Lexer Pty Ltd
SOC 2 Type 1 Report

Service Organisation Controls Assurance Report on Trust Services Principles and criteria for Security and Confidentiality (TSP Section 100A - 2016)

Prepared pursuant to ASAE 3150, 'Assurance Engagements on Controls'

13 December 2018

TABLE OF CONTENTS

SECTION I: INTRODUCTION

This report is designed to provide information to be used for supplier risk management purposes by Lexer Pty Ltd (Lexer) customers.

The focus of the report is on Security and Confidentiality controls related to the provision of the Lexer Identify platform that may be relevant to Lexer customers, but does not encompass all aspects of the services provided or procedures followed by Lexer.

This report has been prepared in accordance with requirements of the Australian Standard on Assurance Engagements ASAE 3150 'Assurance Engagements on Controls'.

The focus of this report is on the design and implementation of the Security and Confidentiality controls Lexer has established within the Lexer Identify control environment that may be relevant to its customers, and encompasses:

- Section II - statement by the management of Lexer
- Section III - a report prepared by PwC, Lexer's independent service auditor
- Section IV - an overview of Lexer's business prepared by the management of Lexer
- Section V - the description of the operations and applications covered by this report, the control environment, summary of the control objectives and user control considerations prepared by the management of Lexer
- Section VI - the control objectives, related controls as well as results of tests performed by PwC, the independent service auditor
- Appendix A - management's response to findings raised by PwC.
- Appendix B – list of criteria.

SECTION II: MANAGEMENT STATEMENT

STATEMENT BY LEXER PTY LTD (LEXER) ON THE DESIGN AND DESCRIPTION OF CONTROLS OVER LEXER'S IDENTIFY SYSTEM

The accompanying description has been prepared for customers of Lexer's Identify system who have a sufficient understanding to consider the description. Lexer confirms that:

b) The accompanying description at Section V fairly presents the Lexer Identify system (the system) designed and implemented for clients as at 13 December 2018, including:

- The types of functions or services provided and, where relevant, locations, including, as appropriate, the nature of the data stored and/or information processed.
- The procedures by which data was recorded and stored and information was processed.
- How the system dealt with significant events and conditions.
- The process used to prepare reports for clients.
- Relevant control objectives and controls designed to achieve those objectives.
- Controls that we assumed, in the design of the system, would be implemented by clients, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by Lexer alone.
- Identification of any parts of the system which were operated by a third party service organisation (sub-service organisation) on Lexer's behalf and whether the description is inclusive or exclusive of the relevant control objectives and controls.
- Other aspects of Lexer's control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting clients' information.
- Information relevant to the scope of the system being described, without omission or distortion, while acknowledging that the description is prepared to meet the needs of Customers and may not, therefore, include every aspect of the system that other users may consider important in their own particular environment.

c) The controls related to the control objectives stated in the accompanying description were suitably designed as at 13 December 2018, including that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified; and
(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

Yours sincerely,

Chris Brewer

CFO

To: Chris Brewer (Chief Financial Officer, Lexer)

Type 1 Independent assurance report on Security and Confidentiality Trust Services Principles for Lexer Identify

Scope

We have undertaken a reasonable assurance engagement on:

- the design and implementation of controls within Lexer's Identify system (the controls), comprising of Security and Confidentiality related controls as at 13 December 2018 relevant to the Security and Confidentiality control objectives as specified by the American Institute of Certified Public Accountants within their "Section 100A – Trust services principles and criteria for security, availability, processing integrity, confidentiality, and privacy (2016)" (TSP Section 100A) publication; and
- Lexer's description of its Identify system at Section V (the description).

Lexer's responsibilities

Lexer is responsible for:

a) the services within the Identify system;

b) identifying the control objectives;

c) identifying the risks that threaten achievement of the control objectives;

d) designing controls to mitigate those risks, so that those risks will not prevent achievement of the identified control objectives;

e) implementing the controls as designed; and

f) preparing the description and accompanying Statement, Section II, including the completeness, accuracy and method of presentation of the description and Statement.

