KEYFACTOR

REPORT ON KEYFACTOR, INC.'S DESCRIPTION OF ITS PUBLIC KEY INFRASTRUCTURE MANAGED SERVICE SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS RELEVANT TO SECURITY THROUGHOUT THE PERIOD NOVEMBER 1, 2018 TO OCTOBER 31, 2019

SKODA MINOTTI
CPAs, BUSINESS & FINANCIAL ADVISORS

Delivering on the Promise.

Acronym Table

➢ ADS	Architecture and Design Session
➢ CA	Certificate Authority
➢ CBRE	CBRE Group, Inc.
➢ CRL	Certificate Revocation List
➢ FIPS	Federal Information Processing Standards
➢ GSA	Government Services Administration
➢ GUI	Graphical User Interface
➢ HSM	Hardware Security Module
➢ IDS	Intrusion Detection System
➢ IT	Information Technology
➢ Keyfactor	Keyfactor, Inc.
➢ NAT	Network Address Translation
➢ OH	Ohio
➢ PKI	Public Key Infrastructure
➢ PKIaaS	Public Key Infrastructure as a Service
➢ RACI	Responsible, Accountable, Consulted, and Informed
➢ SCEP	Simple Certificate Enrollment Protocol
➢ TSP	Trust Service Principles
➢ VCS	Version Control System
➢ VPN	Virtual Private Network

Assertion of Keyfactor Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Keyfactor's Public Key Infrastructure Managed Service System (system) throughout the period November 1, 2018 to October 31, 2019, to provide reasonable assurance that Keyfactor's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in section 3 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 November 1, 2018 to October 31, 2019, to provide reasonable assurance that Keyfactor's service commitments and system requirements were achieved based on the trust services criteria relevant to security (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*). Keyfactor'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 3.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their 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 1, 2018 to October 31, 2019, to provide reasonable assurance that Keyfactor's service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/ Andrew Prayner, Director of Information Security & Compliance
Keyfactor, Inc.
November 22, 2019

SKODA MINOTTI & CO.
CERTIFIED PUBLIC ACCOUNTANTS

Delivering on the Promise.

Independent Service Auditors' Report

To: Keyfactor:

We have examined Keyfactor Corporation's (Keyfactor's) accompanying assertion titled "Assertion of Keyfactor Management" (assertion) that the controls within Keyfactor's Public Key Infrastructure Managed Service System (system) were effective throughout the period November 1, 2018 to October 31, 2019, to provide reasonable assurance that Keyfactor'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*).

Service Organization's Responsibilities

Keyfactor 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 Keyfactor's service commitments and system requirements were achieved. Keyfactor has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Keyfactor 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 Keyfactor'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 Keyfactor'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

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

There are inherent limitations in 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 or 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 Keyfactor's Public Key Infrastructure Managed Service System were effective throughout the period November 1, 2018 to October 31, 2019, to provide reasonable assurance that Keyfactor's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

SKODA MINOTTI & CO.

Skoda Minotti

November 22, 2019

Cleveland, Ohio

Company Overview and Services Provided

Keyfactor is a C Corporation under United States federal income tax law, incorporated in the state of Delaware, with its principal place of business at 6050 Oak Tree Blvd., Suite 450, Independence, OH 44131. Keyfactor was originally Certified Security Solutions, Inc. which was founded in 2000. Certified Security Solutions, Inc. was rebranded as Keyfactor, effective November 1, 2018 with articles of incorporation amended February 1, 2019.

Keyfactor is committed to simplifying the proper application of digital security to protect its clients' identities, data, and business processes. Keyfactor's solutions simplify the design, deployment, monitoring, and management of trusted digital identities making them scalable, flexible, and affordable for the most demanding of enterprises. Keyfactor software and solutions enable digital authentication, encryption and signing technologies that safeguard access to identities, data, devices and applications. By protecting clients' most valuable resources, Keyfactor helps companies minimize risk, protect assets, and reduce operational expense by safeguarding access to information.

Products

- Managed Services: Management services by Keyfactor of user's trusted PKI environment; provisioning of customer-specific cloud-based PKI solutions.
- Software: Assists clients in efficiently manage millions of certificates to help ensure the client's systems are protected and accessible 24/7.
- Professional Services: Helps clients established their own scalable PKI to issue their own trusted digital certificates for a host of use cases.

