institute of Certified Public Accountants, *Statement on Standards for Attestation Engagements* (SSAE) 18, specifically, AT-C Sections 105 and 205 and the guidance contained in the *AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. It is each user entity's responsibility to evaluate this information in relation to the internal control structure in place at each user entity in order to assess the total internal control structure. If an effective internal control structure is not in place at user entities, the Productiv controls may not compensate for such weaknesses.

This description is intended to focus on Productiv's controls surrounding the SaaS Management Platform system throughout the period September 1, 2019 to August 31, 2020; it does not encompass all aspects of the services provided or controls performed by Productiv. Unique processes or control situations not described in the report are outside the scope of this report.

Tests of Controls

Our examination of the description of the service organization's SaaS Management Platform system and the suitability of the design and operating effectiveness of the controls to achieve the related service commitments and system requirements, based on the services criteria stated in the description, involved performing procedures to obtain evidence about the presentation of the description of the system in accordance with the description criteria and the suitability of the design and operating effectiveness of those controls to achieve the related service commitments and system requirements, based on the services criteria stated in the description. Our procedures included assessing the risks that the description is not presented in accordance with the description criteria and that the controls were not suitably designed or operating effectively to achieve the related service commitments and system requirements based on the services stated in the description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related service commitments and system

requirements based on the applicable trust services criteria stated in the description were achieved throughout the period September 1, 2019 to August 31, 2020.

Our tests of controls were designed to cover a representative number of activities throughout the period September 1, 2019 to August 31, 2020, for each of the controls listed in Section IV, which are designed to achieve the related service commitments and system requirements based on the applicable trust services criteria. In selecting particular tests of controls, we considered: (a) the nature of the controls being tested, (b) the types and competence of available evidential matter, (c) the criteria to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

BDO USA, LLP's testing of controls was restricted to the controls specified by Productiv in Section IV, and was not extended to controls in effect at user locations or other controls that were not documented as tested under each control criteria listed in Section IV. The description of BDO USA, LLP's tests of controls and results of those tests are presented in this section of the report. The description of the tests of controls and the results of those tests are the responsibility of BDO USA, LLP and should be considered information provided by BDO USA, LLP.

Types of testing methods include:

Type	Description
Inquiry	Made inquiries of appropriate personnel and corroborated responses with management
Observation	Observed the application, performance, or existence of the specific control(s), as represented by management
Inspection	Inspected documents and records indicating performance of the control
Reperformance	Reperformed the control or processing application to ensure the accuracy of its operation

