

BLACK KITE

NormShield, Inc. (“Black Kite”)

Independent Service Auditor’s SOC 3 Report
For Black Kite’s Third-Party Risk Intelligence System
For the Period April 1, 2024 to March 31, 2025

SOC 3 ® - SOC for Service Organizations: Trust Services Criteria for General Use Report



DANSA D’ARATA SOUCIA LLP

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITORS' REPORT 3

II. ASSERTION OF THE MANAGEMENT OF NORMSHIELD, INC. 6

III. ATTACHMENT A - BLACK KITE'S BOUNDARIES OF THE SYSTEM 8

IV. ATTACHMENT B - BLACK KITE'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 21

SECTION I:

INDEPENDENT SERVICE AUDITORS' REPORT

INDEPENDENT SERVICE AUDITORS' REPORT

To: **NormShield, Inc.**
Vienna, Virginia

Scope

We have examined NormShield, Inc.'s ("Black Kite") accompanying assertion titled "Assertion of the Management of NormShield, Inc." ("assertion") that the controls within Black Kite's Third-Party Risk Intelligence System ("the System") were effective throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that Black Kite's service commitments and system requirements were achieved based on 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 (With Revised Points of Focus - 2022)* in AICPA, Trust Services Criteria.

Black Kite uses a subservice organization for cloud hosting services. Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Black Kite, to achieve Black Kite's service commitments and system requirements based on the applicable Trust Services Criteria. Attachment A presents the applicable Trust Services Criteria and types of complementary subservice organization controls assumed in the design of Black Kite's controls. Attachment A does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Attachment A indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Black Kite, to achieve Black Kite's service commitments and system requirements based on the applicable trust services criteria. Attachment A presents the applicable Trust Services Criteria and the complementary user entity controls assumed in the design of Black Kite'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

Black Kite 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 Black Kite's service commitments and system requirements were achieved. Black Kite has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Black Kite is responsible for selecting, and identifying in its assertion, the applicable trust service 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 Black Kite'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 Black Kite'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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

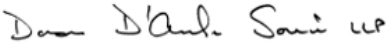
Inherent Limitations

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 conclusions about the suitability of the design and operating 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 Black Kite's Third-Party Risk Intelligence System were effective throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that Black Kite's service commitments and system requirements were achieved based on the applicable Trust Services Criteria is fairly stated, in all material respects.



DANSA D'ARATA SOUCIA LLP
Buffalo, New York
May 13, 2025

SECTION II:

ASSERTION OF THE MANAGEMENT OF NORMSHIELD, INC.



Assertion of the Management of NormShield, Inc.

We are responsible for designing, implementing, operating, and maintaining effective controls within NormShield, Inc.'s ("Black Kite") Third-Party Risk Intelligence System ("the System") throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that Black Kite's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. The boundaries of the System are presented in Attachment A and identifies the aspects of the System covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the System throughout the period April 1, 2024 to March 31, 2025, to provide reasonable assurance that Black Kite'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 (With Revised Points of Focus - 2022)* in AICPA, *Trust Services Criteria*. Black Kite's objectives for the System in applying the applicable Trust Services Criteria are embodied in its service commitments and systems requirements relevant to the applicable Trust Services Criteria. The principal service commitments and system requirements related to the applicable Trust Services Criteria are presented in Attachment B.

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 April 1, 2024 to March 31, 2025, to provide reasonable assurance that Black Kite's service commitments and systems requirements were achieved based on the applicable Trust Services Criteria.

NormShield, Inc.

ATTACHMENT A:

BLACK KITE'S BOUNDARIES OF THE SYSTEM

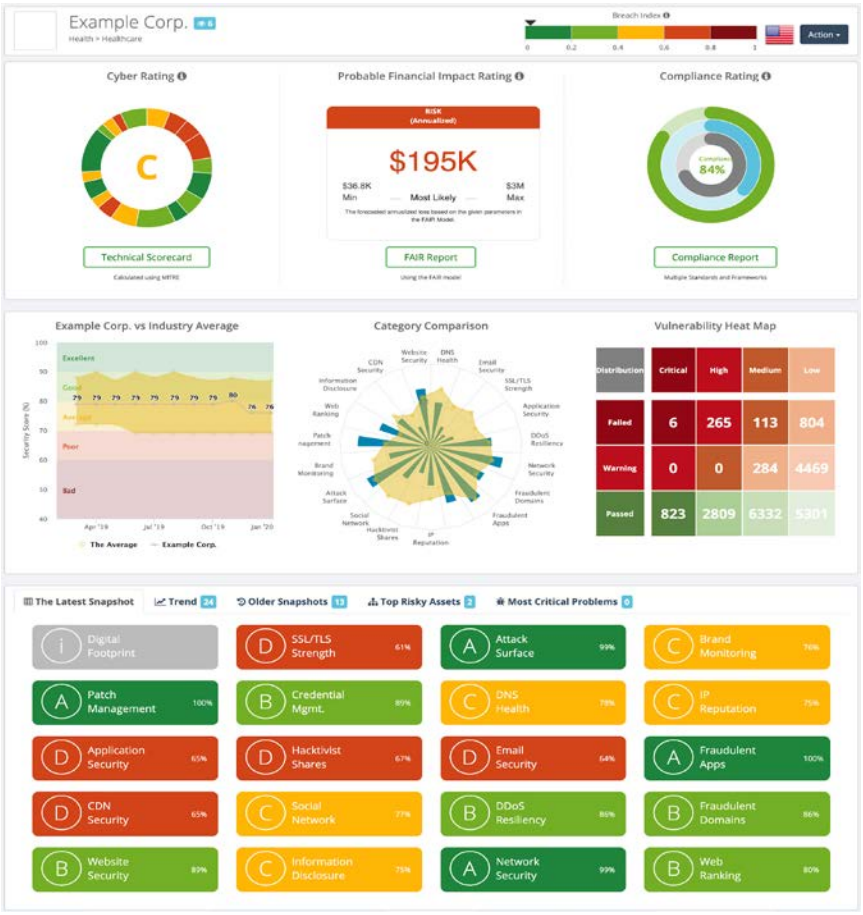
Company Overview and Background

NormShield, Inc. DBA Black Kite ("Black Kite" or "the Company") provides a defensible platform that spans the entirety of the third-party risk management life cycle for cyber risk professionals looking to quantify and maintain visibility of their risk exposure.

Overview of Products and Services

Black Kite's core application, Third-Party Risk Intelligence System ("TRIS", "the System" or "the Platform"), is a multi-user, transaction based application suite that gives companies a multi-dimensional view of risk throughout their third-party cyber ecosystem through:

- Risk Score: An easy-to-understand letter grade system based on industry standards and best practices (NIST, MITRE CVSS, OpenFAIR, etc.) evaluating risk across 20 categories.
- Risk Quantification: Calculation of probable financial impact of a cyber breach using Open FAIR™.
- Compliance Engines: Automated compliance analysis powered by a cyber-aware AI engine.
- Automated Cyber Assessments: AI-powered parsing of vendor documentation mapped to assessment criteria for fast and accurate evaluations.
- Threat Intelligence: Tracking of high-profile cyber events and affected vendors via Black Kite FocusTags™.
- Ransomware Susceptibility: Assessment of ransomware attack likelihood with the Ransomware Susceptibility Index®.
- Supply Chain Visibility: Identification of Nth-party risk through a first-of-its-kind monitoring module.
- Vendor Engagement: Centralized, trackable, and scalable process for working with vendors to reduce risk via Black Kite Bridge™
- Cyber Risk Report for Executives: Easy-to-understand report with letter grade scores and financial impact.
- Technical Drill-Down for IT: Detailed technical information behind each risk category.
- Risk/Vulnerability Prioritization: Prioritization by severity for quick identification and mitigation.
- Industry Benchmarks and Comparisons: Identification of trends and areas for improvement.



Boundaries of the System

Infrastructure

The TRIS runs on Google Cloud (GC).

Employees access the application either through their desktop on company-supplied computers or through an internet protocol security (IPSec) tunnel. Data communications between employee systems and production are encrypted with OpenVPN (VPN) technology using advanced encryption standard (AES) 256-bit encryption to protect data and intra-company communications.