System Description

Keyfactor PKI Managed Service is a comprehensive offering providing a highly available PKI and certificate management solution for our customers either on their premises or in the Keyfactor-managed cloud computing platform. The solutions provide customers with a robust and secure certificate infrastructure.

The PKI managed service is a combination of hardware, software, services and operations, giving customers the ability to issue certificates from a privately rooted CA hierarchy without possessing in-house, requiring the dedicated staff and specific skill sets required to run such an infrastructure.

The service is made up of various components. Collectively, they define the system. They are categorized as follows:

Initial PKI Design

- Design of an enterprise PKI architecture specific to meet the customer use case requirements.

Installation of PKI Core and Ancillary Services

- Installation and configuration of a hosted root CA.
- Installation and configuration of issuing CAs.
- Installation and configuration of PKI ancillary services.

PKI Managed Services

- Hosted root CA operational services.
- Issuing certificate authority operational services.
- PKIaaS.

Escrow Services

- Escrow of the root CA key material.

PKI Support Services

- PKI support and planning credits.
- Fault handling support.

The following sections provide additional detail for each component of the PKI managed service.

Initial PKI Design

The PKI design takes input from the customer, provides information to the customer regarding critical design elements and yields a set of documents. These documents are:

- Architecture and Design Document – The design elements for the customers' implementation of the Managed Service PKI. This document is the basis for installation and configuration and provides a baseline for future support.
- Key Signing Ceremony – Key signing document that provides step-by-step instruction on the root CA build process.
- Certificate Policy Document – document which aims to define the different actors of a PKI and their roles and their duties.
- Certificate Practice Statement – document from a CA which describes their practice for issuing and managing public key certificates.

The initial PKI design phase typically begins with an ADS. The ADS requires approximately two to three days, and covers the critical design criteria for the PKI, ensuring the customer's use cases and security requirements are addressed.

Installation of services begins after design finalization and customer sign-off.

Installation and configuration of the Hosted Root CA

The root CA is built by following the key signing ceremony document. The root is built with a minimum of two people present and can optionally be witnessed by the customer. Each step in the process is reviewed and initialed by the installer upon completion, and a 2nd party then reviews the steps and bears witness to each section of the key signing ceremony document and notes any deviation from the script.

Installation and configuration of the issuing CAs

The installation of the issuing CAs for both the fully-hosted and customer premise solutions are performed using a combination of operating system tools and programmatic scripts.

Installation and configuration of the PKI Ancillary Services

Installation of the PKI ancillary services is performed in accordance with documented design decisions. The Ancillary PKI services include:

- Keyfactor Command Reporting: software used for certificate management and status reporting for the managed service
- NDES: enrollment service providing a SCEP interface to an issuing certificate authority
- Keyfactor Command Issuing (if applicable): software used to aid the secure issuance of certificates to mobile devices
- CRL Hosting: redundant web based CRL hosting
- Certificate Templates: Configuration and deployment of a specified number of certificate templates based on the customer's business requirements

Upon completion of the above, the PKI managed service is transitioned to a steady state of operational service.

PKI Managed Services

As a managed PKI transitions from design and installation to operational steady state, a series of internal meetings are conducted to transition and confirm information regarding the design and configuration. This information is captured by the operations team and documented in the customer's run book.

Once the operations team confirms the configuration parameters, it installs the required monitoring software on the issuing CAs.

Ongoing operations then become the day to day focus for the PKI Managed Service. Tasks include:

Hosted Root CA Operational Services

- Administering multi-part control over the root key material (k of n)
- Secure facility storage and sign in / sign out
- Administration of HSM protection of the root CA's private keys
- CRL publishing
- Subordinate CA (SubCA) certificate revocation / issuance
- Root CA operating system management
- Maintenance of third party escrow of root CA materials
- Testing of disaster recovery and business continuity capabilities

Issuing Certificate Authority Operational Services

- Monitoring and maintenance of service health of issuing CA PKI services
- Changing CRL parameters
- CA service starting and stopping
- Configuration of CA extensions
- Maintenance of certificate managers
- Maintenance of certificate manager restrictions
- Maintenance of enrollment agent restrictions
- Definition of other authorized CA administrators
- Configuration of audit parameters

Escrow Services

As a standard, customers' root CA key material is deposited into an escrow account. Use of this service requires acceptance of Keyfactor's agreement with National Software Escrow Inc., and the subsequent registration of the customer as a beneficiary under Keyfactor's escrow agreement. If authorized, the following material is deposited:

- HSM security world software
- Root CA database
- Root CA registry settings
- Root CA certificates
- Required authentication quorum

The customer receives the passphrases to the card set so as to avoid storage of the passphrases with the cryptographic materials.