When using information produced by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Control Environment					
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	1.1A	New hires are required to read and acknowledge the Employee Handbook during the first week of onboarding. The Employee Handbook includes a code of conduct and the consequences of noncompliance with policies and procedures and is available to employees on Productiv's internal document repository.	Inspected the signed Employee Handbook for a selection of new hires and determined that new hires are required to read and acknowledge the Employee Handbook during the first week of onboarding, and that the Employee Handbook includes a code of conduct and the consequences of noncompliance with policies and procedures.	Exceptions noted. Four of seven new hires selected for testing did not acknowledge the Employee Handbook during the first week of onboarding.
				Inspected a screenshot of Productiv's internal document repository and determined that the Employee Handbook was available to employees.	No exceptions noted.
		1.1B	Background checks are performed on personnel who will have access to Productiv production systems and sensitive customer information prior to onboarding.	Inspected a selection of background check results for new hires and determined that background checks are performed on personnel who have access to Productiv production systems and sensitive customer information prior to onboarding.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Control Environment					
		1.1C	Management performs employee performance reviews annually, at minimum to help ensure that internal business and control requirements are achieved.	Inspected the performance evaluations for a selection of employees and determined that management evaluates employee performance annually, at minimum.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	1.2A	The Board of Directors operates independently from management to provide guidance and works with management to help ensure business and internal control objectives are met.	Inspected Productiv's list of board members and compared it to Productiv's organizational chart and determined that there are board members independent from management.	No exceptions noted.
				Inspected the board meeting calendar invites and board meeting agendas for a selection of board meetings and determined that the Board of Directors provides guidance to help ensure business and internal control objectives are met.	No exceptions noted.
		1.2B	Management presents a slide deck of security and compliance information and discusses company risks with the Board on an annual basis.	Inspected a Board update slide deck and determined that management presents a slide deck of security and compliance information and discusses company risks with the Board on an annual basis.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Control Environment					
CC1.3	Management establishes, with board oversight, structures, reporting lines and appropriate authorities and responsibilities in the pursuit of objectives.	1.3A	Management and the Board of Directors have established an organizational structure supporting the Platform and review the structure on an annual basis.	Inspected Productiv's Organizational Chart and evidence of review and determined that management and the Board of Directors have established an organizational structure supporting the Platform and review the structure on an annual basis.	No exceptions noted.
		1.3B	Roles, responsibilities, professional requirements, and key competencies are documented in job descriptions.	Inspected the job description for a selection of new hires and determined that roles, responsibilities, professional requirements, and key competencies are documented in job descriptions.	No exceptions noted.
		1.3C	The Board of Directors operates independently from management to provide guidance and works with management to help ensure business and internal control objectives are met.	Inspected Productiv's list of board members and compared it to Productiv's organizational chart and determined that there are board members independent from management.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Control Environment					
				Inspected the board meeting calendar invites and board meeting agendas for a selection of board meetings and determined that the Board of Directors provides guidance and works with management to help ensure business and internal control objectives are met.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	1.4A	New hire candidates are interviewed and evaluated as part of the hiring process.	Inspected a selection of new hire evaluation forms and determined that new hire candidates are interviewed and evaluated as part of the hiring process.	No exceptions noted.
		1.4B	Background checks are performed on personnel who will have access to Productiv production systems and sensitive customer information prior to onboarding.	Inspected a selection of background check results for new hires and determined that background checks are performed on personnel who have access to Productiv production systems and sensitive customer information prior to onboarding.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Control Environment					
		1.4C	New hires are required to complete security awareness and e-learning courses during the first week of onboarding.	Inspected the security awareness training materials and acknowledgment of training for a selection of new hires and determined that new hires are required to complete security awareness and e-learning courses during the first week of onboarding.	No exceptions noted.
		1.4D	Roles, responsibilities, professional requirements, and key competencies are documented in job descriptions.	Inspected the job description for a selection of new hires and determined that roles, responsibilities, professional requirements, and key competencies are documented in job descriptions.	No exceptions noted.
		1.4E	Productiv requires employees to complete security awareness training on an annual basis.	Inspected the security awareness training course materials and the employee acknowledgment for a selection of employees and determined that Productiv requires employees to complete security awareness training on an annual basis.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Control Environment					
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	1.5A	Management performs employee performance reviews annually, at minimum to help ensure that internal business and control requirements are achieved.	Inspected the performance evaluations for a selection of employees and determined that management evaluates employee performance annually, at minimum.	No exceptions noted.
		1.5B	Management establishes formal policies and standards to support the security and confidentiality of the Platform. These policies are approved by the CTO.	Inspected the security and confidentiality-related policies and determined that management establishes formal policies and standards to support the Platform which are approved by the CTO.	No exceptions noted.
		1.5C	Management communicates data handling expectations for confidential data to internal personnel and requires them to sign Productiv's confidentiality policy upon hire.	Inspected a selection of signed Offer Letters containing the confidentiality policy and determined that management requires internal personnel to sign Productiv's confidentiality policy within the Company's online payroll, benefits and HR solution.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Communication and Information					
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	2.1A	Productiv has configured a tool to scan the production environment for vulnerabilities on a weekly basis. The Engineering team reviews scan results and remediates medium and high-risk vulnerabilities identified by the scanning tool.	Inspected Productiv's vulnerability scanning configuration and determined that Productiv has configured a tool to scan the production environment for vulnerabilities on a weekly basis.	No exceptions noted.
				Inspected the remediation documentation for a selection of medium and high-risk vulnerabilities and determined that the Engineering team reviews scan results and remediates medium and high-risk vulnerabilities identified by the scanning tool.	No exceptions noted.
		2.1B	Productiv deploys a threat detection and alerting solution to monitor its production systems for unauthorized behavior, intrusions, and anomalies. Identified medium and high-risk events are assigned remediation actions via the ticketing system and tracked to resolution.	Inspected the threat detection solution configuration and an example alert and determined that Productiv deploys a threat detection solution to monitor its production systems for unauthorized behavior, intrusions, and anomalies.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Communication and Information					
		2.1C	Application penetration tests are performed by an independent third-party on an annual basis. High, medium, and low-risk findings are assigned remediating actions as needed and tracked to resolution.	Inspected the most recent third-party penetration test report and determined that application penetration tests are performed by an independent third-party on an annual basis.	No exceptions noted.
				Inspected a selection of high, medium, and low-risk findings and determined that high, medium, and low-risk findings are assigned remediating actions as needed and tracked to resolution.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	2.2A	Productiv communicates and supports internal control compliance responsibilities through the use of a security-compliance calendar, which is available to the Security team.	Inspected the security-compliance calendar for a selection of months and determined that Productiv communicates and supports internal control compliance through the use of a security-compliance calendar made available to the Security team.	No exceptions noted.
		2.2B	Management establishes formal policies and standards to support the security, confidentiality, and availability of the Platform. These policies are approved by the CTO.	Inspected the security-related policies and determined that management establishes formal policies and standards to support the Platform and policies are approved by the CTO.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Communication and Information					
		2.2C	Management communicates data handling expectations for confidential data to internal personnel and requires them to sign Productiv's confidentiality policy upon hire.	Inspected a selection of signed Offer Letters containing the confidentiality policy and determined that management requires internal personnel to sign Productiv's confidentiality policy within the Company's online payroll, benefits and HR solution.	No exceptions noted.