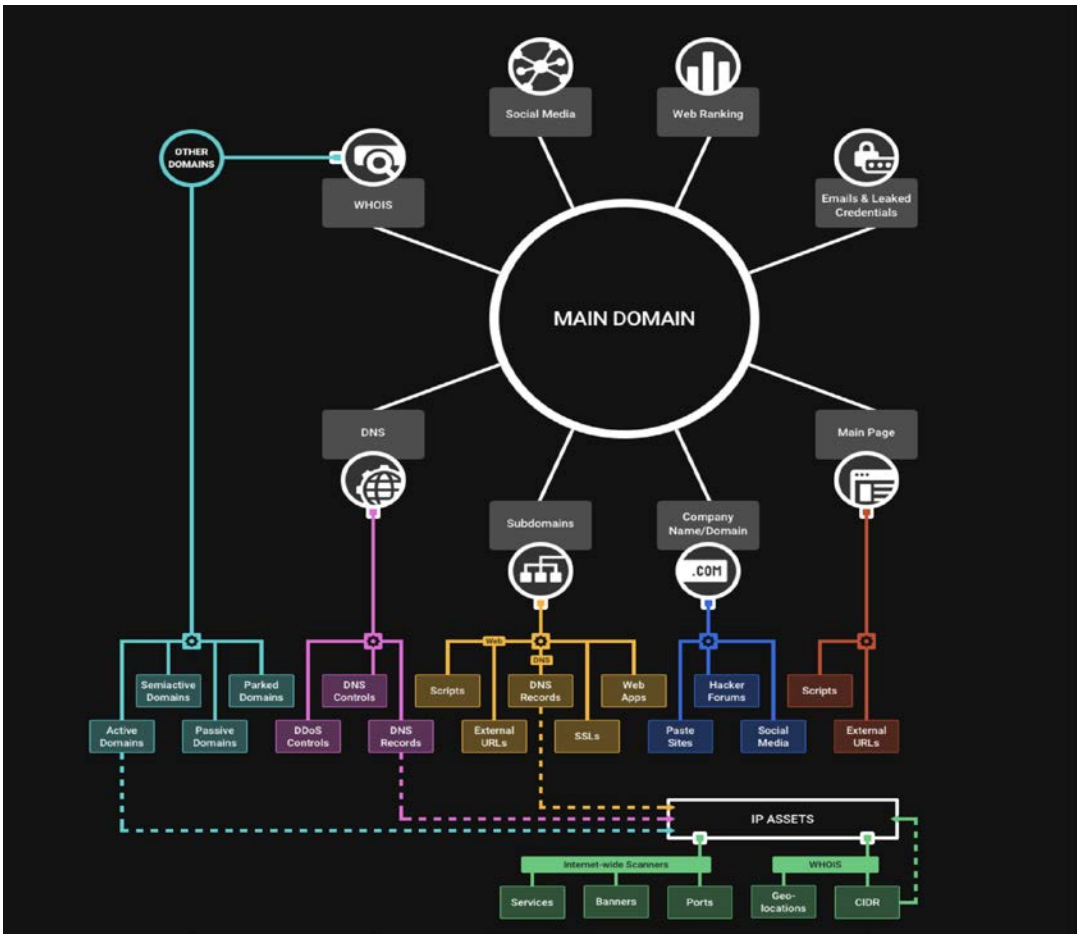
The TRIS uses Microsoft SQL relational database management system. These database servers and file servers are housed in Black Kite's secured network operations centers (NOCs) on GC.

