360 ADVANCED

SOC 3® Report on Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy for Compliance Management Software as a Service – KCM GRC

KnowBe4, Inc.

March 16, 2019 to March 15, 2020

KnowBe4
Human error. Conquered.

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations™

KNOWBE4, INC.

Table of Contents

SECTION 1:

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S SOC 3® REPORT RELEVANT TO SECURITY, AVAILABILITY, PROCESSING INTEGRITY, CONFIDENTIALITY, AND PRIVACY

To KnowBe4, Inc.:

Scope

We have examined KnowBe4, Inc.'s ("KnowBe4") assertion included in Section 2 of this report that the controls within KnowBe4's Compliance Management Software as a Service ("KCM GRC") system were effective throughout the period March 16, 2019 to March 15, 2020, to provide reasonable assurance that KnowBe4's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (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*).

KnowBe4 uses the following sub-service organizations: (1) Amazon Web Services, Inc. ("AWS") for application hosting, backups, and cloud storage services; and (2) Datadog, Inc. ("Datadog") for application log monitoring, system logging, and analytics services. KnowBe4's assertion and description of the boundaries of the KCM GRC system, included in Section 2 and Section 3 of this report, respectively, indicate that certain applicable trust services criteria can only be met if certain types of controls at the aforementioned sub-service organizations are suitably designed and operating effectively. The description does not include any of the controls expected to be implemented at the sub-service organizations. Our examination did not extend to the services provided by the sub-service organizations, and we have not evaluated whether the controls management expects to be implemented at the sub-service organizations have been implemented or whether such controls were suitability designed and operating effectively throughout the period March 16, 2019 to March 15, 2020.

Service Organization's Responsibilities

KnowBe4 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 KnowBe4's service commitments and system requirements were achieved. KnowBe4 has also provided the accompanying assertion titled "Management's Assertion" included in Section 2 of this report about effectiveness of controls within the system. When preparing its assertion, KnowBe4 is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve KnowBe4's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve KnowBe4's service commitments and system requirements based on the applicable trust services criteria

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

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that 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 conclusion about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within KnowBe4's KCM GRC system were effective throughout the period March 16, 2019 to March 15, 2020, to provide reasonable assurance that KnowBe4's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

April 15, 2020
St. Petersburg, Florida

SECTION 2:

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

April 15, 2020

We are responsible for designing, implementing, operating, and maintaining effective controls with KnowBe4, Inc.'s ("KnowBe4") Compliance Management Software as a Service ("KCM GRC") system throughout the period March 16, 2019 to March 15, 2020, to provide reasonable assurance that KnowBe4's service commitments and system requirements relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy were achieved. Our description of the boundaries of the system is presented in Section 3 of this report and identifies the aspects of the system covered by our assertion. KnowBe4 uses the following sub-service organizations: (1) Amazon Web Services, Inc. ("AWS") for application hosting, backups, and cloud storage services; and (2) Datadog, Inc. ("Datadog") for application log monitoring, system logging, and analytics services. The description included in Section 3 excludes the applicable trust services criteria and related controls of the sub-service organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period March 16, 2019 to March 15, 2020, to provide reasonable assurance the KnowBe4's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). KnowBe4's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section 4 of this report.

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

We assert that the controls within the system were effective throughout the period March 16, 2019 to March 15, 2020, to provide reasonable assurance that KnowBe4's service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/ KnowBe4, Inc.

Brian Jack – Chief Information Security Officer

SECTION 3:

KNOWBE4'S DESCRIPTION OF THE BOUNDARIES OF THE SYSTEM

OVERVIEW OF OPERATIONS AND THE SYSTEM

Company Overview and Background

KnowBe4 is a provider of an integrated security awareness training and simulated phishing platform along with the Governance Risk and Compliance (KCM GRC) platform. Founded by data and IT security expert Stu Sjouwerman, with backing from Elephant Partners and Goldman Sachs Growth Equity, KnowBe4 helps organizations address the human element of security by raising awareness of ransomware, CEO fraud, and other social engineering tactics through a new-school approach to security awareness training. Kevin Mitnick, internationally recognized computer-security expert and KnowBe4's Chief Hacking Officer, helped design KnowBe4's training based on his documented social engineering tactics. Thousands of organizations leverage KnowBe4's platform to train their workforce to make smarter security decisions and create a human firewall as an effective last line of defense. The KCM GRC platform supplements the awareness practice and is a stand-alone product used for compliance, risk, and governance processes.