		2.2D	Changes or updates to the Platform are communicated to employees through the corporate collaborative workspace.	Inspected the communication for a Platform change and determined that changes or updates are communicated to employees through the corporate collaborative workspace.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	2.3A	Productiv communicates customer obligations, responsibilities, and restrictions, including requirements for handing confidential information, through master service agreements, which also includes the services provided and the standard terms and conditions.	Inspected a selection of customer master service agreements and determined that Productiv communicates customer obligations, responsibilities, and restrictions through a master service agreement.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Communication and Information					
		2.3B	Confidentiality and/or non-disclosure agreements are required to be in place with third-parties prior to sharing information designated as confidential.	Inspected the confidentiality agreement and/or non-disclosure agreement for a selection of third-parties and determined that confidentiality agreements and/or non-disclosure agreements are in place with third-parties prior to sharing information designated as confidential.	No exceptions noted.
		2.3C	Productiv has a formal customer onboarding process to help ensure that customers are familiar with the Platform and their security-related responsibilities.	Inspected the onboarding slide decks for a selection of customers and determined that Productiv has a formal customer onboarding process to help ensure that customers are familiar with the Platform and their security-related responsibilities.	No exceptions noted.
		2.3D	Productiv maintains a support ticketing system to track, prioritize, and address inbound customer communication and reporting of incidents.	Inspected a screenshot of the support ticketing system and determined that Productiv uses a support ticketing system to track, prioritize, and address inbound customer communication and reporting of incidents.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Communication and Information					
		2.3E	Confirmed security incidents impacting the Platform are escalated to the appropriate teams and management for resolution. Vendors and/or customers are notified if service issues impact them.	Inspected the Incident Response Policy and determined that an Incident Response Policy is in place and provides instructions for contacting vendors and customers that would be notified if a security issue impacts them.	No exceptions noted.
				Inquired with the COO and corroborated with Lead Security Engineer and were informed that that there were no confirmed security incidents impacting the Platform during the examination period.	Since the circumstances that warrant the operation of this control did not occur during the examination period, this control could not be tested.
		2.3F	Changes that impact the Platform's security, availability, and confidentiality features are communicated to customers by Customer Support prior to the change implementation or as a result of a reported outage or incident.	Inspected evidence of communication with customers for a selection of changes that impacted the Platform's security, availability and confidentiality features to determine customers are notified.	No exceptions noted.
				Inquired with the COO and corroborated with Lead Security Engineer and were informed that that there were no confirmed security incidents impacting the Platform during the examination period.	Since the circumstances that warrant the operation of this control did not occur during the examination period, this control could not be tested.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Risk Assessment					
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	3.1A	The Board of Directors operates independently from management to provide guidance and works with management to help ensure business and internal control objectives are met.	Inspected Productiv's list of board members and compared it to Productiv's organizational chart and determined that there are board members independent from management.	No exceptions noted.
				Inspected the board meeting calendar invites and board meeting agendas for a selection of board meetings and determined that the Board of Directors provides guidance to help ensure business and internal control objectives are met.	No exceptions noted.
		3.1B	Productiv has a Risk Management Policy and performs an annual risk assessment to document risks and identify actions to mitigate risks to levels deemed acceptable by management.	Inspected the Risk Management Policy and the Risk Register and determined that Productiv has a Risk Management Policy and performs an annual risk assessment to document risks and identify actions to mitigate risks to levels deemed acceptable by management.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Risk Assessment					
		3.1C	Productiv has established a Records Retention, Archival and Destruction Policy to define requirements for storage and disposal of records in adherence to a defined schedule.	Inspected the Records Retention, Archival and Destruction Policy and determined that Productiv has established a standard to define requirements for storage and disposal of records in adherence to a defined schedule.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	3.2A	Productiv has a Risk Management Policy and performs an annual risk assessment to document risks and identify actions to mitigate risks to levels deemed acceptable by management.	Inspected the Risk Management Policy and the Risk Register and determined that Productiv has a Risk Management Policy and performs an annual risk assessment to document risks and identify actions to mitigate risks to levels deemed acceptable by management.	No exceptions noted.
		3.2B	Management assigns action and remediation plans for high and critical risks identified in the annual risk assessment.	Inspected the Risk Register and evidence of remediation for a selection of identified risks and determined that high and critical risks identified have action and remediation plans assigned.	No exceptions noted.
		3.2C	Management actively identifies and assesses fraud risk. Reporting procedures are in place which allow employees to report	Inspected Productiv's Risk Register and determined that Management actively identifies and assesses fraud risk.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Risk Assessment					
			unacceptable behavior or actual or suspected fraud to the appropriate parties.	Inspected Productiv's Employee Handbook and determined that reporting procedures are in place which allow employees to take action to report unacceptable behavior or actual or suspected fraud to the appropriate parties.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	3.3A	Management actively identifies and assesses fraud risk. Reporting procedures are in place which allow employees to report unacceptable behavior or actual or suspected fraud to the appropriate parties.	Inspected Productiv's Risk Register and determined that Management actively identifies and assesses fraud risk.	No exceptions noted.
				Inspected Productiv's Employee Handbook and determined that reporting procedures are in place which allow employees to take action to report unacceptable behavior or actual or suspected fraud to the appropriate parties.	No exceptions noted.
		3.3B	Productiv has a Risk Management Policy and performs an annual risk assessment to document risks and identify actions to mitigate risks to levels deemed acceptable by management.	Inspected the Risk Management Policy and the Risk Register and determined that Productiv has a Risk Management Policy and performs an annual risk assessment to document risks and identify actions to mitigate risks to levels deemed acceptable by management.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Risk Assessment					
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	3.4A	Productiv has a Risk Management Policy and performs an annual risk assessment to document risks and identify actions to mitigate risks to levels deemed acceptable by management.	Inspected the Risk Management Policy and the Risk Register and determined that Productiv has a Risk Management Policy and performs an annual risk assessment to document risks and identify actions to mitigate risks to levels deemed acceptable by management.	No exceptions noted.
		3.4B	Productiv has a formal code release and rollback process to address Productiv Platform standard changes, hotfix changes, and rollbacks.	Inspected the code release and rollback procedures and determined that a defined change management release and rollback process is in place to address Productiv Platform standard changes, hotfix changes, and rollbacks.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Monitoring Activities					
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	4.1A	Application penetration tests are performed by an independent third-party on an annual basis. High, medium, and low-risk findings are assigned remediating actions as needed and tracked to resolution.	Inspected the most recent third-party penetration test report and determined that application penetration tests are performed by an independent third-party on an annual basis.	No exceptions noted.
				Inspected a selection of high, medium, and low-risk findings and determined that high, medium, and low-risk findings are assigned remediating actions as needed and tracked to resolution.	No exceptions noted.
		4.1B	On a quarterly basis, the CTO reviews internal user access to the source code repository and the production Platform to verify that permissions are valid.	Inspected documentation for a selection of quarterly Platform access reviews and determined that the CTO reviews internal user access to the source code repository and the production Platform and determined that permissions are valid.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Monitoring Activities					
		4.1C	Productiv has configured a tool to scan the production environment for vulnerabilities on a weekly basis. The Engineering team reviews scan results and remediates medium and high-risk vulnerabilities identified by the scanning tool.	Inspected Productiv's vulnerability scanning configuration and determined that Productiv has configured a tool to scan the production environment for vulnerabilities on a weekly basis.	No exceptions noted.