Our Independence and Quality control

We have complied with the relevant ethical requirements relating to assurance engagements, which include independence and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

In accordance with Auditing Standard ASQC 1 *Quality Control for Firms that Perform Audits and Reviews of Financial Reports and Other Financial Information, and Other Assurance Engagements*, PwC maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Our responsibilities

Our responsibility is to express an opinion on Lexer's Statement regarding the suitability of the design of controls to achieve the control objectives, the presentation of Lexer's description of the Identify system and implementation of Lexer's controls within the Identify system as designed, based on our procedures. We conducted our engagement in accordance with Standard on Assurance Engagements ASAE 3150 *Assurance Engagements on Controls* issued by the Auditing and Assurance Standards Board. That standard requires that we comply with relevant ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the controls are suitably designed to achieve the control objectives, the description is fairly presented and the controls, necessary to achieve the control objectives, were implemented as designed as at 13 December 2018.

An assurance engagement to report on the design, description and implementation of controls involves performing procedures to obtain evidence about the suitability of the design of controls to achieve the control objectives, the completeness, accuracy and method of presentation of the description of the Identify system and the implementation of those controls as designed as at 13 December 2018.

The procedures selected depend on our judgement, including the assessment of the risks that the controls are not suitably designed, the description is not fairly presented or the controls were not implemented as designed. Our procedures included testing the implementation of those controls that we consider necessary to achieve the control objectives stated in the description. An assurance engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Inherent limitations

Because of the inherent limitations of any internal control structure it is possible that, even if the controls are suitably designed and implemented as designed, once the controls are in operation the control objectives may not be achieved so that fraud, error, or non-compliance with laws and regulations may occur and not be detected.

An assurance engagement on the implementation of controls at a specified date does not provide assurance on whether the controls operated effectively as designed or will operate effectively in the future. Any projection of the outcome of the evaluation of the suitability of the design of controls to future periods is subject to the risk that the controls may become unsuitable because of changes in conditions.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. In our opinion, in all material respects, Lexer's Statement is fairly presented, in that:

a) the controls within the Identify system were suitably designed as at 13 December 2018 to achieve the TSP Section 100A Security and Confidentiality control objectives;

b) the controls were implemented as designed as at 13 December 2018; and

c) the description fairly presents the Identify system as at 13 December 2018.

Use of report

This report has been prepared for use by Lexer Identify Customers for the purpose of supplier risk management. We disclaim any assumption of responsibility for any reliance on this report to any person other than Lexer Identify Customers, or for any other purpose other than that for which it was prepared.

PricewaterhouseCoopers

Matthew Hunt
Partner

Melbourne
13 December 2018

SECTION IV: OVERVIEW OF LEXER AND THE SERVICES PROVIDED TO CUSTOMERS

POWERFUL DATA. SOPHISTICATED PRODUCTS. EXPERT ADVICE. GENUINE RESULTS.

Lexer believe that nothing matters more than customers, so we offer data, products and advice to help **customer-loving companies genuinely understand and engage** customers with utmost security.

The combination of Lexer's **Customer Data Platform, Customer Engagement Hub** and **Client Success Team** provide the **genuine understanding of customers** you need to effectively **sell to and serve them.**

Genuinely Understand & Engage

We put data to work, so brands can genuinely engage with customers and prospects.

Lexer is a whole of company solution, putting actionable data and sophisticated products in the hands of your strategy, sales, marketing, service, investor teams and beyond. We deliver the peace of mind that teams are operating with a genuine understanding of your customers and have the products to engage with them in real time.

DATA

Enriched profiles: Combine data to provide an enriched profile of your current and prospective customers.

Even companies that have spent hundreds of days and millions of dollars on a single view of customer don't have one. They generally only have a customer's interactions with the brand. Lexer securely bring all accessible data together in one place. And in weeks or months, not years.

LEARN

Customer insight: Uncover valuable actionable insights about your current and prospective customers.

Traditional segmentation and personas are useful. But today that's not enough, we need to know more. Who are they really? What motivates and entertains them? What distinguishes and unifies them? Where are they and why? Lexer's 15,000+ human attributes provide insights about human beings and their behaviours.

SELL

Drive revenue: Targeted and relevant sales messaging in paid, owned and earned media.

Customers hate irrelevant advertising almost as much as your CFO hates paying for it. With an enriched profile of current and prospective customers, there's nothing to stop relevant marketing. Lexer provides data and products that enable genuine targeting, speed to market and return on investment.