Overview of the KCM GRC system

The KCM GRC is designed to simplify the complexity of getting compliant and ease the burden of staying compliant year-round. Pre-built requirement templates are designed to enable clients to implement the system efficiently. Control owners can be assigned responsibility for the controls under their management. Dashboards with automated reminders are available for quick viewing of tasks that have been completed, not met, and are past due. Automated email reminders are configurable for users to manage their compliance initiatives.

Key Features of KCM GRC include:

- Managing Governance, Audits, and Compliance – KCM GRC is designed to aid in the management of one or more compliance initiatives. KCM GRC also aids in the management of internal policies and procedures, as well as an internal risk framework. KCM GRC is designed to reduce the time needed to satisfy requirements necessary to meet compliance goals, leading to increased efficiencies with maintaining compliance.
- Compliance Requirements Templates – KCM GRC includes pre-built requirements templates for several regulations. Templates are created and / or updated as regulations change.
- Evidence Repository and DocuLinks – KCM GRC provides two ways of maintaining audit evidence and documentation. Users can either upload files to be securely stored in the cloud or provide a URL that links to an existing document or location of evidence files. The Evidence Repository allows users to safely and securely store policies, procedures, and compliance/audit evidence for each control and task. Audit evidence being available for auditors to review, reduces the amount of time an auditor has to spend on-site.
- Compliance Dashboards with Automated Reminders – KCM GRC Compliance Dashboards allow users to see what tasks have been completed, tasks that have not been met, and tasks that are past due. Automated email reminders can be configured to notify users of any gaps in compliance that need to be addressed.
- Job Completion – KCM GRC's automation of processes are intended to save time and create efficiencies for users. KCM GRC enables users to assign responsibility for controls to the personnel who are responsible for maintaining those controls. KCM GRC can be configured to assign an approving manager to ensure that the documentation the user is providing is acceptable for audit evidence. This feature identifies the employee responsible for maintaining compliance related to each control and provides accountability over the quality of the documentation being provided.
- Policy Workflow Management – KCM GRC allows owners to upload a finalized policy, select a targeted list of users, and generate user reports to satisfy compliance requirements. Policy campaigns can be created to manage policy distribution, reminders, and user acknowledgement process from a centralized repository.

- Risk Management – KCM GRC includes a risk management module that is based on NIST 800-30. The interface and wizards are available for users to aid in risk identification, risk response and risk monitoring.
- Vendor Management - KCM includes a vendor management module that lets users centralize your third-party risk management processes. Users can prequalify risk, assess your vendors, and conduct remediation efforts all in one platform. Users can set a frequency for how often your vendors are assessed to continually monitor the associated risk.

Sub-Service Organizations and Complementary Controls

KnowBe4 uses the following sub-service organizations: (1) Amazon Web Services, Inc. ("AWS") for application hosting, backups, and cloud storage services; and (2) Datadog, Inc. ("Datadog") for application log monitoring, system logging, and analytics services. To monitor and evaluate the adequacy and effectiveness of controls in place at the sub-service organization, KnowBe4's management obtains and reviews the Service Auditor's report and / or compliance certifications for the sub-service organizations.

The sub-service organizations are responsible for implementing logical, physical, and environmental control activities to ensure KnowBe4's IT infrastructure is protected from certain threats. The sub-service organizations are also responsible for implementing administrative, physical, and technical safeguards to protect the services and prevent the accidental loss or unauthorized access, use, alteration, or disclosure of customer data under its control.