Software

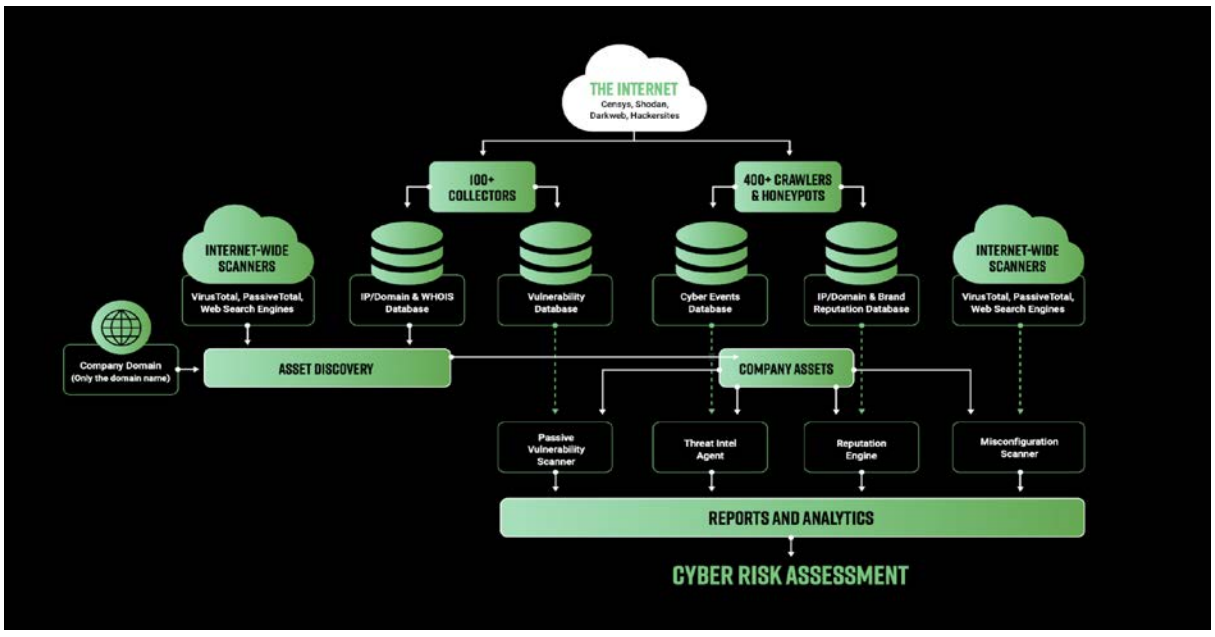
The TRIS is a software-as-a-service (SaaS) application developed and maintained by Black Kite's in-house software engineering group. The software engineering group enhances and maintains the TRIS to provide service to calculate the risk level of vendors by using the Open FAIR™ model to define risk management as the combination of cyber risk scorecard, policies, procedures, and financial numbers that enable an organization to cost-effectively achieve and maintain an acceptable level of loss exposure. Our vision is to complete the risk picture of a vendor by providing Black Kite's Cyber Risk Assessment (technical implementations), Universal Questionnaire and Policy Processor (UniQuE), Open FAIR™ Model (the risk in financial numbers), the Black Kite Bridge™ (for vendor collaboration), the Black Kite Assessments Module (for automated vendor assessments) and Nth-party insights via our Supply Chain Module. Black Kite's software is not sold on the open market. Black Kite provides a service that scans business' public access methods for possible security risks, such as known but unpatched vulnerabilities, or open network ports. Black Kite also monitors social media, dark-web forums, and other sources of information leaks, searching for company information such as compromised passwords, email addresses, or network structure details. Other potent attack methods such as fake/fraudulent websites or programs and/or services masquerading as legitimate sites, or a business' products are also hunted down.

Black Kite uses open-source intelligence (OSINT) techniques to gather information. Both hackers and legitimate security companies continually scan social media websites and networks for information on vulnerabilities and publish their findings on the internet. The map below shows how hackers can leverage their attack vectors by using OSINT resources, namely hacker forums, social networks, Google, leaked database dumps, paste sites, and even legitimate security services like VirusTotal, Censys, Cymon, Shodan, and Google Safe Browsing. Black Kite's cyber risk assessment gathers data from all these sources and performs contextualization and analysis to convert data into risk intelligence presented in a comprehensive ratings format.

To generate the assessment, Black Kite only requires a company's domain name. Black Kite's asset-discovery engine collects the related information from VirusTotal, PassiveTotal, web search engines, and other internet-wide scanners. Black Kite has one of the largest IP and Whois domain databases holding more than one billion historical items. The asset-discovery engine searches the database to find all company-related IP address ranges and domain names.



The results generated by the asset-discovery engine are used as the input for passive vulnerability and configuration scanners, threat intelligence agent and reputation engine.