SERVE

Build loyalty: Personalised and genuine customer service and support via social media.

Most people understand that it's more valuable to keep a good customer than win a new one. But the decisions regarding the channel within which to do this is often misunderstood. Lexer offers customer service products for the most cost effective channels that exist.

Customer Data Platform

POWERFUL DATA

Lexer's Customer Data Platform provides a secure environment that offers privacy compliant data from Public and Partner sources on over 500 million people. And that's before we add any of your 1st party data.

CONSUME

Consume customer data from first, second and third party data sources including CRM, transaction, Wi-Fi, Beacon, Mobile app and survey data and importantly beyond their interactions with your brand from partners including Experian, Roy Morgan and Dun and Bradstreet and across social, news, blogs, forum and other publicly available sources.

UNIFY

Machine learning is applied to perform unification using determinative and probabilistic methods to perform linkage across all accessible data sources.

ENHANCE

Artificial intelligence and machine learning is applied to build and maintain over 15,000 attributes that Lexer has built to help users understand human beings and their behaviours

SECURE

The approach to privacy and security is paramount, both in process and compliance. There is good reason why multi-billion dollar companies trust Lexer to handle and store their customer data.

All accessible customer data enriched and secured in one place.

Customer Engagement Hub

SOPHISTICATED PRODUCTS

Multi-vendor SaaS stacks introduce security risks and operational cost inefficiency. Lexer's antidote to this is the Customer Engagement Hub, one interface, including three products to enable the whole organisation to genuinely understand and engage customers.

LISTEN

Customer and competitor monitoring & analytics

Monitor competitors, identify influencers, monitor risk, engage in trending topics across all social and news content in real-time. Live dashboard reports, custom reports and notifications.

IDENTIFY

Customer insight, segmentation & activation

Uncover valuable insights and segments with the most comprehensive customer and prospect data set available. Create segments and target in paid and owned media.

ENGAGE

Customer service, support and sales

Customer service across Facebook, Twitter and Instagram with insightful profiles on each customer, full contact history, status management, team analytics and monitoring.

One solution available to the whole company.

Client Success Team

EXPERT ADVICE

Innovative companies know that data and software alone isn't sufficient to transform the way an organisation understand and engage customers. So Lexer offer expert strategy, solutions, success and support talent to work with your internal team and strategic partners.

An expert team to lead the successful implementation and ongoing relationship made up of:

STRATEGY

Lead and support the development of a data transformation roadmap documenting problems, opportunities and solutions - both short and long term in a bid to drive your business towards a data first operating culture.

SOLUTIONS

Data and dashboard solutions architecture to support your use cases and help get the greatest possible value out of Lexer data and products.

SUPPORT

Onboarding, training, product and technical support via dashboard chat, email, phone and in person to ensure an optimal user experience.

Expert advice to help you accelerate and execute your data transformation.

SECTION V: MANAGEMENT'S DESCRIPTION OF THE SYSTEM

Terminology

"**AWS**" means Amazon Web Services

"**Board**" means the board of directors of Lexer

"**ELT**" means the executive leadership team of Lexer

"Information Security Management System" or "ISMS" means the set of policies and procedures for systematically managing Lexer's Restricted Information

"Lexer" means Lexer Pty Ltd

"Restricted Information" means information that is very sensitive in nature and is strictly restricted by Lexer, the government or any other agreements between Lexer and third parties (including clients and partners).

"Services" means the Lexer Identify products and services that are purchased by a client and made available online by Lexer, including associated offline components

"VPN" means virtual private network

Introduction

This Service Organization Controls 2 (SOC 2) report is designed to provide assurance to Lexer clients that the company maintains an effective control environment to mitigate risks that impact systems connected with the handing of Restricted Information. This report has been prepared to provide information on the AICPA Trust Service Principles of Security and Confidentiality applicable to Lexer.

This section of the report (Section V) provides an overview of Lexer, describing the processes and controls in place that comprise an effective control environment. Section VI provides the principles and criteria and details of the control activities supporting each criterion.

Scope of Report

This report focuses on processes and controls applicable to Lexer's internal control environment.

The scope of this report covers critical systems, applications, networks, telecommunication links, human resources, and information assets connected with the handling of Restricted Information.