PKI Support Services

PKI support services are provided through two different vehicles: PKI planning credits and fault handling.

Fault Handling

Fault Handling is the reporting, management and resolutions of errors and outages of the PKI managed service. Each reported fault receives a case number and is assigned to Keyfactor's support team to work towards resolution with a customer. Faults are also assigned a severity level as outlined in each customer's contract with Keyfactor.

Principal Service Commitments and System Requirements

Keyfactor designs its processes and procedures related to its Managed PKI Service System to meet its objectives. Those objectives are based on the service commitments that Keyfactor makes to user entities, the laws and regulations that govern SaaS providers, and the financial, operational, and compliance requirements that Keyfactor has established for the services.

Security commitments to user entities are documented in customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Public Key Infrastructure Managed Service System that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect customer data at rest and in transit.

Keyfactor establishes operational requirements that support the achievement of security relevant laws and regulations, and other system requirements. Such requirements are communicated in Keyfactor'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 Managed PKI Service System.

Infrastructure

Infrastructure supporting Keyfactor Managed PKI Service System resides in a third party datacenter, SecureData 365, a secure hosting facility in Cleveland, OH. Keyfactor maintains five assets within the datacenter. A computer equipment rack housing Keyfactor corporate IT services (retired effective August 26, 2019 due to corporate IT infrastructure migration), and four GSA Class 5 combination vaults for housing PKI Managed Service offline data. The GSA Class 5 combination safes are isolated from the datacenter floor by a dedicated key-locked cage. The cage is monitored by a dedicated motion activated video camera with 90-day video retention. Datacenter personnel do not possess keys to the dedicated cage housing the combination safe and do not possess the safe combination. Keys for the computer equipment rack are maintained by datacenter personnel in a secure container at the datacenter and all equipment rack access events are logged.

The secure cage and vault configuration (a single GSA Class 5 vault) is also in place at SecureData 365's North Canton, OH location to support Keyfactor's Managed Service Disaster Recovery and Business Continuity capabilities.

Software

The following provides a summary of software products used to deliver the PKI Service System:

- Microsoft DevOps is used as the VCS in application development.
- Microsoft SQL Server is used as the database server to store customer and application data.
- Microsoft Office Suite products are used for the general office productivity suite.
- Microsoft Azure Windows Server is used as the underlying operating system for the internal operating system and supporting services.
- Azure Recovery Services Vaults are used for backup storage and recovery.
- Box is used for the secure file transfer site with customers.
- Salesforce Service Cloud is used for IT operations and Support case management and customer incident ticketing and tracking.
- SharePoint is used for the Company's intranet and internal document sharing.
- pfSense is used for firewall and NAT.
- SonicWall is used for IDS/IPS.
- Bitlocker is used for the encryption of employee workstations.
- Webroot is utilized for antivirus and Sentinel One is utilized for anti-malware software.
- Splunk Cloud is used for operational logging, monitoring, and alerting for managed service systems
- WSUS is used as the operating system patch management system.
- PasswordManager-Pro is used as the password vault application.

People

People involved in the operation and use of the system are:

- Executive Management is responsible for leading the organization, managing sales activities, and managing the day-to-day operations of Keyfactor.
- Finance is responsible for managing overall financials of the organization and certain contractual obligations to clients and vendors.
- Sales and Marketing is responsible for generating new clients and additional sales from existing clients.
- Platform Enablement is responsible for the overall management of day-today activities that directly support customer services.

Procedures

Backup and Recovery

Keyfactor's backup location for PKI Managed Service system information is a dedicated GSA Class 5 security vault within SecureData 365's North Canton, OH location. Access is restricted to Keyfactor named personnel with a signature on file at SecureData 365. Security vault keys are stored by Keyfactor in a GSA Class 5 combination safe in a restricted area of the Keyfactor corporate office.

Keyfactor's location for corporate IT backup media is a GSA Class 5combination safe located in a restricted area of the Keyfactor corporate office.

Escrow materials are held in a vault managed by Keyfactor's escrow agent, National Software Escrow, Inc.

