360ADVANCED

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

KnowBe4, Inc.

November 16, 2018 to March 15, 2019

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 1

SECTION 2: MANAGEMENT'S ASSERTION 4

SECTION 3: DESCRIPTION OF THE BOUNDARIES OF THE SYSTEM 6

OVERVIEW OF OPERATIONS AND THE SYSTEM 7
Company Overview and Background..7
Overview of the Compliance Management SaaS system...7
Sub-Service Organizations and Complementary Controls 8
Infrastructure 8
Software 8
People 8
Procedures 9
Data...9

SECTION 4: SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 10

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS.............11

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 (SaaS) system were effective throughout the period November 16, 2018 to March 15, 2019, 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 Amazon Web Services, Inc. ("AWS"), a sub-service organization, for application hosting, backups, and cloud storage services. KnowBe4's assertion and description of the boundaries of the Compliance Management SaaS 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 organization are suitably designed and operating effectively. The description does not include any of the controls expected to be implemented at the sub-service organization. Our examination did not extend to the services provided by the sub-service organization, and we have not evaluated whether the controls management expects to be implemented at the sub-service organization have been implemented or whether such controls were suitability designed and operating effectively throughout the period November 16, 2018 to March 15, 2019.

Service Organization's Responsibilities

KnowBe4's management 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's management 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's management 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 Compliance Management SaaS system were effective throughout the period November 16, 2018 to March 15, 2019, 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.

360 Advanced

April 17, 2019
St. Petersburg, Florida

SECTION 2:

MANAGEMENT’S ASSERTION

MANAGEMENT'S ASSERTION

April 17, 2019

We are responsible for designing, implementing, operating, and maintaining effective controls with KnowBe4, Inc.'s ("KnowBe4") Compliance Management Software as a Service (SaaS) system throughout the period November 16, 2018 to March 15, 2019, 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 Amazon Web Services, Inc. ("AWS"), a sub-service organization, application hosting, backups, and cloud storage services. The description included in Section 3 excludes the applicable trust services criteria and related controls of the sub-service organization.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 16, 2018 to March 15, 2019, 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 is 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 November 16, 2018 to March 15, 2019, 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:

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 Compliance Management SaaS 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 include:

- Managing Governance, Audits, and Compliance - KCM is designed to aid in the management of one or more compliance initiatives. KCM also aids in the management of internal policies and procedures, as well as an internal risk framework. KCM 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 includes pre-built requirements templates for several regulations. Templates are created and / or updated as regulations change.
- Evidence Repository and DocuLinks - KCM 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 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's automation of processes are intended to save time and create efficiencies for users. KCM enables users to assign responsibility for controls to the personnel who are responsible for maintaining those controls. KCM 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 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 includes a risk management module that is based on is based on NIST 800-30. The interface and wizards are available for users to aid in risk identification, risk response and risk monitoring.

Sub-Service Organizations and Complementary Controls

KnowBe4 uses Amazon Web Services, Inc. (“AWS”), a sub-service organization, for application hosting, backups, and cloud storage 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 organization.

The sub-service organization is responsible for implementing logical, physical, and environmental control activities to ensure the IT infrastructure is protected from certain threats.

Infrastructure

KnowBe4’s services 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 is hosted in AWS facilities. KnowBe4 has systems and processes hosted in AWS datacenters in the US East region. KnowBe4’s services are built taking into consideration both business continuity and disaster recovery. The IT infrastructure, including systems and databases, are spread across multiple AWS availability zones 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.

Data communications between the web clients and KnowBe4’s backend systems are encrypted using SSL/TLS – 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.

The following describes the in-scope components supporting the Compliance Management SaaS system:

System / Application	Description	Infrastructure
KCM GRC	Compliance Management	AWS Cloud Infrastructure and AWS Relational Databases

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 is developed internally by the Product & Software Development teams of KnowBe4. The Software Development team maintains and enhances the feature sets of KCM on an on-going basis to provide a platform for clients to manage their governance, audit and compliance processes.

Components are written using PHP, Yii Framework, MySQL, Postgresql, Nginx, and Linux.

People

KnowBe4 has nine main divisions: (1) Executive Team; (2) Marketing; (3) Sales; (4) Customer Success; (5) Support; (6) Engineering; (7) Quality and Training; (8) Accounting and Finance; and (9) Operations.

The roles and responsibilities of key functions include the following:

- Chief Executive Officer: Sjoerd Sjouwerman, Oversees the executive team.
- Chief Technology Officer: Alin Irimie, Responsible for technical direction of the company.

- Chief Product Officer: Gregory Kras, Head of Engineering, Support and Product Management. Responsible for tech direction of products and customer facing issues.
- Chief Information Security Officer: Brian Jack, Responsible for security and risk related issues for the company and for the product. Responsible for privacy related issues.
- Chief Financial Officer: Krish Venkataraman, Head of finance, accounting, and order processing.
- Corporate Legal Counsel: Alicia Dietzen, Contracts, privacy, agreements, internal and external matters regarding litigation.

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

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 Compliance Management SaaS 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 Compliance Management SaaS 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 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.