INFRASTRUCTURE AND SOFTWARE

The Lexer Identify application is written in Ruby, Scala and Javascript running on Debian and Ubuntu Linux in AWS. The in-scope software and applications are as follows:

System	Description
Lexer Identify Platform Processing Environment	AWS hosted processing environment operating the Lexer Identify Service
Lexer Identify Platform Dashboard	Client facing, browser based software (SaaS) used by clients to access the Lexer Identify Services
Lexer API	Client facing, server-to-server software used to securely transfer Client Data and Partner Data
Lexer SFTP	Client facing, sftp server used to securely transfer Client data and Partner Data
AWS Console	AWS infrastructure management system
Github	Code version management system
BuildKite	Build & release management system

The in-scope Lexer applications, databases and operating systems are hosted and controlled within AWS using a combination the following AWS technologies:

System	Description
AWS Elastic Compute Cloud (EC2)	Virtualization Platform (database and application servers)
AWS Elastic Block Storage (EBS)	Block Storage attached to EC2 nodes
AWS Simple Storage Service (S3)	Object Storage for social data and backups
AWS Relational Data Service (RDS)	PostgreSQL as a service for dashboard services
AWS Identity Access Manager (IAM)	Control groups, roles and user access to services
AWS DynamoDB	Data Storage for social data
AWS Route53	Domain name management
AWS VPC & Networking	Firewall, Access & VPN configuration
Elasticsearch (ES)	Elasticsearch search engine
RabbitMQ	Message Broker for high-volume services

All work performed in relation to control objectives and control procedures as documented in Section VI was conducted based on this scope. The carve-out approach was used in relation to all AWS services as noted in the Controls at Subservice Organisations Section below.

Operating effectiveness of controls has not been considered as part of this report. PwC's independent testing relates only to the design and implementation of controls.

Company Overview

ORGANISATIONAL STRUCTURE

Board of Directors
The Board is the overall and final body responsible for all decision-making within Lexer. The Board is composed of experienced executives, with a broad and diverse range of technology, financial, sales, and general business experience.

Executive Leadership
The ELT serves as the link between the Board and operational level management. The ELT plays a critical role in the operations of the Company. The ELT has representation from all business functions and serves as the multidisciplinary decision-making body of the Company.

The ELT meets on a weekly basis to discuss operational matters for quick decision-making and implementation, and on a monthly basis to discuss strategic aspects of the business. The mandate of the ELT is to ensure the business is executing the defined strategy.

Security Team
The security team is led by the Information Security Officer. The team defines security policies and is responsible for security governance, training and awareness, product and platform security and security operations.

Development Team
The Development Team is led by the Chief Technology Officer and is broadly divided into two sub-teams; infrastructure and product.

The infrastructure team is responsible for the architecture of the Services which exists across the AWS environment and for the design and implementation of adequate and appropriate measures for ensuring that security and confidentiality requirements are met.

The product team is responsible for design and delivery of the product roadmap, secure and stable applications and incident and bug resolution.

The collective development team is responsible for change management, supporting the production environment, monitoring for issues and events, and incident management.

Sales, Service, Support & Marketing
The sales, services, support and marketing functions are organised into the geographical segments in which they operate. These division spearhead the marketing, sales and service initiatives and are responsible for positioning Lexer's services in the global market.

Finance & Legal
The Finance & Legal team is responsible for meeting financial reporting compliance requirements, as well as corporate compliance and risk management, and is led by the Chief Financial Officer.

Human Resources
The human resource team is led by the HR Manager and is responsible for identifying, on-boarding and retaining suitably qualified team members, overseeing ongoing training and education requirements and off-boarding terminated personnel.

Services provided by a Third Party
Lexer's facilities do not host any systems that transmit, process, or store Restricted Information. Lexer uses Amazon Web Services (AWS) for services, including Identity and Access Management (IAM), cloud computing (EC2), Elastic Block Storage (EBS) and electronic storage (S3). AWS' controls are reviewed annually via third party attestation reports to provide Lexer with comfort the control environment deployed by AWS on its behalf aligns with the Lexer Security and Confidentiality governance framework.