Authentication and Authorization

Logical access software is used to identify and authenticate authorized users to Keyfactor's corporate network and to restrict authorized user access to system areas as determined by Keyfactor management. A unique user ID and password is required for all corporate network access by Keyfactor personnel. Keyfactor enforces password complexity and age policies. As specified by policy, certain storage areas of the Keyfactor network are restricted to a subset of employees as determined and authorized by management. Vendors requiring the use of Keyfactor computer assets are restricted by network control policy from accessing Keyfactor's internal corporate network, and are temporarily granted access only to systems required for the performance of their work.

System administrators do not use their regular user accounts for administrative functions; administrators have dedicated and unique administrator accounts which are not shared. Privileged account information that is not unique to individuals is stored in an encrypted data file that can be accessed and decrypted only by authorized individuals.

Specifically for the PKI Managed Service system, additional identification, authorization, and restriction controls are in place. Only PKI Managed Service authorized personnel are allowed to access customer specific architecture and support documentation. Physical access to offline system data requires physical control materials granted only after an approved request through Keyfactor's ticketing system. Offline system data can only be started with a smart card and passphrase quorum unique to each customer. Passphrase information is encrypted and accessible only to PKI Managed Service authorized personnel.

Operational activities for the PKI Managed Service system may require that Keyfactor personnel access systems on customer networks. Access to customer networks is accomplished through a customer VPN where required. User credentials are assigned to authorized Keyfactor personnel and stored in a manner that complies with customer security policies.

User Provisioning

User account provisioning requests are authorized by Keyfactor Management prior to being issued network credentials. User provisioning requests are logged in Keyfactor's case management system and membership in default roles is provided at the time of provisioning. Membership in restricted roles for access to specific data to systems requires the approval of the owners of the respective systems and all role-modification requests initiate a review of current access to prevent inadvertent rights escalation over time.

Planned user de-provisioning actions occur as scheduled events. Emergency changes are performed immediately. All de-provisioning events are ticketed.

Specifically for the PKI Hybrid Managed Service system, system operators are authorized and provisioned by customer personnel. Access lists are reviewed with customer personnel on a periodic basis and changes in staffing models are communicated to customer personnel when required.

Physical Security – Data Center

Keyfactor maintains policies and standards for physical security to help protect production and corporate servers, network devices, and network connections within Keyfactor third party data centers and approved access lists are maintained at these facilities. All data centers that house Keyfactor systems are reviewed annually for ongoing security compliance.

Physical Security – Keyfactor Corporate Office

Keyfactor's corporate office suite is located in Park Center Plaza, a Class-A business park property owned by CBRE. External doors to Park Center Plaza III, which houses Keyfactor's corporate office suite, automatically lock at 7:00 PM and unlock at 7:00 AM weekdays. Weekend and holiday access is restricted. Common areas of the property are patrolled by security officers during non-business hours.

Access to Keyfactor's corporate office suite is controlled by electronic door locks. Suite doors are locked at all times, and employees must badge in using their issued corporate badge. All badge unlock events are automatically logged.

Access to critical facility areas within Keyfactor's suite are further restricted to authorized personnel. All badge unlock events are automatically logged.

Visitors to Keyfactor's suite must ring for entry. Visitor entry and exit is logged at the reception desk, and visitors are not allowed to move about the corporate office unescorted. Visitors are issued a badge allowing suite entry and exit for the day if a badge is requested by the Keyfactor employee escort. Visitor badges are a distinctive color, cannot unlock suite doors outside of normal business hours, and are collected at visitor sign-out.

Video surveillance is in place for all entry points to the Keyfactor corporate office suite and for restricted facility areas.

Information Security Policy

Keyfactor's Information Security Policy codifies a management and reporting structure for information security management functions including policy definition, risk management, change control, and incident management. The organizational structure contains three bodies, each of which has a defined composition and charter: a Governing Body made up of a subset of the management team; an Information Security Management team headed by the Director of Information Security & Compliance; and an Information Technology Operations team.

Keyfactor's Information Security Governing Body is headed by Keyfactor's Director of Information Security & Compliance, who provides the authority on business requirements and acceptable risk and the Keyfactor Chief Financial Officer, who provides authority to allocate resources necessary to implement policy. The Governing Body contains other members of the management team to ensure sufficient representation of corporate knowledge. Responsibilities of the Governing Body include the approval of security policy, risk review and acceptance, and organization-wide communication.

