



SOC 3<sup>®</sup> 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, 2021 TO MARCH 15, 2022*



# KNOWBE4, INC.

## Table of Contents

<b>SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT .....</b>	<b>1</b>
<b>SECTION 2: MANAGEMENT'S ASSERTION .....</b>	<b>4</b>
<b>SECTION 3: DESCRIPTION OF THE BOUNDARIES OF THE SYSTEM .....</b>	<b>6</b>
OVERVIEW OF OPERATIONS AND THE SYSTEM .....	7
Company Overview and Background.....	7
Overview of the KCM GRC system.....	7
Sub-Service Organizations and Complementary Controls .....	8
Infrastructure .....	8
Software .....	9
People .....	9
Procedures.....	10
Data.....	12
<b>SECTION 4: SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS .....</b>	<b>14</b>

---

**SECTION 1:**

**INDEPENDENT SERVICE AUDITOR'S REPORT**

## INDEPENDENT SERVICE AUDITOR'S REPORT

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, 2021 to March 15, 2022, 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, web application firewall, 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 suitably designed and operating effectively throughout the period March 16, 2021 to March 15, 2022.

### **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, 2021 to March 15, 2022, 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.

A handwritten signature in black ink that reads "360 Advanced". The signature is written in a cursive, flowing style.

April 25, 2022  
St. Petersburg, Florida

---

**SECTION 2:**

**MANAGEMENT'S ASSERTION**

## MANAGEMENT'S ASSERTION

April 25, 2022

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, 2021 to March 15, 2022, 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, web application firewall, 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, 2021 to March 15, 2022, 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, 2021 to March 15, 2022, 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 (Nasdaq: KNBE) is the world's first and largest new-school security awareness training and simulated phishing platform (KMSAT); lightweight security orchestration, automation, and response platform (PhishER); along with the Governance Risk and Compliance (KCM GRC) platform. Founded by data and IT security expert Stu Sjouwerman, 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

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. Email reminders are automatically sent to 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 are sent 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 the third-party risk management processes. Users can prequalify risk, assess vendors, and conduct remediation efforts in one platform. Users can set a frequency for how often 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 are in the AWS cloud and KnowBe4 does not host their own routers, load balancers, DNS servers, or virtual systems within the datacenter. Except for a small number of data sub-processors, services and all data are hosted in AWS facilities. KnowBe4 has systems and processes hosted in AWS data centers in the US East region. For customers wanting to keep their data within the United Kingdom (UK) except for a small set of sub-processors that are US only, KnowBe4 has systems located in AWS data centers in the UK region. KnowBe4’s systems 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.

Note that the primary datacenter for European customers is UK London with the backup and recovery site in Ireland.

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. AWS Fargate manages the underlying infrastructure and clusters. It also automatically scales the application based on demand. AWS Fargate eliminates the need to scale, monitor, patch, and secure EC2 instances.

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 table describes the in-scope components supporting the KCM GRC system:

System / Application	Description
AWS	Application hosting, backups, and cloud storage services
Airbrake	Application error monitoring
Datadog	Application log monitoring, system logging, and analytics
Salesforce	CRM
Zendesk	Ticketing system
Mixpanel	Business analytics
Pendo	Analytics
LaunchDarkly	Deploying new features through 'feature-flagging'.

## Software

The KCM GRC platform is offered as a SaaS-based application built using a combination of web programming 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 sectors: (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 / Chief Cloud Officer (CPO / CCO): The CPO / CCO is Head of Engineering, Support and Product Management as well as the internal IT department. The CPO / CCO is responsible for tech direction of products and customer facing issues.
- Chief Information Security Officer / Privacy Officer (CISO / DPO): The CISO / DPO is responsible for security and risk related issues for the company and for the product. The CISO / DPO is 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.
- EVP of Engineering: Responsible for leading and mentoring the Software Development, Quality Assurance, and Site Reliability Engineering teams.
- Chief Human Resources Officer (CHRO): Responsible for directing the people functions of the organization in accordance with the policies and practices of KnowBe4.

## 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

## TRANSACTION PROCESSING

To ensure proper setup and use of the system, KnowBe4 provides end users with product training material prior to initial use. Ongoing support of the system is provided and requests for assistance and / or issues are tracked through a ticketing system. The application also provides the ability for authorized administrative end users to control their team's access based on roles and permissions thus providing the ability to ensure data maintains its confidentiality and access is limited by need.

Multiple input fields within the application accept user data. Before data is entered and accepted by the system, it is required to pass validity checks. The validity checks ensure the data meets requirements of the relative field, and / or does not conflict with existing data already within the system. Errors result in immediate on-screen feedback to assist users in resolving data input issues easily and timely.

Where normalized input is required, the application is configured with dropdown lists for selection by the user. These dropdowns prevent users from making invalid entries that require normalized data.