Criteria and Controls

The criteria for the Security and Confidentiality principles are organized into (a) the criteria that are applicable to both principles (common criteria) and (b) criteria applicable only to a single principle. The common criteria constitute the complete set of criteria for the Security principle. For the principle of Confidentiality, a complete set of criteria is comprised of all of the common criteria and all of the criteria applicable to the principle being reported on.

A list of the Criteria / Control Objectives which form the basis of this report have been provided in Appendix B: List of Criteria.

Common Criteria for Security and Confidentiality

The common criteria are organized into seven categories as described further below.

ORGANIZATION AND MANAGEMENT

Lexer Organization & Management
Lexer's organizational structure provides the framework within which its activities for achieving entity wide objectives are planned, executed, controlled, and monitored. The organization has established documented procedures to ensure those criteria relevant to how the organization is structured and the process that organization has implemented to manage and support people within its operating unit, are satisfied. Lexer operates under the general direction of its Board, and is managed day-to-day by ELT.

Job descriptions are in place and define roles and responsibilities, skills and knowledge requirements.

Lexer's organisational structure, reporting relationships, authorities and responsibilities are evaluated and reviewed at least annually by the ELT. Once approved by the ELT any changes are communicated to employees.

Lexer Security
Lexer has developed an organisation wide Information Security Management Framework aligned with the ISO/IEC 27000 family of security standards. Included in the framework are policies, standards and procedural documentation relating to security and confidentiality of information and information systems.

The Information Security Officer (ISO) has overall responsibility for Lexer's security framework. Information Security is a standing item on the agenda of the ELT meetings, which includes security initiatives, projects, reviewing open items and discussions around current and emerging threats occurring in the industry.

The ISO is responsible for reviewing Lexer's Information Security Policy on an annual basis, and for aligning the changes in policy to new business and technology requirements as they are identified. Changes to any of Lexer's policies and standards, including the Information Security Policy, are reviewed and approved by the ELT.

AWS provides managed security and security operations as part of the service it provides to Lexer, however these servers are out of scope for this report. Refer to the Controls at Subservice Organisations section below.

Human Resources

A Human Resources Policy forms part of the IT Policies and describes security measures that Lexer has in place for the Human Resources function.

The Human Resources Team defines policies and procedures for recruitment and termination of employment. The policies define terms and conditions of employment, requirements for information security awareness, education and training, termination or change of employment and pre-employment checks.

All policies, standards and procedures are documented and made available to personnel through Lexer's intranet, know.lexer.io.

Before being granted access to Restricted Information:

- The Human Resources Team performs background screening and requisite verification checks for the candidate/employee. The background checks are used to assess a candidate's education, training / qualifications, previous employment and experience as well as any criminal record. These checks are carried out in accordance with applicable local laws.
- The employee is required to sign an Employment Agreement with the Company which includes clauses for maintaining confidentiality and non-disclosure of information.
- The employee must read and acknowledge their understanding of Lexer's IT Policies
- The employee must read and acknowledge their understanding of Lexer's Employee Handbook
- The employee must complete Lexer's Security Awareness Training.

Following termination of employment (either by Lexer or the employee), the HR Team work with the employee's manager to ensure a separation checklist is followed and all tasks completed.

COMMUNICATION

Internal Communication

Lexer maintains communication with personnel using internal collaboration tools, knowledge databases and e-mail. The communication includes but is not limited to communication of Lexer's policies and procedures, corporate events, new initiatives, and awareness and training (including security awareness).

Changes and updates to Lexer policies and procedures, and implementation of changes on Lexer network and security devices are communicated to relevant Lexer personnel through internal collaboration tools.

Policies and procedures specific to Lexer's operations, including those for managing security and confidentiality, are made available to Lexer personnel through the company intranet, know.lexer.io.

Security Awareness training is provided to personnel at least annually, which provides them with an understanding and awareness of their responsibility and accountability for Lexer's information security and confidentiality matters. Training materials are developed jointly by the Information Security Officer, Chief Technology Officer and HR Manager, and maintained annually or more frequently as changes occur.

External Communication

Lexer utilizes agreements, its website and email to communicate to external customers, vendors, and other parties.