Black Kite has more than 100 data collectors, 400 crawlers, and tens of honeypots. The crawlers and collectors continuously collect IP, domain reputation feeds, cyber events, hacker shares, social media shares, and known vulnerabilities. They also collect internet-wide scanner (Censys, Shodan) databases and put the results into the corresponding data stores. The reports and analytics agent then analyzes the findings and generates the categorized and letter-graded assessment.

This data is analyzed and compiled by Black Kite into a simple, readable report with letter-grade ratings to help identify and mitigate potential security risks and to present technical data as readily understandable business concepts. Black Kite does all of this information gathering and analysis in a non-intrusive way, i.e., without scanning or modifying any business assets.

The System utilizes the following third-party software applications for major business functions:

Software	
Production Application	**Business Function**
Gainsight	Customer success platform/customer relationship management (CRM)
Azure DevOps	Continuous integration
Splunk Enterprise Security	Log and system monitoring
Wazuh	Intrusion detection system (IDS)
Zendesk	Help desk and ticketing system
GC	Cloud hosting platform, key management
SentinelOne	Endpoint protection
Jira	Code and vulnerability ticketing system
Visual Studio	Development environment
Cloudflare	DDoS protection, web application firewall (WAF), domain name system (DNS), and certificate management
Pendo	Platform usage heatmapping and user interface improvements
Google Gemini Flash	AI model used to power the current UniQuE Parser

Data

Data, as defined by Black Kite, constitutes the following:

- Cyber threat intelligence data
- Customer data, including uploaded compliance/assessment artifacts
- Output reports
- System files
- Error logs

Black Kite uses OSINT techniques to gather data, perform contextualization and analysis to convert data to risk intelligence in the form of a risk assessment. Black Kite's assessment is an objective, external measure of an organization's cyber risk posture. The risk ratings provide easy to understand cyber risk information for executives while providing detailed technical data and mitigation strategies to frontline engineers.

The passive Black Kite assessment evaluates a company in twenty security-related categories and one informational category. Each category provides specific information about an aspect of a firm's cyber security posture.

Black Kite also correlates cyber risk findings to industry standards and best practices. The classification makes it possible to measure the compliance level of any company for different regulations and standards, including NIST 800-53, ISO 27001, PCI DSS, HIPAA, GDPR, Shared Assessments, and others. The Platform estimates the external compliance of target companies. The cross-correlation capability measures the compliance level of a target company based on the standard input.

Processes and Procedures

Management has developed and communicated to employees and customers procedures to restrict logical access to the TRIS. Changes to these procedures are performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Data classification (data at rest, in motion, and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess 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 backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (such as firewalls)
- AI usage and risk monitoring

Change Management

Black Kite has a formalized change management process in place, which requires identification and recording of significant changes, assessment of risk and potential effect of such changes, approval of proposed changes, and testing of changes to verify operational functionality. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed. The IT and Engineering team meets weekly to review and schedule changes to the IT environment.

Emergency changes follow the formalized change management process, but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented.

Changes to infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments.

Black Kite has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.

Black Kite uses a standardized server build checklist to help secure its servers, and it conducts monthly vulnerability assessments to identify potential system vulnerabilities. Patches are applied regularly in accordance with Black Kite's patch management process.

Security Management

Black Kite has a dedicated Information Security team consisting of a security officer, security specialists, and incident response specialists responsible for management of information security throughout the Company. They maintain security credentials and are required to annually sign and acknowledge their review of the information security policies. They are responsible for developing, maintaining, and enforcing Black Kite's information security policies. The information security policies are reviewed annually by the Information Security team under the direction of the Chief Security Officer and are approved by executive management.

As the Information Security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly IT maintenance meetings or through system alerts.

During annual security training and awareness programs, management ensures communication of the latest information security policies as well as written job descriptions for security management.

Additionally, management is responsible for ensuring business associate agreements are current for third parties and for updating the annual IT risk assessment.

System Monitoring

The Information Security team uses a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection tools, vulnerability assessment reports, and operating system event logs. These alerts and notifications are reviewed daily by the Information Security team using a security incident and event monitoring (SIEM) product. Additionally, the Information Security team has developed and will review the following SIEM reports:

- Failed object level access
- Devices not reporting in the past 24 hours
- Failed login detail
- Firewall configuration changes
- Security events requiring further investigation are tracked using a Slack incident ticket and monitored until resolved

Incident Management

The Company's Incident Response Policy is initiated when a security event is detected and reported. Appropriate personnel are informed of the event regardless of whether reported by an internal or external source, with alerts prioritized based on severity.