				Inspected the remediation documentation for a selection of medium and high-risk vulnerabilities and determined that the Engineering team reviews scan results and remediates medium and high-risk vulnerabilities identified by the scanning tool.	No exceptions noted.
		4.1D	Productiv deploys a threat detection and alerting solution to monitor its production systems for unauthorized behavior, intrusions, and anomalies. Identified medium and high-risk events are assigned remediation actions via the ticketing system and tracked to resolution.	Inspected the threat detection solution configuration and an example alert and determined that Productiv deploys a threat detection solution to monitor its production systems for unauthorized behavior, intrusions, and anomalies.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Monitoring Activities					
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	4.2A	An Incident Response Plan is in place and provides instructions for tracking, reporting, and resolving internal and external security incidents.	Inspected the Incident Response Plan and determined that an Incident Response Plan is in place and provides instructions for tracking, reporting, and resolving internal and external security incidents.	No exceptions noted.
		4.2B	Confirmed security incidents impacting the Platform are escalated to the appropriate teams and management for resolution. Vendors and/or customers are notified if service issues impact them.	Inspected the Incident Response Policy and determined that an Incident Response Policy is in place and provides instructions for contacting vendors and customers that would be notified if a security issue impacts them.	No exceptions noted.
				Inquired with the COO and corroborated with Lead Security Engineer and were informed that that there were no confirmed security incidents impacting the Platform during the examination period.	Since the circumstances that warrant the operation of this control did not occur during the examination period, this control could not be tested.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Control Activities					
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	5.1A	Productiv has established a Disaster Recovery Plan to address operating procedures during events that significantly impact customer services. The plan is reviewed and tested on an annual basis.	Inspected the Disaster Recovery Plan and the test results and determined that Productiv has established a Disaster Recovery Plan and tests it on an annual basis.	No exceptions noted.
		5.1B	Management communicates data handling expectations for confidential data to internal personnel and requires them to sign Productiv's confidentiality policy upon hire.	Inspected a selection of signed Offer Letters containing the confidentiality policy and determined that management requires internal personnel to sign Productiv's confidentiality policy within the Company's online payroll, benefits and HR solution.	No exceptions noted.
		5.1C	Management establishes formal policies and standards to support the security, confidentiality, and availability of the Platform. These policies are approved by the CTO.	Inspected the security-related policies and determined that management establishes formal policies and standards to support the Platform and policies are approved by the CTO.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Control Activities					
		5.1D	Productiv has a formal code release and rollback process to address Productiv Platform standard changes, hotfix changes, and rollbacks.	Inspected the code release and rollback procedures and determined that a defined change management release and rollback process is in place to address Productiv Platform standard changes, hotfix changes, and rollbacks.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	5.2A	Productiv deploys a threat detection and alerting solution to monitor its production systems for unauthorized behavior, intrusions, and anomalies. Identified medium and high-risk events are assigned remediation actions via the ticketing system and tracked to resolution.	Inspected the threat detection solution configuration and an example alert and determined that Productiv deploys a threat detection solution to monitor its production systems for unauthorized behavior, intrusions, and anomalies.	No exceptions noted.
		5.2B	Productiv has established a Records Retention, Archival and Destruction Policy to define requirements for storage and disposal of records in adherence to a defined schedule.	Inspected the Records Retention, Archival and Destruction Policy and determined that Productiv has established a standard to define requirements for storage and disposal of records in adherence to a defined schedule.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Control Activities					
		5.2C	Productiv has a formal code release and rollback process to address Productiv Platform standard changes, hotfix changes, and rollbacks.	Inspected the code release and rollback procedures and determined that a defined change management release and rollback process is in place to address Productiv Platform standard changes, hotfix changes, and rollbacks.	No exceptions noted.
		5.2D	Management establishes formal policies and standards to support the security, confidentiality, and availability of the Platform. These policies are approved by the CTO.	Inspected the security-related policies and determined that management establishes formal policies and standards to support the Platform and policies are approved by the CTO.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	5.3A	An Incident Response Plan is in place and provides instructions for tracking, reporting, and resolving internal and external security incidents.	Inspected the Incident Response Plan and determined that an Incident Response Plan is in place and provides instructions for tracking, reporting, and resolving internal and external security incidents.	No exceptions noted.
		5.3B	Management establishes formal policies and standards to support the security, confidentiality, and availability of the Platform. These policies are approved by the CTO.	Inspected the security-related policies and determined that management establishes formal policies and standards to support the Platform and policies are approved by the CTO.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Control Activities					
		5.3C	Productiv has established a Records Retention, Archival and Destruction Policy to define requirements for storage and disposal of records in adherence to a defined schedule.	Inspected the Records Retention, Archival and Destruction Policy and determined that Productiv has established a standard to define requirements for storage and disposal of records in adherence to a defined schedule.	No exceptions noted.
		5.3D	Productiv has a formal code release and rollback process to address Productiv Platform standard changes, hotfix changes, and rollbacks.	Inspected the code release and rollback procedures and determined that a defined change management release and rollback process is in place to address Productiv Platform standard changes, hotfix changes, and rollbacks.	No exceptions noted.
		5.3E	Management communicates data handling expectations for confidential data to internal personnel and requires them to sign Productiv's confidentiality policy upon hire.	Inspected a selection of signed Offer Letters containing the confidentiality policy and determined that management requires internal personnel to sign Productiv's confidentiality policy within the Company's online payroll, benefits and HR solution.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Logical and Physical Access					
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	6.1A	Non-production and production environments are logically separated.	Inspected the AWS Organizations dashboard and determined that non-production and production environments are logically separated.	No exceptions noted.
		6.1B	Productiv configures the AWS IAM system such that users have read-only access and code can only be deployed to production through the continuous integration and development tool.	Inspected the IAM and continuous integration tool configurations and determined that users have read-only access to production and code can only be deployed to production through key-restricted access of the continuous integration tool.	No exceptions noted.
		6.1C	Productiv configures AWS security groups to restrict inbound traffic into the production environment.	Inspected the AWS security group configurations and determined that Productiv configures AWS security groups to restrict inbound traffic into the production environment.	No exceptions noted.
		6.1D	Production databases are configured to be stored encrypted at the cloud platform.	Inspected the encryption configuration for a selection of production databases and determined that production databases are stored encrypted at the cloud platform.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Logical and Physical Access					
		6.1E	Productiv employs an endpoint management platform that enforces a username and password, password complexity, auto-lock, and full-disk encryption for employee workstations.	Inspected the endpoint management platform configurations and enforced policies and determined that Productiv employs an endpoint management platform.	No exceptions noted.
				Inspected the list of enforced devices on the endpoint management platform and traced a selection of employees to the list of enforced devices and determined that Productiv employs an endpoint management platform to enforce a username and password, password complexity, auto-lock, and full-disk encryption for employee workstations.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered	6.2A	User access provisioning to the production environment and the code repository is restricted to appropriate personnel.	Inspected the list of administrators with access to the production environment and code repository and determined that user access provisioning to the production environment and the code repository is restricted to appropriate personnel.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Logical and Physical Access					
	by the entity, user system credentials are removed when user access is no longer authorized.	6.2B	The Platform is configured to restrict customer access to their own accounts.	Reperformed for a test production account, logging in and attempting to access a customer's production account, to determine that the Platform is configured to restrict customer access to their own accounts.	No exceptions noted.
		6.2C	On a quarterly basis, the CTO reviews internal user access to the source code repository and the production Platform to verify that permissions are valid.	Inspected documentation for a selection of quarterly Platform access reviews and determined that the CTO reviews internal user access to the source code repository and the production Platform and determined that permissions are valid.	No exceptions noted.