A service description is included on the website at www.lexer.io. Lexer's Master Services Agreement (or equivalent customer contract) clearly communicates to customers the functionality of the services provided, and the responsibilities of each party in relation to such services (this includes information on the boundaries that exist between Lexer's provision of the services, and a customer's use of the services). Links on the website include details about the Lexer service, its intended use and privacy policy.

Lexer's security webpage https://lexer.io/trust-and-compliance/ describes security measures that Lexer has in place, including network infrastructure and data security, privacy and availability.

An impact analysis is performed prior to contracting with any third party service provider in line with the Service Provider Security Policy. A non-disclosure agreement is signed by third-parties prior to confidential information being shared with those parties.

All non-disclosure agreements, and third party contracts, communicate Lexer's security commitments and required security obligations, terms, conditions, and responsibilities and are signed by authorised approvers and their approval signifies management agreement.

3. RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS

Risk Identification

Lexer generates information on information security risks from the following sources:

- Risk and threat modelling by the Information Security Officer and third-party contractors in relation to business assets
- Risk and threat modelling by internal business and software development teams during the development of new or updated product features.
- Regular penetration testing by third party specialists.
- Regular vulnerability assessments of the application.
- Alerting services providing real-time information on security trends and threats.
- Operational data and alerts from application and infrastructure log analysis.
- Ongoing monitoring of compliance activities and trends by the Information Security Officer and Chief Technology Officer
- Review of user logs showing system log in attempts and failures
- Subscription to relevant newsletters and attendance at relevant forums

Information security risks are managed through a number of processes:

Application level controls for risks that have been identified by risk and threat modelling, penetration or vulnerability testing, or bug bounties are managed using the normal "systems development lifecycle" workflow management and tracking tools, with defined fast track processes for high-risk vulnerabilities or bugs in production systems.

Infrastructure risks, including infrastructure patching and configuration, are managed as an integral part of operational management processes by the Infrastructure team, who are also responsible for infrastructure security monitoring.

Application security monitoring, including anomalous application behaviour detection and response, is managed by the Infrastructure teams.

Risk Management
Oversight of information security risk at a corporate level is undertaken by the ELT and is managed by the Information Security Officer. Information security is a standing item on the agenda of the ELT meetings, and the ELT considers key risks for which high level governance and management decisions are required.

Lexer has a formalised risk management process and maintains a Risk Register which tracks key risks to the organization, including information security risks. Risk assessments include a review of internal and external factors that threaten the achievement of business objectives. Mitigating controls are identified for all risks and risks with residual scores above the acceptable risk threshold have mitigating actions agreed that are then tracked by the Information Security team.

Controls Overview
Lexer has developed formal company-wide policies and procedures for meeting the requirements related to security and confidentiality. Policies are available via the company intranet to all personnel. The Information Security Policy includes:

- Human Resources Management
- Information Classification
- Physical Security
- IT Communications & Operations Management
- Network & Platform Security
- Access Management
- Service Provider Security
- System Acquisition, Development & Maintenance
- Cryptographic Control
- Acceptable Usage
- Information & IT Asset Inventory and Ownership
- Regulatory & IP Compliance
- Tidy & Secure Workplace
- Anti-Piracy
- Password & Authentication
- Backup
- Portable Device
- Remote Access & Mobile Working
- Security Breach & Weakness
- Monitoring

Separate policies and procedures are defined for Business Continuity and Disaster Recovery, which are tested on a periodic basis.

All policies are kept up to date, and reviewed and approved by the ELT on an annual basis, or more frequently as necessary (for example, based on an updated risk assessment).

4. MONITORING OF CONTROLS

Security
A security incident management process is employed to document incidents and resolutions. A root cause analysis may also be performed on security incidents, as deemed necessary. For high severity security incidents, regular status update meetings are held to discuss and monitor the status.

The Chief Technology Officer conducts at least quarterly compliance checks against the security policy and access control standards. This includes checks that quarterly user access reviews are performed for production systems and network access. Password settings for systems are also included in the review.

On an annual basis the Information Security Officer completes supplier reviews. This includes receiving compliance reporting from subservice organizations (i.e. SOC 2 reporting for AWS) and reviewing the reports for any issues. Review results are presented to the ELT for discussion and approval of the ongoing supplier relationship. Should any issues be identified they will be logged and assessed to determine the impact on the Lexer environment. All issues will be tracked through to successful resolution.