Infrastructure

KnowBe4's systems run in the cloud and do not run their own routers, load balancers, DNS servers, or virtual systems. Except for a few data sub-processors, services, and data are hosted in AWS facilities. For US-based customers and customers wanting to keep their data residing in the US, KnowBe4 has systems in AWS datacenters in the US region. For customers wanting to keep their data within the European Union (EU), except for a small set of sub-processors that are US only, KnowBe4 has systems located in AWS datacenters in the EU region. KnowBe4's systems are built taking into consideration both business continuity and disaster recovery. The IT infrastructure, including systems and databases, is spread across multiple AWS data centers (availability zones) for both the US and EU regions for redundancy and continuity purposes. Systems are within KnowBe4's own virtual private cloud (VPC) with network access control lists (ACLs) to prevent unauthorized requests gaining access to the internal network.

KnowBe4 uses the AWS Fargate platform as a service. AWS Fargate is a serverless compute engine for Amazon Elastic Container Service (ECS) that allows KnowBe4 to run containers without having to provision, configure, and scale clusters of Virtual Machines (VMs). The service runs in the cloud, eliminating the need for infrastructure management. Fargate manages the underlying infrastructure and clusters. It also automatically scales the application based on demand. Fargate eliminates the need to scale, monitor, patch, and secure EC2 instances.

Data communications between the web customers and KnowBe4's backend systems are encrypted – which protects data in transit. Data is held in an encrypted Amazon Relational Database Service (RDS), which provides for availability and data durability. Storage is provided by encrypted Amazon Simple Storage Service (S3) buckets dedicated to KnowBe4. Encryption is enabled to protect data at rest.

Software

The KCM GRC platform is offered as a SaaS-based application built using a combination of web programing technologies and leveraging AWS infrastructure. KCM GRC is developed internally by the Engineering Development team of KnowBe4. The Engineering Development team maintains and enhances the feature sets of KCM GRC on an on-going basis to provide a platform for clients to manage their governance, audit and compliance processes.

Components are written using standard frameworks and languages.

People

KnowBe4 has nine main divisions: (1) Executive Team; (2) Marketing and Public Relations; (3) Revenue; (4) People Operations / Human Resources; (5) Finance; (6) Research & Development; (7) Product; (8) Courseware; and (9) Quality and Growth.

The roles and responsibilities of key functions include the following:

- Chief Executive Officer (CEO): The CEO oversees the executive team and is responsible for strategic vision and execution of the organization.
- Chief Product Officer (CPO): The CPO is Head of Engineering, Support and Product Management. Responsible for tech direction of products and customer facing issues.
- Chief Information Security Officer (CISO): The CISO is responsible for security and risk related issues for the company and for the product. Responsible for privacy related issues.
- Chief Financial Officer (CFO): The CFO is head of finance, accounting, and order processing.
- Corporate Legal Counsel: Responsible for contracts, privacy, agreements, internal and external matters regarding litigation.
- SVP of Engineering: Responsible for leading and mentoring the Software Development, Quality Assurance, and Site Reliability Engineering teams.
- SVP of People Operations: Responsible for directing all of the people functions of the organization in accordance with the policies and practices of KnowBe4.
- SVP of Property Operations: Responsible for handling all facility needs for the organization, including planning, budgeting, and scheduling the facility modifications to align with the growth plans for the organization.

Procedures

KnowBe4's management has developed and communicated to its users, procedures to restrict logical access to KnowBe4's systems. The procedures cover the following key security lifecycle areas:

- Policy management and communication.
- Selection, documentation, and implementation of security controls.
- Authorization, changes to, and termination of information system access.
- Monitoring security controls.
- Management of access and roles.
- Maintenance and support of the security system and necessary backups and media storage.
- Incident response.
- Maintenance of restricted access to system configurations, administrative functionality, passwords, powerful utilities, and security devices.
- HR policies including conduct and ethics, computer usage, disciplinary actions, non-disclosure / confidentiality.

INFRASTRUCTURE MANAGEMENT

Physical Security

Entrances to the KnowBe4 suites are controlled by a biometric access system. Employees and contractors who need access to the offices are registered in the system and their fingerprints recorded. Access is granted as employees are hired and is revoked as a regular part of the termination process.

Afterhours access to the KnowBe4 suits requires a key fob for access to the building or use of a PIN for elevator access to the suites. Visitors required to sign-in at the reception desk and wear a visitor badge while on-site.

