armanino

System and Organization Controls (SOC) 3

Report on Controls Relevant to the Security, Availability, and Confidentiality Trust Services Categories

January 1, 2024 to March 31, 2024

REPORT PREPARED FOR

Lightbend

TABLE OF CONTENTS

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of

Lightbend, Inc.

San Francisco, California

Scope

We have examined Lightbend, Inc.'s ("Lightbend" or the "Company") accompanying assertion titled "Management's Assertion" (assertion) that the controls within Lightbend's Kalix and Akka platforms were effective throughout the period January 1, 2024 to March 31, 2024, to provide reasonable assurance that Lightbend'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 Implementation Guidance—2022)* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Lightbend 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 Lightbend's service commitments and system requirements were achieved. Lightbend has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Lightbend 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 Lightbend'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 Relativity's service commitments and system requirements based 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 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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions 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.

Service Auditor's Independence

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

Opinion

In our opinion, management's assertion that the controls within Lightbend's Kalix and Akka platforms were effective throughout the period January 1, 2024 to March 31, 2024, to provide reasonable assurance that Lightbend's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Armanino[LLP]

San Ramon, California

June 21, 2024

MANAGEMENT'S ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within Lightbend, Inc.'s ("Lightbend" or the "Company") Kalix and Akka platforms throughout the period January 1, 2024 to March 31, 2024, to provide reasonable assurance that Lightbend's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in the Description of the System 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 January 1, 2024 to March 31, 2024, to provide reasonable assurance that Lightbend'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 Implementation Guidance—2022)* (AICPA, *Trust Services Criteria*). Lightbend'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 the "Description of the System."

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 January 1, 2024 to March 31, 2024, to provide reasonable assurance that Lightbend's service commitments and system requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE LIGHTBEND KALIX AND AKKA SYSTEM

Overview of Operations

Company Overview

Founded in 2010, Lightbend, Inc. ("Lightbend" or the "Company") provides leading technology and support for building and optimizing applications that unleash the full power of the cloud and edge so organizations can implement any digital strategy, regardless of how ambitious, challenging, or innovative.

Services Provided

Lightbend offers two primary product lines and associated services:

- Akka, a toolkit for building highly concurrent, distributed, and resilient message-driven applications for Java and Scala. Akka provides the building blocks that make it easy for businesses to build, deploy, and run large-scale applications that support digitally transformative initiatives. Akka is delivered as a library (and set of supporting software and services) developers can integrate with their own systems.
- Kalix, a Platform as a Service ("PaaS"), built using Akka, abstracts away the complexity of the backend so our customers' teams can focus solely on building the business logic behind their apps, allowing any developer to code highly performant and scalable distributed systems to modernize and transform our customer's business. Kalix is available online, running on major cloud platforms.

In-scope Applications

The SOC 3 report includes testing of the following in-scope applications:

Application	Description
Kalix	Kalix is a Platform as a Service tool that manages the challenging aspects of building scalable, data-centric microservices and APIs from the application architecture, data management, and cloud infrastructure perspectives. Kalix enables developers to rapidly deliver the high-performance, low-latency services that enterprises need as they move their critical business workloads to the cloud.
Akka	Akka is a library toolkit used for businesses to build, deploy, and rune large-scale applications.
GitHub	GitHub is the code repository tool used by the Company to host code for the production system.
Okta	Okta is the identity and access management (IAM) service used to provide access management and single sign-on services for the Company.

Principal Service Commitments and System Requirements

Lightbend designs its toolkits and PaaS solutions to meet its regulatory and contractual commitments. These commitments are based on the services that Lightbend provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Lightbend has established for its services.

Principal Service Commitments and System Requirements (continued)

Lightbend establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Lightbend's system policies and procedures, system design documentation, and contracts with clients.

Lightbend has the following key commitments to provide:

- Security, which includes but is not limited to:
    - Securing customer data,
    - Limiting system users access to the least information needed to perform their job responsibilities, and
    - Use of encryption technologies to protect customer data both at rest and in transit.
- Availability - maintaining 24/7 system availability.
- Confidentiality - classifying data and maintaining confidentiality of data classified as such and restricting access to this information to only those who are authorized.

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 Lightbend toolkits and platforms.

Significant Changes to the System

There were no changes that are likely to affect report users' understanding of how the system is used to provide the service for the period January 1, 2024 to March 31, 2024.