Roles for incident response and handling are defined and assigned, and a multi-stage process is followed until the risk has been mitigated and the outcome(s) is documented. The cause is assessed, and the lessons learned are documented, as necessary.

The Company notifies affected parties, including individual data subjects in the instance personal information is compromised, and legal and regulatory authorities, as necessary.

Data Backup and Recovery

Black Kite uses data replication to back up its data files and software. Full system backups are conducted daily and tested monthly. Access to backup devices, scheduling utilities, systems, and media is restricted to authorized personnel.

System Account Management

Black Kite has implemented role-based security to limit and control access within the TRIS. Employees are granted access to in-scope systems based on documented approvals by appropriate management personnel. The ability to create or modify user access accounts and user access privileges is limited to authorized personnel. User access is reviewed quarterly to verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts.

The human resources department notifies the Information Security team concerning employee termination prior to the time of termination. All standard accounts and permissions to which Black Kite employees would typically have access are terminated within 24 hours. After the offboarding process is documented for reference purposes, and notes are taken as to which tools or systems:

- The employee had access to it, but access was revoked.
- The employee never had access to and so were out of scope.
- Any additional systems that the specific employee had access to where access was revoked.

These reports are then checked against Vanta and other access management documents to verify that all ex-employee access to company resources has been revoked. If there are any additional systems that the employee may have access to, this access is then removed and documented.

Administrative access to Google Workspace, TRIS servers and databases is restricted to authorized employees.

Unique user identification numbers, names, and passwords are required to authenticate all users to the TRIS. Password parameters consist of the following:

- Passwords contain a minimum of ten characters, including one non-alphanumeric character and one special character.
- Passwords expire every 90 days.
- Company policy dictates the use of a password manager. This control is tracked for compliance in Vanta.

Vendor Management

To initiate a vendor relationship, management negotiates and manages the vendor contract clauses and additional data protection agreements with vendors who process or store the Company's data, customer data, or employee data, as well as systems that connect to the Company's systems. The Information Security team manages the vendor security risk assessment process and documents this process via a ticketing system. Black Kite maintains operational processes to assess security risk considerations related to vendors. These vendors are required to undergo an initial security risk assessment prior to contracting with the Company. Those vendors who do not meet Black Kite's baseline security requirements are not moved forward for procurement. The Information Security team reviews vendor security risk assessments annually, or upon expansion or changes to the contracted service offering. Vendors deemed high risk, such as data center providers or other vendors storing or processing data in scope for Black Kite's regulatory or contractual requirements, undergo reassessment annually.

Internal Audit

Black Kite follows the three lines of defense model established by the Institute of Internal Auditors, discussed in "The Three Lines of Defense in Effective Risk Management and Control" whitepaper. Per this model, management is the first layer of defense, various risk control, and compliance oversight functions established by management are second, and independent assurance as needed is the third.

Given the size of Black Kite and personnel resources, the Company contracts with Vanta, an independent third-party service provider, to provide internal audit services. While the Information Security team is responsible for identifying risks and implementing appropriate controls to mitigate those risks when necessary, Vanta monitors the operating effectiveness of implemented controls relevant to human resources, risk assessment, monitoring, logical access, system operations, and change management on a continuous basis. Vanta reports on the operating effectiveness of controls in real-time and sends alerts to management when exceptions are discovered. Management is responsible for responding appropriately to any discovered exception or deficiency.

Additionally, Black Kite works with a third-party assessor and undergoes an independent compliance examination (e.g. SOC 2®) on at least an annual basis.

Monitoring

The systems within the boundary are configured to prevent and detect vulnerabilities. In addition to daily oversight and monthly reviews of logs and other usage of virtual infrastructure, management provides monitoring and audit logging in the form of preventive, detective, and corrective reporting. Relevant output from monitoring and detection mechanisms are distributed at monthly meetings with executive and management personnel. Security testing, both automated and manual, occurs at regular intervals. Black Kite performs external network scanning and authenticated web application scanning monthly. Additionally, the Company has deployed anti-malware technology for environments commonly susceptible to malicious attack and has configured it to be updated routinely, logged, and installed on all relevant production servers.