		6.2D	When an employee or contractor is terminated, access to Productiv systems is revoked within one business day.	Inspected access to Productiv systems being revoked for a selection of terminated employees and contractors and determined that when an employee or contractor is terminated, access to Productiv systems is revoked within one business day.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Logical and Physical Access					
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	6.3A	Administrator access to the AWS management console is restricted to appropriate personnel and requires two-factor authentication.	Inspected the list of users with administrator access to the AWS account and compared the users against the list of employees and determined that administrator access to the AWS management console is restricted to appropriate personnel and that two-factor authentication is enforced.	No exceptions noted.
		6.3B	Productiv restricts access to the source code repository to appropriate personnel.	Inspected the source code repository access list and traced a selection of account users to the list of employees and determined that access was restricted to appropriate personnel.	No exceptions noted.
		6.3C	Access to customer data is restricted to the Engineering team through AWS IAM.	Inspected the list of users with access to customer data and compared a selection of users to the list of employees and determined that access to customer data is restricted to the Engineering team through AWS IAM.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Logical and Physical Access					
		6.3D	Productiv configures the AWS IAM system such that users have read-only access and code can only be deployed to production through the continuous integration and development tool.	Inspected the IAM and continuous integration tool configurations and determined that users have read-only access to production and code can only be deployed to production through key-restricted access of the continuous integration tool.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	6.4A	Management performs due diligence during onboarding and annually thereafter, such as obtaining third-party attestation reports to monitor subservice organizations who are critical to supporting the delivery of Productiv services and the security of customer data. Reports or security questionnaires are reviewed for issues or findings that might impact customer services, compliance, and access.	Inspected a vendor review ticket for a selection of vendors and determined that management performs due diligence, such as obtaining third-party attestation reports before granting subservice organizations access to production data.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Logical and Physical Access					
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	6.5A	Productiv has established a Records Retention, Archival and Destruction Policy to define requirements for storage and disposal of records in adherence to a defined schedule.	Inspected the Records Retention, Archival and Destruction Policy and determined that Productiv has established a standard to define requirements for storage and disposal of records in adherence to a defined schedule.	No exceptions noted.
		6.5B	When an employee or contractor is terminated, access to Productiv systems is revoked within one business day.	Inspected access to Productiv systems being revoked for a selection of terminated employees and contractors and determined that when an employee or contractor is terminated, access to Productiv systems is revoked within one business day.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	6.6A	A web application firewall is in place to help prevent unauthorized access from outside of Productiv systems.	Inspected the web application firewall configuration and determined that a web application firewall was in place to help prevent unauthorized access from outside of Productiv systems.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Logical and Physical Access					
		6.6B	Productiv deploys a threat detection and alerting solution to monitor its production systems for unauthorized behavior, intrusions, and anomalies. Identified medium and high-risk events are assigned remediation actions via the ticketing system and tracked to resolution.	Inspected the threat detection solution configuration and an example alert and determined that Productiv deploys a threat detection solution to monitor its production systems for unauthorized behavior, intrusions, and anomalies.	No exceptions noted.
		6.6C	Productiv configures AWS security groups to restrict inbound traffic into the production environment.	Inspected the AWS security group configurations and determined that Productiv configures AWS security groups to restrict inbound traffic into the production environment.	No exceptions noted.
		6.6D	Productiv configures employee workstations to automatically install security patches and updates.	Inspected the security patching configuration for a selection of employees and determined that Productiv configures employee workstations to automatically install security patches and updates.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Logical and Physical Access					
		6.6E	Productiv configures automatic managed patching through AWS to help ensure that production resources are updated with current patches.	Inspected the patch management configurations for production resources and determined that Productiv configures automatic managed patching through AWS to help ensure that production resources are updated with current patches.	No exceptions noted.
		6.6F	Productiv requires employee workstations to have anti-virus software installed, including enabling automatic virus signature definition updates and scheduled periodic scans.	Inspected the workstation anti-virus software configurations for a selection of employee workstations and determined that Productiv requires employee workstations to have anti-virus software installed.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	6.7A	Productiv enforces encryption of data transmitted from their Platform to the user's web browser.	Inspected the transfer protocol for each production service load balancer and determined that transmission of customer data is performed using industry-standard encryption technology.	No exceptions noted.
		6.7B	Production data is anonymized when used in non-production environments.	Inspected the data-masking configuration and a selected masked data export and determined that production data is anonymized when used in non-production environments.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Logical and Physical Access					
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	6.8A	Productiv deploys a threat detection and alerting solution to monitor its production systems for unauthorized behavior, intrusions, and anomalies. Identified medium and high-risk events are assigned remediation actions via the ticketing system and tracked to resolution.	Inspected the threat detection solution configuration and an example alert and determined that Productiv deploys a threat detection solution to monitor its production systems for unauthorized behavior, intrusions, and anomalies.	No exceptions noted.
		6.8B	Productiv requires employee workstations to have anti-virus software installed, including enabling automatic virus signature definition updates and scheduled periodic scans.	Inspected the workstation anti-virus software configurations for a selection of employee workstations and determined that Productiv requires employee workstations to have anti-virus software installed.	No exceptions noted.
		6.8C	Productiv configures employee workstations to automatically install security patches and updates.	Inspected the security patching configuration for a selection of employees and determined that Productiv configures employee workstations to automatically install security patches and updates.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to System Operations					
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		7.1A	Productiv deploys a threat detection and alerting solution to monitor its production systems for unauthorized behavior, intrusions, and anomalies. Identified medium and high-risk events are assigned remediation actions via the ticketing system and tracked to resolution.	Inspected the threat detection solution configuration and an example alert and determined that Productiv deploys a threat detection solution to monitor its production systems for unauthorized behavior, intrusions, and anomalies.	No exceptions noted.
		7.1B	Productiv has configured a tool to scan the production environment for vulnerabilities on a weekly basis. The Engineering team reviews scan results and remediates medium and high-risk vulnerabilities identified by the scanning tool.	Inspected Productiv's vulnerability scanning configuration and determined that Productiv has configured a tool to scan the production environment for vulnerabilities on a weekly basis.	No exceptions noted.
				Inspected the remediation documentation for a selection of medium and high-risk vulnerabilities and determined that the Engineering team reviews scan results and remediates medium and high-risk vulnerabilities identified by the scanning tool.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to System Operations					
		7.1C	Application penetration tests are performed by an independent third-party on an annual basis. High, medium, and low-risk findings are assigned remediating actions as needed and tracked to resolution.	Inspected the most recent third-party penetration test report and determined that application penetration tests are performed by an independent third-party on an annual basis.	No exceptions noted.
				Inspected a selection of high, medium, and low-risk findings and determined that high, medium, and low-risk findings are assigned remediating actions as needed and tracked to resolution.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives;	7.2A	Productiv deploys a threat detection and alerting solution to monitor its production systems for unauthorized behavior, intrusions, and anomalies. Identified medium and high-risk events are assigned remediation actions via the ticketing system and tracked to resolution.	Inspected the threat detection solution configuration and an example alert and determined that Productiv deploys a threat detection solution to monitor its production systems for unauthorized behavior, intrusions, and anomalies.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to System Operations					