RELEVANT ASPECTS OF INTERNAL CONTROL

As defined by the American Institute of Certified Public Accountants (AICPA), internal control is a process affected by an entity's board of directors, management, and other personnel and consists of five interrelated components:

- Control Environment
- Risk Management
- Information and Communication
- Monitoring
- Control Activities

This section briefly describes the essential characteristics and other interrelated components over the trust services criteria of security, availability, and confidentiality, as they pertain to the Company.

Control Environment

Management and the board of directors take their role in overseeing internal controls seriously, and their responsibilities are defined and documented. The board meets at least quarterly to oversee controls, operations, and business objectives. The Company has a Corporate Ethics Policy and a procedure for reporting violations.

The Company distributes the Acceptable Use and Corporate Ethics policies to all employees and requires that each employee acknowledge the policies at the time of hire and annually thereafter. The Company believes it has the proper incentives in place that would tend to discourage conflicts of interest and/or improper behavior.

Control Environment (continued)

The Company exercises significant diligence in hiring competent, qualified professionals, and then providing employees with the appropriate on-the-job training. Company employees receive new hire orientation training, and most employees receive continuing education through online industry-related training and periodic industry conferences. The board of directors has sufficient independence to effectively oversee management.

The Company's management team meets at least every other week. The members of the management team are the:

- Chief Executive Officer ("CEO")
- Director of Finance
- Chief Financial Officer ("CFO")
- Chief Marketing Officer ("CMO")
- Chief Technology Officer ("CTO")
- Executive Vice President
- Vice President, Business Development and Alliances
- Vice President, Global Solution Architecture and Technology Alliances
- CISO/Chief of Staff
- Vice President, Engineering
- Senior Product Manager, Cloud
- Vice President, Marketing
- Vice President, Strategic Accounts

Lightbend uses One Trust's Certification Automation system to maintain policies and supporting controls, to track review of such controls, as well as employee/contractor awareness training around each applicable policy.

Lightbend has a defined organizational structure. The Company organizational chart is made available to all employees, and reporting relationships are kept current on that chart. Roles and responsibilities are defined in written job descriptions and communicated to employees, as well as supervisors and managers. Job descriptions document the objectives, responsibilities, reporting lines, needed qualifications, and other elements of the role. Senior management periodically reviews reporting relationships, job descriptions, and the organizational structure as part of planning and adjusts the reporting structures, as needed, based on changing commitments, requirements and goals.

Human Resources ("HR")

The Lightbend Chief Financial Officer, as well as upper management, oversees HR functions, including employee search, recruiting, orientation and industry-related training.

The Lightbend HR function is guided by established policies and procedures for hiring, promoting and compensating, training, and termination of employees.

Employee compliance with behavioral expectations is evaluated as part of their job performance. Candidates for promotion must have demonstrated a commitment to ethical standards through their own actions, and by setting an example for other employees.

Lightbend has a process in place to evaluate the competency of employees and identify any development needs or opportunities on a regular basis. Complaints indicating departure from behavioral standards are investigated by managers and are documented as necessary.

Control Environment (continued)

Human Resources ("HR") (continued)

As part of Lightbend's performance management process, all managers are required to establish expectations and evaluate performance for the employees they manage. Managers frequently meet with their employees on an individual basis to discuss performance and set expectations.

A critical part of providing a work environment with strong ethics and controls starts with the hiring and training processes. Management takes an active role in recruitment, including screening applicants, checking references, completing background checks, and providing the orientation of new team members.

Potential employees must pass a background check as part of the onboarding process.

New Hire Onboarding

Before an individual joins the Lightbend team, management must first identify the need for additional personnel. A job requisition is drafted and approved by the head of the relevant department. If the job requisition does not have a corresponding job description, one is created and reviewed by the appropriate manager. This is then posted internally and to various online job boards and career sites.

The Lightbend management team reviews resumes to identify qualified candidates. When a qualified candidate is identified, he or she is further evaluated through an online or phone screening process. If the candidate passes the phone screening, they are scheduled for a series of interviews with the individuals in the respective team in which they will work.

When interviews are completed, a hiring decision is made. If management chooses to issue an offer letter to the prospective hire, Lightbend management contacts the CFO, who assists with issuance of the offer letter and communication with prospective employees. If the prospective employee formally accepts the offer letter, the HR manager completes a background check for the individual.

When the new employee begins work on his or her first day, they meet with their manager and HR to review necessary documentation. The new employee then attends a new employee orientation meeting.

Throughout the hiring process, progress and completion of tasks are recorded on a new hire checklist. This checklist is maintained by the Lightbend management team.