A security camera system in place that records access to, and throughout the KnowBe4 suites. Security guards employed by KnowBe4 are on premises during business hours. Third party security personnel are contracted to patrol the suites after hours. Security coverage of KnowBe4 spaces is available 24 hours a day. A third-party alarm system is in place and continuously monitored for physical security breaches. Triggered alarms or other identified security incidents are immediately reported to on-duty security personnel or the Director of Physical Security using a dedicated phone line.

Development and Change Management

KnowBe4 has implemented a formal change management process that will allow staff to request, manage, approve, and control changes that modify services or systems within the KnowBe4 environments. The change control process is designed to enforce key development controls each time a change to the software is made including development and emergency changes. The change management process begins with the identification, recording, and classification of the change, and continues with its review and approval, test, and staging for implementation. Once implementation has been completed, measured, and reported, the change process is complete.

The Engineering Development team has been structured to promote communication through each stage in the design process. This results in the Management Team ultimately being responsible for ensuring development initiatives meet client needs and strategic direction of the application including transition from concept to production functionality. A code repository (change control software) tool is utilized and is combined with documentation of each release which provides for the ability to quickly revert to a previously functioning state version in the event that new code does not function as intended at any point in the development process.

Backups

KnowBe4's backup and recovery infrastructure is hosted and utilizes the combination of S3 and Amazon Relational Database Service (RDS) which provides resizable database capacity with scalable and efficient data storage infrastructure.

Information Security

Information security policies have been established to set the overall framework for managing security of the IT infrastructure and applications. These policies are approved at the executive management level and establish standards for information security throughout KnowBe4's information resources. The Engineering Development team has primary responsibility for interpreting these standards, developing procedures, and processes for implementing the standards, and overseeing logical security for KnowBe4 IT and applications.

Employees who no longer require access to the AWS environment are deactivated upon notification. Quarterly access reviews are also performed to ensure access to systems within the environment are appropriate.

KnowBe4's production systems are virtualized and hosted by AWS. Amazon Fargate combined with Amazon S3 supports several mechanisms that allow flexibility to how access to data is controlled as well as how, when, and where it can be accessed.

Data Communications

The internal network is protected from public internet traffic via stateful inspection firewalls provided by AWS. A security group acts as a firewall that controls the traffic allowed into a group of instances. For each security group, custom rules are added that govern the allowed inbound traffic to instances in the group. All other inbound traffic is denied.

Encrypted communications are utilized to protect remote internet sessions to the KnowBe4 applications and internal network. Encryption is used to ensure the privacy and integrity of the data being passed over the public network.

Incident Response

KnowBe4 maintains documented incident response procedures to guide personnel through identification, response, and resolution of breaches, events, and incidents. Identified incidents are recorded and tracked within a ticketing system through their resolution.

Disaster Recovery

KnowBe4 maintains a formal Business Continuity Plan and Disaster Recovery plan that outlines the roles and responsibilities of employees, communication plans, and emergency monitoring and activation procedures to be employed in the event of an unexpected disruption in normal operations. An Emergency Support Team has been assembled to ensure the safety of the staff, maintain business continuity, and communicate to internal and external customers.

Data

Customer data is stored in a multi-tenant multi-schema database architecture. Single database with individual customer tables. Privacy controls exist in the application code to ensure data privacy and prevent one customer from accessing another customer's data. This is done using unique account identifiers which attribute each user to a specific account. Knowbe4 has unit and integration tests in place to ensure these privacy controls work as expected. Unit and integration tests are run each time the code base is updated, and any single test failing will prevent new code being shipped to production.

SECTION 4:

SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

KnowBe4's management designs its processes and procedures related to KCM GRC system to meet its objectives. Those objectives are based on the service commitments that KnowBe4's management makes to user entities, the laws and regulations that govern the provision of the KCM GRC system and the financial, operational, and compliance requirements that KnowBe4 has established for the services.

KnowBe4's management establishes operational requirements that support the achievement of security, availability, processing integrity, confidentiality, and privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated via KnowBe4's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the system. Management retains legal counsel to provide guidance on legal matters affecting services.