Black Kite utilizes a distributed approach to scale the security monitoring function by using a combination of commercially available tools, custom code, and an instant messaging platform. Black Kite has created a system that provides for the determination of attributions for most critical security relevant events and target notifications to the staff with the authority and the context necessary to vet that security alert. The interface of this system allows the targeted staff member to either resolve the security alert if they can do so safely or to escalate to the Information Security team if response is required.

The monitoring toolset includes the following GC services:

- **Cloud IAM** - Identity and Access Management (IAM) service for defining policies based on role-based access control.
- **Cloud Key Management Service** - Cloud-hosted key management service (KMS) integrated with IAM and audit logging.
- **Cloud Resource Manager** - Service to manage resources by project, folder, and organization based on the hierarchy.
- **Cloud Security Command Center** - Security and data risk platform for data and services running in GC.
- **Cloud Security Scanner** - Automated vulnerability scanning service for applications deployed in App Engine.
- **Access Transparency** - Near real-time audit logs providing visibility to GC administrators.
- **VPC Service Controls** - Service to manage security perimeters for sensitive data in GC services.

Availability

Black Kite considers the likely causes of data loss, the commitments and requirements related to availability, the timeliness of back-up procedures, the reliability of the back-up process, and the ability to restore backed-up data. In evaluating the design of data availability controls, Black Kite considers that most data loss does not result from disasters but from routine processing errors and failures of system elements. Black Kite maintains robust system capacity and infrastructure monitoring for performance and availability. Backups are performed in near-real-time and are largely a continuous process. Business contingency and disaster recovery planning at Black Kite takes into consideration a business impact analysis, incident handling, contingency, and business continuity plans, which collectively make up the framework for maintaining a continuity and contingency strategy, management, and operational plans. The Company has designed policies and procedures that cover a partial or complete failure of cloud service providers (CSPs).

Confidentiality

The confidentiality category refers to the protection of customer information as committed by the Company's service level agreements (SLAs). The confidentiality of the System is dependent on many aspects of the Company's operations. The risks that would prevent the Company from meeting its confidentiality commitments and requirements are diverse. The Company has designed its controls to address both internal and external confidentiality risks specifically related to protection from improper use and disclosure (including the monitoring of vendor services), as well as the proper retention and disposal of confidential customer information. Confidentiality risks are addressed through controls over the use, retention, and disposal of confidential data, data classification policies and procedures, confidentiality and information sharing agreements, remote access and transmission restrictions, and vendor risk assessments. By design, Black Kite limits the data we collect from customers to the minimum amount strictly necessary to provide services. Confidential customer data is not used in testing environments, and any data collected or processed is appropriately masked. In evaluating the suitability of the design of confidentiality controls, the Company considers the likely causes of improper disclosure or handling of confidential information, and the commitments and requirements related to confidentiality.

Complementary User Entity Controls (CUECs)

Black Kite's controls related to the System cover only a portion of overall internal control for each user entity. It is not feasible for the criteria related to the System to be achieved solely by Black Kite. Therefore, each user entity's internal controls should be evaluated in conjunction with Black Kite's controls described in Section IV of this report, considering the related CUECs identified for the specific criterion. For user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The user entity controls presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities are responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1	User entities are responsible for the security and integrity of data housed under user entity control, particularly the data utilized by Black Kite systems and services.
CC6.2	Determination of personnel who need specific functionality and the granting of such functionality is the responsibility of authorized personnel at the user entity. This includes allowing access to Black Kite's application keys and API keys for access to the web service API.
CC6.3	Authorized users and their associated access are reviewed periodically.
CC6.6	User entities will ensure protective measures are in place for their data as it traverses from user entity to Black Kite.
CC6.6	User entities should establish adequate physical security and environmental controls of all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity in order to provide authorized information to Black Kite.
C1.1	User entities assign responsibility to personnel, and those personnel identify which data used by Black Kite is to be considered "sensitive."