Policy for Training

All new employees are required to attend an orientation that introduces them to the Lightbend culture, business operations, policies and procedures, and the applications comprising the Lightbend system.

Ongoing employee training consists principally of on-the-job training. When external training for an employee will contribute to Lightbend's business goals, Lightbend will pay for pre-approved, job-related courses and, if applicable, related travel expenses. Additionally, Lightbend offers optional internal training seminars regarding specific Lightbend products and processes, as well as access to course material on our learning platform, Lightbend Academy. Employees are also provided access to industry publications and resources for continued self-education.

Security Awareness Training

Lightbend maintains a security awareness program through various mechanisms including:

- Employee orientation program
- Security awareness training at the time of hire and annually thereafter, which includes online acknowledgement of the information security policy and completing the Company's information security program training course, as well as information regarding the roles and responsibilities of all employees and contractors with respect to information security.

Control Environment (continued)

Security Awareness Training (continued)

- Periodic email communications from the information security team and other management, including training and videos on new security features and requirements.

Employment Termination

Employment can be terminated by Lightbend at any time as it operates as an at-will employer. Employee terminations can be voluntary or involuntary. Involuntary terminations require prior documentation of issues and performance coaching with the individual in question to resolve those issues.

Risk Assessment

As part of Lightbend's risk management activities, Lightbend conducts an enterprise risk assessment at least annually. The assessment is a collaborative process whereby the management team draws on collective industry, enterprise, technical, and regulatory knowledge to identify key risks to business operations. As part of the management team meeting, a formal risk assessment matrix is created to memorialize identified risks, risk rankings, and mitigation strategies. The risk assessment matrix guides internal risk management and monitoring activities for the forthcoming year. The risk assessment matrix is revisited and revised for marked changes or developments in market, industry, regulatory or legal risks.

For financial risks and risks for the overall business, Lightbend maintains insurance coverage through an external service provider.

As part of the regular risk assessment, management identifies information technology ("IT") risks, ranks those risks, and develops mitigation strategies which are monitored by the information security team for successful mitigation. In addition to the regular risk assessment, risk is evaluated daily through defined and repeatable IT and business processes. These processes consider a multitude of risks, including security, logical access, availability of application services, and confidentiality of customer data at the heart of the Lightbend system. Mitigation strategies are developed by management iteratively to respond in an agile fashion to ever-changing risk landscapes.

The need for high availability warranted Lightbend's investment in redundant cloud infrastructure to support the Company's application, thereby eliminating single points of failure.

To support IT risk management activities, management conducts annual penetration testing. Each item identified on the penetration tests is reviewed and prioritized for mitigation. Mitigations may include a change in policy as well as monitoring or periodic evaluation. Controls may be evaluated daily, weekly, monthly, or quarterly, per the risks and business needs.

Information and Communication

Information Systems

Lightbend's information systems have been engineered on the principles of high availability, security and confidentiality.

Lightbend's Kalix product is available on several different cloud providers, including Amazon Web Services ("AWS") and Google Cloud Platform ("GCP"). In each environment, Kalix is set up to offer customers multi-zone redundancy to ensure availability. The portion of Kalix where customer data is stored is separated and secured logically in a separate database from all other customers and does not share infrastructure with any other Lightbend systems.

Through methodology which is documented and tested within the Lightbend business continuity and disaster recovery plan, our essential systems, and especially our platform Kalix, are highly resilient and resistant to disaster.

Information and Communication (continued)

Information Systems (continued)

Kalix customer execution clusters (where the customer's business logic runs) are located in multiple regions, according to the customer's data sovereignty requirements, and always replicated across zones within each region, on any cloud provider.

Lightbend offers each customer training and enablement materials on the systems as part of the customer onboarding process.

Communication

Lightbend endeavors to inform internal and external users of the structure of the system so they may understand their role in the system and the results of system operation.

System descriptions are available to authorized external users that describe relevant system components as well as the purpose and design of the system.

Internal users learn about Lightbend systems beginning with their orientation and continuing as needed with on-the-job training and/or specific training courses. The internal wiki holds both written documentation as well as links to specific documents on the Lightbend internal file server for Lightbend employees such as product and system information.

Lightbend maintains an online ticketing system to capture and handle support requests, for both internal users and customers. Lightbend responds to such requests in a timely manner.

Lightbend also reviews all customer contracts to ensure that security and confidentiality commitments are met.