	anomalies are analyzed to determine whether they represent security events.	7.2B	Productiv utilizes a system performance monitoring tool to monitor Platform capacity and performance and provide alerts to the Security team on a real-time basis. Performance and capacity issues are assigned remediating actions as needed and tracked to resolution.	Inspected the capacity and performance monitoring tool dashboard, configurations, and an example alert and determined that Productiv utilizes a system performance monitoring tool to monitor Platform capacity and performance and provide alerts to the Security team on a real-time basis.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	7.3A	An Incident Response Plan is in place and provides instructions for tracking, reporting, and resolving internal and external security incidents.	Inspected the Incident Response Plan and determined that an Incident Response Plan is in place and provides instructions for tracking, reporting, and resolving internal and external security incidents.	No exceptions noted.
		7.3B	Confirmed security incidents impacting the Platform are escalated to the appropriate teams and management for resolution. Vendors and/or customers are notified if service issues impact them.	Inspected the Incident Response Policy and determined that an Incident Response Policy is in place and provides instructions for contacting vendors and customers that would be notified if a security issue impacts them.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to System Operations					
				Inquired with the COO and corroborated with Lead Security Engineer and were informed that that there were no confirmed security incidents impacting the Platform during the examination period.	Since the circumstances that warrant the operation of this control did not occur during the examination period, this control could not be tested.
		7.3C	Security incidents are assigned a ticket. For high-severity incidents, a postmortem is performed, and remediating actions are assigned.	Inspected a selection of postmortems and determined that for high-severity incidents a postmortem is performed, and remediating actions are assigned.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	7.4A	An Incident Response Plan is in place and provides instructions for tracking, reporting, and resolving internal and external security incidents.	Inspected the Incident Response Plan and determined that an Incident Response Plan is in place and provides instructions for tracking, reporting, and resolving internal and external security incidents.	No exceptions noted.
		7.4B	Confirmed security incidents impacting the Platform are escalated to the appropriate teams and management for resolution. Vendors and/or customers are notified if service issues impact them.	Inspected the Incident Response Policy and determined that an Incident Response Policy is in place and provides instructions for contacting vendors and customers that would be notified if a security issue impacts them.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to System Operations					
				Inquired with the COO and corroborated with Lead Security Engineer and were informed that that there were no confirmed security incidents impacting the Platform during the examination period.	Since the circumstances that warrant the operation of this control did not occur during the examination period, this control could not be tested.
		7.4C	Security incidents are assigned a ticket. For high-severity incidents, a postmortem is performed, and remediating actions are assigned.	Inspected a selection of postmortems and determined that for high-severity incidents, a postmortem is performed, and remediating actions are assigned.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	7.5A	An Incident Response Plan is in place and provides instructions for tracking, reporting, and resolving internal and external security incidents.	Inspected the Incident Response Plan and determined that an Incident Response Plan is in place and provides instructions for tracking, reporting, and resolving internal and external security incidents.	No exceptions noted.
		7.5B	Confirmed security incidents impacting the Platform are escalated to the appropriate teams and management for resolution. Vendors and/or customers are notified if service issues impact them.	Inspected the Incident Response Policy and determined that an Incident Response Policy is in place and provides instructions for contacting vendors and customers that would be notified if a security issue impacts them.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to System Operations					
				Inquired with the COO and corroborated with Lead Security Engineer and were informed that that there were no confirmed security incidents impacting the Platform during the examination period.	Since the circumstances that warrant the operation of this control did not occur during the examination period, this control could not be tested.
		7.5C	Security incidents are assigned a ticket. For high-severity incidents, a postmortem is performed, and remediating actions are assigned.	Inspected a selection of postmortems and determined that for high-severity incidents, a postmortem is performed, and remediating actions are assigned.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Change Management					
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	8.1A	Productiv has a formal code release and rollback process to address Productiv Platform standard changes, hotfix changes, and rollbacks.	Inspected the code release and rollback procedures and determined that a defined change management release and rollback process is in place to address Productiv Platform standard changes, hotfix changes, and rollbacks.	No exceptions noted.
		8.1B	A continuous integration and delivery tool is configured to perform automated unit tests over code changes prior to merge to the master branch.	Inspected the automated testing configuration and unit test results for a selected code change and determined that a continuous integration and delivery tool is configured to perform automated unit tests over code changes prior to merge to master.	No exceptions noted.
		8.1C	Productiv configures the code repository to ensure that independent change approval is required prior to merging changes to the master branch.	Inspected the code repository configuration and a review and approval ticket for a selected merge and determined that Productiv configures the code repository to ensure that independent change approval is required prior to merging changes to the master branch.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Change Management					
		8.1D	Productiv performs a security review on code that was developed by third-parties, such as open source code, prior to merging to the master branch. Note: Control was implemented January 1, 2020	Inspected a selection of tickets from changes that include externally developed code from third-parties and determined that Productiv performs a security review on the code prior to merging the code to master.	No exceptions noted.
		8.1E	Productiv configures its code repository such that independent code approvals are required to be re-performed once a code-modifying commit is pushed to the master branch following the initial review.	Inspected the code repository configuration and a ticket for a selected merge and determined that Productiv configures its code repository such that independent code approvals are required to be re-performed once a code-modifying commit is pushed to the branch following the initial review.	No exceptions noted.
		8.1F	Software Engineers independent of code development perform functional manual tests before code changes are deployed to production.	Inspected the release notes for a selection of software code changes and determined that Software Engineers independent of code development perform functional manual tests before code changes are deployed to production.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Change Management					
		8.1G	Productiv requires builds to pass automated integration and performance tests prior to automated production deployment.	Inspected the build and deployment tool configurations and test results for a selected change and determined that Productiv requires builds to pass automated integration and performance tests prior to automated production deployment.	No exceptions noted.
		8.1H	Productiv configures automatic managed patching through AWS to help ensure that production resources are updated with current patches.	Inspected the patch management configurations for production resources and determined that Productiv configures automatic managed patching through AWS to help ensure that production resources are updated with current patches.	No exceptions noted.
		8.1I	Non-production and production environments are logically separated.	Inspected the AWS Organizations dashboard and determined that non-production and production environments are logically separated.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Risk Mitigation					
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	9.1A	Productiv has a Risk Management Policy and performs an annual risk assessment to document risks and identify actions to mitigate risks to levels deemed acceptable by management.	Inspected the Risk Management Policy and the Risk Register and determined that Productiv has a Risk Management Policy and performs an annual risk assessment to document risks and identify actions to mitigate risks to levels deemed acceptable by management.	No exceptions noted.
		9.1B	Productiv configures its production databases containing customer data for continuous backups, which are configured to be stored for 35 days at the cloud platform.	Inspected the backup configurations for production databases containing customer data and determined that Productiv configures its production databases containing customer data for continuous backups, which are stored for 35 days at the cloud platform.	No exceptions noted.
		9.1C	Management assigns action and remediation plans for high and critical risks identified in the annual risk assessment.	Inspected the Risk Register and evidence of remediation for a selection of identified risks and determined that high and critical risks identified have action and remediation plans assigned.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Risk Mitigation					
		9.1D	Productiv has established a Disaster Recovery Plan to address operating procedures during events that significantly impact customer services. The plan is reviewed and tested on an annual basis.	Inspected the Disaster Recovery Plan and the test results and determined that Productiv has established a Disaster Recovery Plan and tests it on an annual basis.	No exceptions noted.