Once data is input into the application, controls are assigned an owner and the status of controls are tracked through completion. Task reminder emails are automatically sent for assigned tasks in the application. The system notifies users when a task has been assigned to them and tracks their timeline and progress. Detailed reports are available and generated on-demand by the application user. The application provides the ability to track activity through completion and displays these activities within the dashboard.

## 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. After-hours access to the KnowBe4 suites requires a key fob for access to the building or use of a PIN for elevator access to the suites. Visitors are required to sign-in at the reception desk and wear a visitor badge while on-site. Employees are also required to display a company supplied badge while on-site.

A security camera system is in place that records access to, and throughout the KnowBe4 suites. Security camera footage is available for at least 30 days. Camera footage can be reviewed by KnowBe4 security personnel as needed.

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 promptly 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.

The code repository tool facilitates the development processes by systematically enforcing access controls, testing requirements, approvals, and deployments. Development work is done in a segregated environment. Failure of any tests, or failure to get approval as defined within the workflow prevents the code from further progression within the code repository tool. Once the change has passed testing and the required approvals have been obtained, it is ready for deployment. Product teams have authorization to deploy code only through the code repository tool which systematically enforces testing and approval rules prior to migration to production. Access to the production operating system and database systems is restricted to the infrastructure support teams.

### 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. RDS snapshots are used for launching RDS instances. In case of instance failure, stored RDS snapshots can be used to promptly launch another instance, thereby allowing for fast recovery and business continuity. Amazon RDS also uses Amazon S3 to store snapshots (backup copies) of the data volumes. Snapshots are used for recovering data in case of application or system failures. Snapshots can also be used as a baseline to create multiple new data volumes, expand the size of an existing data volume, or move data volumes across multiple Availability Zones, thereby making data usage highly scalable.

### 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. In addition, the Engineering Development team develops configuration standards for each type of hardware and associated system software. User administration processes for IT systems and applications are tied to the new hire and termination processes established by KnowBe4. Role based access controls for least privilege with additional control requirements for single-sign-on (SSO), MFA, IP restrictions, and VPN have been defined.

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. A formal termination process has been implemented to ensure timely removal of access to systems.

KnowBe4's production systems are virtualized and hosted by AWS. AWS 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. Amazon S3 provides four different access control mechanisms: Identity and Access Management (IAM) policies, ACLs, bucket policies, and query string authentication. IAM enables organizations with multiple employees to create and manage multiple users under a single AWS account. With IAM policies, IAM users can be granted fine-grained control to Amazon S3 buckets or objects. ACLs can be used to selectively grant certain permissions on individual objects. Amazon S3 Bucket Policies can be used to grant or deny permissions across some or all of the objects within a single bucket.

Amazon S3 supports logging of requests made against Amazon S3 resources. Amazon S3 buckets can be configured to create access log records for the requests made against it. The system access logs capture requests made against a bucket or the objects in it and can be used for auditing purposes.

KnowBe4 utilizes AWS security groups and applies them to systems to deny traffic and only allow specific services to the systems. Web Application Firewalls (WAFs) are also in place and configured to protect against external web-based attacks. WAF rules are applied at AWS CloudFront CDN, as well as within the application itself (in-app WAF).

#### Data Communications

The internal network is protected from public internet traffic via stateful inspection firewalls provided by AWS. The firewalls are called security groups in AWS and are configured to deny all traffic and only allow specific services to a specific destination. Access to administer the firewalls is restricted to personnel commensurate with their job responsibilities. 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. Other inbound traffic is denied. Rules for a security group can be modified dynamically and new rules are automatically enforced for existing and future instances in the group.

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. The Emergency Support team conducts a disaster recovery test at least annually in which the Business Continuity and Disaster Recovery plans are tested and examined for areas of opportunity.

## **Data**

Customer data is stored in a multi-tenant single-schema database architecture. A single database with logical segregation of data using account ID fields for each database record. 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.

Policies and procedures are documented to guide personnel in protecting and handling data and assets. Policies include, but not limited to, the following:

- Data Handling and Protection Standards
- Data Retention and Destruction Policy

---

**SECTION 4:**

**SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS**

## PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

KnowBe4's management designs its processes and procedures related to the 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 provisioning of the KCM GRC system and the financial, operational, and compliance requirements that KnowBe4 has established for the services.

Commitments to user entities are documented and communicated in Service Level Agreements (SLAs), licensing agreements, or Master Service Agreements (MSAs), and other customer agreements, as well as in the description of the service offerings online. Commitments and system requirements are standardized and include, but are not limited to, the following:

- Security principles with the fundamental design of the system that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Utilization of multi-factor authentication (MFA) to access confidential data.
- Compliance with General Data Protection Regulation (GDPR).
- Implementing disaster recovery procedures to minimize the effects of an unexpected disruption in business operations.
- Support coverage, response times, and resolution times.
- Implementing vulnerability management and penetration testing protocols.
- Maintaining the confidentiality of client data and non-disclosure to unauthorized persons or entities.
- Encryption of customer and client data in transit and at rest.
- Maintenance and retention of database backups and application logs.

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.