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

Black Kite utilizes GC as a subservice organization for cloud hosting services. GC is responsible for operating, managing, and controlling the components from the host operating system and storage, down to physical security and environmental controls over the facilities in which the services operate. GC is examined annually in accordance with the *AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2®)*. This description and Section IV of this report include only the controls of the System and do not include any of the controls expected to be implemented at GC.

Although the subservice organization has been carved out for the purposes of this report, certain Trust Services Criteria are intended to be met by controls at the subservice organization. Management of Black Kite receives and reviews the most recent SOC 2® reports available from GC at least annually. In addition, through its operational activities, Black Kite's management monitors the services performed by the subservice organization to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also has communication with the subservice organization to monitor compliance with service commitments, stay abreast of changes planned at the hosting facilities, and relay any issues or concerns to their management.

It is not feasible for the criteria related to the System to be achieved solely by Black Kite. Therefore, each user entity's internal control must be evaluated in conjunction with Black Kite's controls and related tests and results described in Section IV of this report, considering the related CSOCs expected to be implemented at the subservice organization as described below.

Criteria	Complementary Subservice Organization Controls
CC2.3 CC7.3 CC7.4 CC7.5	GC is responsible for notifying affected parties of security updates and/or identified security incidents.
CC6.4	GC is responsible for restricting data center access to authorized personnel.
CC6.4	GC is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5 C1.2	GC is responsible for the physical assets located within the data centers, including the secure decommissioning and physical destruction of production media prior to leaving secure zones.
CC7.1	GC is responsible for implementing a vulnerability management process that includes remediation of vulnerabilities in software, systems, and network devices.
CC7.2 A1.2	GC is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2 A1.2	GC is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2 A1.2	GC is responsible for overseeing the regular maintenance of environmental protections at data centers.
A1.1	GC is responsible for monitoring and managing of their data centers' capacity and availability.
A1.2	GC is responsible for identifying and notifying operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
A1.3	GC is responsible for testing their Business Continuity/Disaster Recovery Plan periodically.
C1.2	GC is responsible for providing customers with the ability to delete their content. Once successfully removed the data is rendered unreadable.

ATTACHMENT B:

BLACK KITE'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Principal Service Commitments and System Requirements

Black Kite designs its processes and procedures related to TRIS to meet its objectives for its services. Those objectives are based on the service commitments that Black Kite makes to user entities and regulations that govern the provision of TRIS services, and the financial, operational, and compliance requirements that Black Kite has established for the services. The TRIS services by Black Kite are subject to the security and privacy requirements of any relevant regulations, as well as state privacy and security regulations in the jurisdictions in which Black Kite operates.

Black Kite establishes operational requirements that support the achievement of security, availability, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Black Kite's system policies and procedures, system design documentation, and contracts with customers. Information security policies define the Company's 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.

Trust Services Criteria	Service Commitments	System Requirements
Security	• Black Kite will employ administrative and technical measures in accordance with applicable industry practices to protect the System and prevent the accidental loss or unauthorized access, use, alteration, or disclosure of customer data under its control during each order term. • All data transmitted between the Company and the users of the System is protected using transport layer security (TLS) and HTTP strict transport security (HSTS). • Access to environments that contain customer data requires a series of authentication and authorization controls, including multi-factor authentication (MFA). • The Company monitors critical infrastructure for security-related events by using a custom implementation of open source and commercial technologies.	• Employee provisioning and deprovisioning standards • Logical access controls such as user IDs and passwords to access the System • Encryption of data in transit over public networks • Security monitoring controls
Availability	• The Company will use commercially reasonable efforts to make the System available for access and use by end users over the internet at least 99.8% of the time as measured over the course of each calendar month, excluding unavailability as a result of scheduled maintenance.	• System performance monitoring • Load balancing • Business continuity and disaster recovery planning • Multi-availability zone configuration
Confidentiality	• The Company will protect confidential information against any unauthorized use or disclosure to the same extent that the Company protects its own confidential information, but in no event will the Company use less than a reasonable standard of care to protect such confidential information. • The Company will use confidential information solely for the purpose for which it was disclosed.	• Encryption of data at rest • Data classification • Data management procedures