		9.1E	Productiv mitigates the potential risk of disruption to the business by maintaining a cyber-security insurance that helps address lengthy business disruptions.	Inspected Productiv's cyber-security insurance policy and determined that Productiv mitigates the potential risk of disruption to the business by maintaining a cyber-security insurance.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	9.2A	Management completes a Vendor Management Checklist to evaluate vendor security controls as part of the vendor onboarding process.	Inspected the completed Vendor Management Checklists for a selection of vendors to determine vendors were evaluated as part of the vendor onboarding process.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Security (Common Criteria) Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Common Criteria Related to Risk Mitigation					
		9.2B	Management performs due diligence during onboarding and annually thereafter, such as obtaining third-party attestation reports to monitor subservice organizations who are critical to supporting the delivery of Productiv services and the security of customer data. Reports or security questionnaires are reviewed for issues or findings that might impact customer services, compliance, and access.	Inspected a vendor review ticket for a selection of vendors and determined that management performs due diligence, such as obtaining third-party attestation reports before granting subservice organizations access to production data.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Availability Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Criteria Related to Availability					
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	A1.1A	Production environment resources are configured to be distributed across multiple host-provider availability zones to help provide Platform and service redundancy.	Inspected the production resource availability zone configurations and determined that production environment resources are configured to be distributed across multiple host-provider availability zones.	No exceptions noted.
		A1.1B	Production environment resources are configured with host-provider auto scaling to automatically adjust capacity as-needed, and to help ensure that server configuration deviations do not occur and consistent baseline standards are maintained.	Inspected the production environment resource auto scaling configurations and determined that production environment resources are configured with host-provider Auto Scaling.	No exceptions noted.
		A1.1C	Productiv utilizes a system performance monitoring tool to monitor Platform capacity and performance and provide alerts to the Security team on a real-time basis. Performance and capacity issues are assigned remediating actions as needed and tracked to resolution.	Inspected the capacity and performance monitoring tool dashboard, configurations, and an example alert and determined that Productiv utilizes a system performance monitoring tool to monitor Platform capacity and performance and provide alerts to the Security team on a real-time basis.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Availability Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Criteria Related to Availability					
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	A1.2A	Production environment resources are configured to be distributed across multiple host-provider availability zones to help provide Platform and service redundancy.	Inspected the production resource availability zone configurations and determined that production environment resources are configured to be distributed across multiple host-provider availability zones.	No exceptions noted.
		A1.2B	Production environment resources are configured with host-provider Auto Scaling to automatically adjust capacity as-needed, and to help ensure that server configuration deviations do not occur and consistent baseline standards are maintained.	Inspected the production environment resource Auto Scaling configurations and determined that production environment resources are configured with host-provider Auto Scaling.	No exceptions noted.
		A1.2C	Productiv utilizes a system performance monitoring tool to monitor Platform capacity and performance and provide alerts to the Security team on a real-time basis. Performance and capacity issues are assigned remediating actions as needed and tracked to resolution.	Inspected the capacity and performance monitoring tool dashboard, configurations, and an example alert and determined that Productiv utilizes a system performance monitoring tool to monitor Platform capacity and performance and provide alerts to the Security team on a real-time basis.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Availability Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Criteria Related to Availability					
		A1.2D	Productiv configures its production databases containing customer data for continuous backups, which are configured to be stored for 35 days at the cloud platform.	Inspected the backup configurations for production databases containing customer data and determined that Productiv configures its production databases containing customer data for continuous backups, which are stored for 35 days at the cloud platform.	No exceptions noted.
		A1.2E	Productiv uses a managed DDoS protection service to help safeguard the Platform.	Inspected the DDoS protection service configuration and determined that Productiv uses a managed DDoS protection service to help safeguard the Platform.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	A1.3A	Productiv has established a Disaster Recovery Plan to address operating procedures during events that significantly impact customer services. The plan is reviewed and tested on an annual basis.	Inspected the Disaster Recovery Plan and the most recent test results and determined that Productiv has established a Disaster Recovery Plan and tests on an annual basis.	No exceptions noted.
		A1.3B	Production environment resources are configured to be distributed across multiple host-provider availability zones to help provide Platform and service redundancy.	Inspected the production resource availability zone configurations and determined that production environment resources are configured to be distributed across multiple host-provider availability zones.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Confidentiality Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Criteria Related to Confidentiality					
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	C1.1A	Production databases are configured to be stored encrypted at the cloud platform.	Inspected the encryption configuration for a selection of production databases and determined that production databases are stored encrypted at the cloud platform.	No exceptions noted.
		C1.1B	Management establishes formal policies and standards to support the security, confidentiality, and availability of the Platform. These policies are approved by the CTO.	Inspected the security-related policies and determined that management establishes formal policies and standards to support the Platform and policies are approved by the CTO.	No exceptions noted.
		C1.1C	Management communicates data handling expectations for confidential data to internal personnel and requires them to sign Productiv's confidentiality policy upon hire.	Inspected a selection of signed Offer Letters containing the confidentiality policy and determined that management requires internal personnel to sign Productiv's confidentiality policy within the Company's online payroll, benefits and HR solution.	No exceptions noted.
		C1.1D	Productiv has established a Records Retention, Archival and Destruction Policy to define requirements for storage and disposal of records in adherence to a defined schedule.	Inspected the Records Retention, Archival and Destruction Policy and determined that Productiv has established a standard to define requirements for storage and disposal of records in adherence to a defined schedule.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Confidentiality Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Criteria Related to Confidentiality					
		C1.1E	Productiv enforces encryption of data transmitted from their Platform to the user's web browser.	Inspected the transfer protocol for each production service load balancer and determined that transmission of customer data is performed using industry-standard encryption technology.	No exceptions noted.
		C1.1F	Production data is anonymized when used in non-production environments.	Inspected the data-masking configuration and a selected masked data export and determined that production data is anonymized when used in non-production environments.	No exceptions noted.
		C1.1G	The Platform is configured to restrict customer access to their own accounts.	Reperformed for a test production account, logging in and attempting to access a customer's production account, to determine that the Platform is configured to restrict customer access to their own accounts.	No exceptions noted.
		C1.1H	On a quarterly basis, the CTO reviews internal user access to the source code repository and the production Platform to verify that permissions are valid.	Inspected documentation for a selection of quarterly Platform access reviews and determined that the CTO reviews internal user access to the source code repository and the production Platform and determined that permissions are valid.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Confidentiality Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Criteria Related to Confidentiality					
		C1.1I	Access to backups of customer data is restricted to the Engineering team through AWS IAM.	Inspected the list of users with access to Productiv backups and compared a selection of users to the list of employees and determined that access to backups of customer data is restricted to the Engineering team through AWS IAM.	No exceptions noted.
		C1.1J	Administrator access to the AWS management console is restricted to appropriate personnel and requires two-factor authentication.	Inspected the list of users with administrator access to the AWS account and compared the users against the list of employees and determined that administrator access to the AWS management console is restricted to appropriate personnel and that two-factor authentication is enforced.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	C1.2A	Productiv has established a Records Retention, Archival and Destruction Policy to define requirements for storage and disposal of records in adherence to a defined schedule.	Inspected the Records Retention, Archival and Destruction Policy and determined that Productiv has established a standard to define requirements for storage and disposal of records in adherence to a defined schedule.	No exceptions noted.

Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

Criteria Related to the Confidentiality Category

Criteria	Trust Services Criteria	Control Number	Controls Specified by Productiv, Inc.	Tests of Controls Performed by BDO USA, LLP	Results of Tests
Criteria Related to Confidentiality					
		C1.2B	Productiv has a process to track and purge customer data upon contract termination from the Platform.	Inspected a selection of data deletion tickets and the deletion scripts and determined that Productiv has a process to track and purge customer data upon contract termination from the Platform.	No exceptions noted.

V. Other Information Provided by Productiv, Inc. That Is Not Covered by the Independent Service Auditor's Report

Other Information Provided by Productiv, Inc. That Is Not Covered by the Independent Service Auditor's Report

Management's Response to Exceptions

Control Number	Criteria	Trust Services Criteria	Controls Specified by Productiv, Inc.	Results of Tests	Management Response
A 1.1	CC1.1	The entity demonstrates a commitment to integrity and ethical values.	New hires are required to read and acknowledge the Employee Handbook during the first week of onboarding. The Employee Handbook includes a code of conduct and the consequences of noncompliance with policies and procedures and is available to employees on Productiv's internal document repository.	Exceptions noted. Four of seven new hires selected for testing did not acknowledge the Employee Handbook during the first week of onboarding.	During the COVID-19 pandemic, we experienced a delay in having employees who joined in the March-May 2020 timeframe sign the Employee Handbook. Since that time, all new employees have signed the handbook. We have implemented an improved process to help ensure that all new employees sign the Employee Handbook within 7 days.