Monitoring

Monitoring systems assist Lightbend in meeting service level agreement requirements. Technical processes are monitored by automated systems such as Grafana, Elastic Security Incident and Event Management ("SIEM") and Pingdom. Staff members receive automated alerts via PagerDuty and Slack when there is any substantial decrease in system performance or a significant security event so they can respond to the issue. Lightbend maintains an on-call schedule of responders to react to issues at all times.

Monitoring activities are intended to identify and remediate areas of risk including strategic risk, financial risk, operational risk and legal/regulatory risk.

Management and supervisory personnel monitor the quality of internal control performance via frequent observation, interaction and performance of their assigned duties.

Critical job functions have been designed and implemented to provide inherent monitoring through separation of job functions, management oversight and systematic controls. Management reviews the functionality of software products and application configurations as they move through the development process and into production.

Logging and monitoring software platforms are used to collect data from system infrastructure components and from endpoint systems. The logging and monitoring software is used to monitor system performance, potential security threats and vulnerabilities, and resource utilization, and to detect unusual system activity or service requests.

This software sends an alert message via PagerDuty to the appropriate team members, escalating automatically as needed until the alert is confirmed.

Throughout each of the above processes, identified deficiencies are communicated to the relevant management personnel and appropriate follow up actions are initiated.

Monitoring (continued)

Lightbend uses multiple cloud providers to host portions of its platform and services and has automated alerts that will notify the appropriate team members if essential services on these cloud platforms are unavailable or not performing to expectations.

Lightbend leverages various tools and techniques to proactively monitor the production environment. These tools are designed to identify issues and alert responsible staff of the issue before it impacts Lightbend end users or customers.

CONTROL ACTIVITIES

Policies and Procedures

Policies and procedures are a key tool for process standardization and communication of key control elements. Relevant policies and procedures are updated by their respective owners at least annually and made available to Lightbend employees through the One Trust Certification Automation system. Information security policies include, but are not limited to:

- Incident management policy
- Change management policy
- Data retention and disposal policy
- Vulnerability and penetration testing management policy
- Information classification policy
- Acceptable use policy
- Access control policy

Logical Access

Access controls are in place to prevent any unauthorized access. Lightbend's access control policy requires that access be denied by default, follow a least privilege principle, and be granted only upon business need. Lightbend uses centralized authentication and authorization tools to restrict access to the systems and services within the environment. Each user account is unique and identifiable to an individual user.

Access is controlled through addition of individual user accounts to established groups within Okta. Based on the configuration of a group, any access requests require explicit approval from IT.

All administrator access is controlled through separate administrator accounts individually assigned to appropriate personnel. This allows administrative access to be logged, audited, and managed through our central Okta server.

Employees are granted system access commensurate with their job responsibilities. The departments' managers and network administrator are responsible for assigning and maintaining access rights to the Lightbend internal and production network environments and related devices and applications.

For new hires, the hiring manager communicates with the internal IT department requesting appropriate application access. The internal IT department reviews the request and validates that the request was authorized by an appropriate individual. Once satisfied that the request has been properly authorized, access is granted in accordance with the new hire checklist. Access is granted to the minimal set of permissions appropriate to the new employee's role.

Control Activities (continued)

Physical Access

All server computer facilities and physical access thereto are controlled at cloud infrastructure data centers. No servers or computer facilities for the Lightbend platform are hosted on Lightbend premises.

Access Deprovisioning

Account terminations are initiated by a manager in collaboration with internal IT and HR. Accounts are disabled by the internal IT department in a timely manner once the termination takes effect. Driven by an employee termination checklist, the termination process includes:

- User access to all applications will be revoked or disabled.
- Access to the domain, administrator, database and critical network devices will be revoked or disabled appropriately.
- Physical assets such as equipment, and company credit cards (if applicable) are collected and recorded in the HR asset system.

Under certain conditions, domain accounts may need to remain accessible after the termination date. In these cases, the account password is changed and the account is marked as locked. Any necessary data is migrated from the terminated account to an active account. When management determines that all necessary data has been preserved, the account is fully closed.

Network Security Overview

System Passwords

Users are required to enter a unique user ID and password to access any Lightbend network or application. Complexity standards for passwords have been established to enforce control. The following password policy settings are in place as system-based preventive controls:

- Minimum length of eight (8) characters.
- Maximum age of six months.
- Initial passwords must be changed at first login, and all default passwords must be changed before use.
- Multi-factor authentication (MFA) to be used wherever possible.
- Sessions are locked out after a specified period of inactivity or repeated unsuccessful login attempts.
- Passwords should be difficult to guess and brute force programmatically; higher entropy is better such as longer passwords and phrases, special characters, mixed cases, and passphrases are all encouraged.
- Passwords shall not be repeated whenever required to be rest.
- SMS-based factors are not permitted for MFA.