Keyfactor's Information Security Management Team is responsible for authoring and review of security policy, identification and evaluation of risks and mitigating controls, implementation of change control procedures, audit policy definition, standards for incident response and data classification, and organizational wide communication and training.

Keyfactor's Information Technology Operations Team is a virtual team made up of Keyfactor personnel with a required technical competence and knowledge of Keyfactor infrastructure and the PKI Managed Service system. Responsibilities include the implementation of security policy, advising Information Security on risk management, systems monitoring and maintenance, and the implementation ofchange.

All teams are required to meet at regular intervals to fulfil their respectivecharters.

Incident Management

Keyfactor has implemented an incident reporting process whereby any incident or concern is reported to Information Security for analysis and ticketing; incidents may be reported by any employee, or IT Operations or result from a software alert. Incident management is built into their procedures and tracking platform.

Security and Malicious Software

Keyfactor's corporate network is protected by two firewalls, one at the datacenter ingress point, and one within Keyfactor's data cabinet. Both firewalls are configured with a default "deny all" rule, and opened ports and forwarding rules have a corresponding and reviewed business justification. Keyfactor has implemented additional network protection against floods and attacks at the data cabinet firewall, and will deny requests that exceed predefined limits or that match malicious patterns. Only authorized system administrators can change firewall rules, and all change requests follow normal change management procedures resulting in a ticket and review of the requested change.

Specifically for the PKI Managed Service system, access to customer networks is accomplished through customer supplied VPN infrastructure where required, in accordance with customer security policies. Offline root certification authority system data is never connected to a network.

Corporate workstations run antivirus software. Corporate servers run antivirus software when feasible. Antivirus signatures are updated daily.

Change Management

Change management controls provide a method to manage changes to corporate production and PKI Managed Service infrastructure in a rational and predictable manner, including planning, implementation, and post-change analysis. Change management processes are initiated when deficiencies in design, operational control effectiveness, or system functionality are identified, or when warranted by business requirements.

Keyfactor has implemented change management standard operating procedures that identify the prerequisites, responsibilities and authorization protocols, change windows, and procedures necessary to monitor and authorize change.

Identified changes are reviewed by IT Operations, including PKI Managed Service personnel, at which point the need, criticality, and associated risks and potential impact of implementing the change are evaluated. Changes to infrastructure may be pursued, or not, after this evaluation.

Change requests, and actions to implement change, are submitted to, and tracked in, a centralized ticketing system. If an incident requires an emergency change, then such a change may be performed to remedy the incident outside of normal change control windows, however, all such changes still require authorization and documentation using the service management system.

As part of Keyfactor's change management policy, infrastructure, software, and procedures are updated as necessary to remain consistent with system commitments and requirements. System patches are reviewed and implemented as approved by the change management team.

Hiring Practices and Staff Development

Keyfactor has formalized hiring practices designed to help ensure that new employees are qualified for their functional responsibility. Where local labor law or statutory regulations permit, Keyfactor may conduct criminal, credit, and/or security checks on all potential employees as well as verification of the individual's education, previous employment, and referrals. The specifics or extent of background checks performed depend on the position for which the individual is applying.

Upon acceptance of employment, all employees are required to execute a confidentiality agreement as well as acknowledge receipt and compliance with the Keyfactor Employee Handbook. The confidentiality and privacy of customer data is emphasized in the handbook and also during new employee orientation. Every employee has a written job description, and every job description includes the responsibility to communicate timely significant issues and exceptions to an appropriate higher level of authority within the Company.

Data

Login credentials are encrypted at rest (if stored) and while transmitted for authentication. Access to corporate resources by employees occurs over encrypted channels.

Communication with customers over public networks is encrypted on a case-by-case basis, following consultation with customer on the manner of encryption compatible with the customer's capabilities.

Keyfactor employee workstations are encrypted and required a pre-boot authorization PIN for startup.

Specifically for the PKI Managed Service system, additional controls on systems include the use FIPS 140- 2 level 3 hardware security modules for encryption on the offline root certification authorities and Gemalto's DPoD cloud-hosting key protection services is used on online issuing certification authorities. Production, backup and escrow material is encrypted and protected with a FIPS 140-2 level 3 HSM.