Cryptography

Cryptographic controls and approved algorithms are used for information protection within the service environment and are implemented based on company policies and Federal Information Processing Standard 140-2 Level 1, or higher. Cryptographic keys are managed throughout their lifecycle (e.g., ownership, generation, storage, distribution, periodic rotation, and revocation) using AWS/GCP key management services in accordance with key management procedures.

User requests to Lightbend's systems are encrypted via Transport Layer Security ("TLS") using certificates from an established third-party certificate authority.

Network Security Overview (continued)

Cryptography (continued)

Remote system administration access to Lightbend's web and application servers is available through cryptographic network protocols (i.e., SSL).

All data at rest, whether on workstations or on cloud platforms and databases, and node-to-node communication within the production environment is encrypted.

Workstations

All company workstations have system passwords and storage encryption enabled, as well as antivirus protection. Firewall systems are also enabled on all workstations, and workstations are checked at least quarterly to ensure automatic updates are enabled to keep workstations patched.

Servers

Antivirus protection is also applied to all server systems administered by Lightbend in our cloud provider environments and is updated continually.

This protection is monitored centrally, and any thread detections produce alerts, as well automatically isolating the potential threat node from the remainder of the network.

Firewall

System firewalls are configured for all production systems, limiting unnecessary ports, protocols, and services. These configurations are reviewed on an annual basis.

Intrusion Detection

Suspicious activity triggers alerts that are sent to responsible information security staff via Slack notifications. The responding individuals investigate the alerts and, if necessary, escalate the issue following the defined incident response policy.

A formal network diagram outlining boundary protection mechanisms (e.g., firewalls, IDS, etc.) is maintained for all network connections and reviewed annually by IT management.

Access Reviews

User access lists for applications, secured folders, root accounts and databases are reviewed by the Information security team leads on a quarterly basis. If any unnecessary access accounts are found, appropriate remediation action is taken.

Security Incident Management

Lightbend has implemented a security incident management policy that defines roles and responsibilities and reporting and handling procedures. This policy includes, but is not limited to:

- Triage,
- Escalation/De-escalation,
- Impact analysis,
- Treatment,
- Root cause analysis, and
- Notifications/disclosures to affected internal and external stakeholders.

Automated mechanisms monitor system processes and alert IT teams per defined and configured events, thresholds, or metric triggers. Incidents may also be reported via email.

Lightbend teams use the established incident classification, escalation, and notification process for assessing an incident's criticality and severity, and, accordingly, for escalating to the appropriate groups for timely action.

Network Security Overview (continued)

Security Incident Management (continued)

The IT team documents, tracks, and coordinates responses to security incidents. Where required, security incidents are escalated to the privacy, legal, or executive management team(s) following established forensic procedures to support potential legal action after an information security incident. Incidents are tracked and monitored until resolved.

Post-mortem activities are conducted for customer-impacting incidents or incidents with high severity ratings. Incident and security post-mortem trends are reviewed and evaluated on a periodic basis and, where necessary, the security program may be updated to incorporate improvements identified as a result of incidents.

Vulnerability Assessment and Penetration Testing

Lightbend continually performs scans to identify vulnerabilities and assess the effectiveness of the patch management process. These scans are used to ensure compliance with baseline configuration templates, validate that relevant patches are installed, and identify vulnerabilities. The scanning reports are reviewed by appropriate personnel and remediation efforts are conducted in accordance with the vulnerability and penetration testing management policy.

Lightbend uses the industry-recognized Common Vulnerability Scoring System ("CVSS") scores to help determine the severity of an issue, but Lightbend may deem any issue critical regardless of CVSS score.

The applicable security patches are applied immediately or during a scheduled release to the environment based on the severity of the vulnerability. Processes are in place to evaluate patches and their applicability to the environment.

All changes are reviewed and tested, at a minimum, for their quality, performance, impact on other systems, recovery objectives, and security features before they are merged into the main branch and released to production using a defined release process.

Patches are released in accordance with change management and software development policies. Emergency out-of-band security patches are expedited for more immediate release.

A patch management process exists to confirm that operating system level vulnerabilities are remediated in a timely manner. Production servers are verified for patch compliance on at least a quarterly basis.

Penetration testing is performed at least annually on the system by an independent third party assessor.

The penetration test scope is determined based on Lightbend's areas of risk and compliance requirements. Issues identified are risk-ranked to prioritize the remediation of discovered vulnerabilities. The penetration test results are reviewed, evaluated and remediated based on severity in accordance with the vulnerability and penetration testing management policy.

Change Management

Lightbend change management and software development policies have been established to propose, review, deploy, and manage changes through designated responsibilities with the objective of minimizing risk and customer impact. Software development changes are based on the software development life cycle ("SDLC") methodology which introduces security and privacy control specifications during the feature/component design and throughout the development process.

Changes that affect the functionality and security of the system components are communicated to internal and external users via release notes published on the customer-facing website.

Network Security Overview (continued)

Change Management (continued)

Software, system, and configuration changes, including regular releases and hot fixes, are managed through a formal change and release management procedure and tracked using a centralized ticketing and version control system (GitHub). Changes are requested, approved, tracked, and implemented throughout the release life cycle, which includes product and engineering planning, release management, deployment, and post-deployment support phases. Change requests are documented, assessed for their risks, and evaluated/approved for acceptance by the designated personnel.

Access to promote changes to production is restricted to authorized personnel based on their job responsibilities.

Formal security and quality assurance testing is performed prior to the software release through each pre-production environment (i.e., development and staging) based on defined acceptance criteria. Policy prohibits the use of production data in testing or development environments. The results of the quality assurance testing are reviewed and approved by the appropriate personnel prior to moving the release to production. Changes are reviewed for their adherence to established change and release management procedures prior to closure.

Once deployed, changes are monitored for success; failed implementations are immediately rolled-back, and the change is not considered as completed until it is implemented and validated to operate as intended.

Changes deployed into production are performed one node at a time, so that any error introduced cannot affect the entire platform before it can be resolved, assuming any error is detected at this late stage.

A log management process has been formalized to make sure that access to change the log configuration and access to modify logs is restricted.

Data Backup

The Company maintains backups of the production version of the Akka and Kalix application code in the version control system (Github).

Formal procedures that outline the backup and recovery process are documented. The procedures are reviewed by IT management and updated annually.

Backups of the databases supporting the Kalix platform are performed daily using an automated backup utility. Backups are encrypted at rest. The backup utility is configured to store backups in cloud storage. The Company regularly restores a subset of files from backup, and the results are verified as successful.

Disaster Recovery

Planning for the business continuity of Lightbend in the aftermath of a disaster is an essential part of an organization's risk management program. Preparation for, response to, and recovery from a disaster affecting the administrative functions of the company require the cooperative efforts of many functional areas and supporting organizations.

Lightbend has a detailed business continuity and disaster recovery plan, which is tested and reviewed annually.

Lightbend’s platform, Kalix, is always hosted in multi-zone clusters at the various cloud provider facilities, meaning an entire facility can be offline without affecting availability of our platform.

Our team is distributed, so localized disasters affect a small percentage of the team, allowing the remainder of the company to continue to operate.

Network Security Overview (continued)

Vendor and Contractor Management (continued)

The company maintains detailed plans on failover scenarios for all of our essential infrastructure, ensuring no single failure would prevent us from serving our customers.

Vendor and Contractor Management

Lightbend has a detailed policy in place around vendors and subcontractors and the solutions/products they offer that Lightbend uses.

Contractors working on behalf of Lightbend must acknowledge the applicable information security policies, just as employees do, as part of their onboarding process.

Vendors and their solutions are tracked, and risk assessments are performed annually for existing vendors and for any new vendor being considered. Lightbend then takes appropriate action based on that assessment.

Lightbend has a procedure in place for terminating vendors. This process includes security procedures that need to be followed in the event of any vendor termination.

The Company maintains an inventory of production information assets including details on asset ownership, data classification and location. The asset inventory listing is reviewed and updated by management on an as-needed basis.

Additional Controls Related to Availability

Lightbend's production system is hosted on resilient cloud infrastructure, distributed across multiple zones for high availability, even in the event of an outage. The infrastructure is configured to scale capacity as required whenever practical, and if the bounds of this auto-scaling are predicted to be approached, to notify operators to configure higher limits.

Additional Controls Related to Confidentiality

Lightbend classifies all data it stores and treats sensitive (non-public) data as confidential. Lightbend has a detailed data classification policy which identifies confidential information in the system and defines instructions for handling and labeling of confidential information. The Company also has formalized policies in place detailing data retention and disposal guidelines. All equipment that handles any sensitive data is disposed of or recycled securely. System components are configured such that the Company and its customers' access is appropriately segmented from other tenant users.