Subservice Organizations

The following are identified as subservice organizations used by Keyfactor in support of the PKI Managed Service system. The use of each organization has been evaluated by Information Security Management against Keyfactor's vendor policy. Where risks have been identified to the security of the system through the use of subservice organizations, Information Security Management has implemented policies or guidelines appropriately restricting the use of a subservices organization in order to mitigate identified risks.

The accompanying description includes only relevant policies, procedures, and trust service criteria and activities of Keyfactor and does not include policies, procedures, or trust services criteria and activities of the third-party service organizations described below. The examination of the Independent Service Auditors did not extend to policies, procedures, or trust services criteria and activities at the subservice organizations.

The following subservice organizations are used by Keyfactor for the following:

Service Provider	Nature of Services Provided
SecureData 365	Data center colocation
National Software Escrow	Escrow software as a service
Cornerstone IT	Managed IT services
Microsoft Azure	Cloud hosting services

Monitoring

Management monitors controls to consider whether they are operating as intended and to ensure that they are kept current to address any changes in technical, business or legal and regulatory conditions. Assessments of internal controls occur over time and result in corrective actions when required. In addition, controls are subject to separate evaluations should conditions warrant. This process is supported by the organizational structure of the company and the company's information security policy.

As part of their duties, Keyfactor Information Security Management is directed to monitor control quality and promote the adjustment of procedures based upon the results. Corrective action to address control assessments may be communicated and planned through team meetings and can involve customers as appropriate.

To support control monitoring, computer logging has been enabled for critical corporate production and PKI Managed Service systems. Within the logs, specific events have been identified as important monitors and indicators of risk to the confidentiality, integrity, and availability of the systems. A logging infrastructure is also in place for offline elements of the PKI Managed Service system. Log reviews are scheduled, per policy, to occur regularly as part of IT Operations and Information Security Management team meetings. Thresholds for escalation for logged events have been identified. Unusual, suspicious, or non-optimal functionality are escalated and processed as required.

Information and Communication

Communication policies and practices govern the manner by which Keyfactor employees share information internally and externally, communicate customer commitments and service information, and ensure that customers can provide critical data and information to Keyfactor.

To continue to offer services to its clients, Keyfactor leverages both formal and informal communication protocols and procedures.

- Immediate communication needs are handled through an open-door policy, which encourages and facilitates rapid communication of status, issues and updates.
- Task and planning meetings and progress updates are held during regular team meetings involving the appropriate individuals.
- The board of directors, executive management team, and department and team leads all participate in regularly scheduled meetings to ensure consistent communication.
- Quarterly "All Hands" conference calls are used to provide general strategy communications and to directly solicit employee feedback.

Policies are in place to govern required and essential communication.

Keyfactor policies, procedures, and customer specific information are stored in a centralized location for access by authorized personnel. Data owners are responsible for maintaining information content for their respective areas of ownership.

Keyfactor communicates with its various customers and other stakeholders through formal meetings, the delivery of scheduled status reports, and the use of service and project artifacts. Formal and informal meetings are scheduled as needed and attended by required Keyfactor personnel.

Information regarding the design and operation of the PKI Managed Service system and its boundaries is documented and communicated to authorized Keyfactor personnel and customers. As part of the standard customer on-boarding process, architecture, design, security, and operational documentation is produced and stored in customer-specific repositories accessible to authorized Keyfactor personnel. A subset of the documentation is provided to authorized customer personnel. A RACI chart documents which parties are Responsible, Accountable, Consulted, and Informed for key tasks during customer onboarding and while the system is operational. The RACI Chart is available internally to Keyfactor employees and is provided to customers upon becoming a PKI Managed Service customer.

Keyfactor and customer personnel are informed of their responsibilities for maintaining and operating the system. As part of the onboarding process, a system reference guide, communicating critical system parameters and security controls, is delivered to each customer. The customer specific reference guide is also available to authorized Keyfactor personnel for operational support.

Keyfactor personnel and customers of the system are provided with information on how to report security and operational incidents and concerns. Documentation provided to Customers includes both a telephone number and an e-mail address for PKI Managed Service support. Included in the documentation are instructions for reporting all manner of requests, incidents, and concerns, including those related to security. All customer support requests are logged and ticketed. For escalation, customers of the system also have clear communication paths to their respective account executive and the Vice President of Managed Services at Keyfactor.

System changes affecting Keyfactor and customer personnel responsibilities or Keyfactor commitments are communicated in a timely manner. Changes are documented and follow a documented change management process, including notification of, and approval by, affected parties.