The Information Security Function performs an annual internal audit to review the design and operating effectiveness of internal controls. The results of these reviews are reported to the ELT with response plans developed in relation to material deficiencies.

Ongoing Monitoring
Automated Monitoring Systems: Lexer uses a wide variety of automated monitoring systems, which cover security, service performance and availability. Monitoring tools are implemented to detect and protect against external and internal threats. System performance including availability is also continuously monitored through a specific set of tools and control procedures.

Client Services: A dedicated Client Services team is in place to service customer requests and monitor customer feedback for performance, which makes its way back to the IT teams to action for resolution. External customers communicate with Client Services through live chat in the Lexer application and email.

5. LOGICAL AND PHYSICAL ACCESS CONTROL

Lexer has a defined and documented Access Management Policy that govern the processes for identification and authentication of authorised users, restriction of user access to authorised system components and prevention and detection of unauthorised system access.

Logical Access Path
All access to Lexer systems and applications requires authentication.

Engineers connect to the production environment hosted by AWS. A two-factor user authentication process is required at every logon as well as after the computer enters screen lock.

Lexer personnel access their code version control and change management systems by connecting to the Lexer network using their Lexer user ID and password.

Password Security
Password policies are in place across production environments per the password requirements stipulated in the security policy.

Separate security policies are implemented across company workstations (desktops/laptops) and servers within the Lexer network. Access to environments holding restricted information is controlled via multi-factor authentication.

Unattended workstations are locked using a password protected screen saver after a defined period of inactivity.

Identity & Access Management
User Account Management: Access to in-scope systems is granted on a need to know and least privilege basis. Role-based access privileges are enforced by access control systems, where configurable. General access to in-scope systems is authorised by both the Information Security Officer and the Chief Technology Officer. The initial setting of, and subsequent changes to, access privileges is approved by the Chief Technology Officer. Revocation of access for terminated personnel is performed in a timely manner via a process managed by the HR Team.

User Access Review: A periodic review of user access rights is completed by the Chief Technology Officer to ensure the level of access is appropriate. Any access, which is deemed to be no longer required, is identified and disabled.

Customer Access Management: Administrative access to the Customer Portal is provisioned for an authorised customer representative following execution of a client agreement. The customer administrator is responsible for managing and monitoring access to the customer portal, including optional enforcement of dual factor authentication. All customer accounts and administrative access to the Customer Portal will be revoked following termination of a customer agreement. The customer portal enforces minimum required password settings including the disabling of user accounts after a limited number of unsuccessful logons for a specified duration.

Physical Security
Production Environment Physical Access: All restricted data is stored at a Lexer Red Zone facility, which is hosted within Amazon Web Services (AWS). Controls for ensuring physical and environmental security are implemented and managed by AWS and are therefore out of scope for this report.

The Physical Security Policy sets out the minimum security standards for an acceptable Red Zone facility. Lexer relies on third party attestation reports provided by AWS for ascertaining the design and operating effectiveness of physical and environmental security controls.

Corporate Environment Physical Access: Restricted Information is not stored at any Lexer corporate office.

Network Security & Vulnerability Management
Periodic internal and third-party security reviews, vulnerability assessments and penetration tests are completed. Vulnerabilities identified are logged, reviewed to determine expected remediation timeframes, and tracked through to resolution with reporting to the ELT on a quarterly basis.

Firewall rules limit incoming connections and define the types of activities and service requests that can be performed from external connections. Intrusion detection and prevention systems (IDS/IPS) are also utilised to analyse and report network events. Automated alerts from IDS/IPS are logged and resolved in a timely manner.

6. SYSTEM OPERATIONS

Backups
Lexer has a Data Management policy that governs the performance of data backups and data restoration. AWS services are utilised to maintain a 7-day rolling backup of all Restricted Information. Alerts for failed backups are raised for resolution via log monitoring processes.

Restorability and integrity of backups is periodically assessed and provides confirmation of Disaster Recovery capabilities.

Patch Management
An immutable infrastructure is in place comprised of immutable components that are replaced at each redeployment, rather than updated. Controls for ensuring patching of environments are implemented and managed by AWS and are therefore out of scope for this report.

Security Incident Management
Security Incidents: The Lexer team follows documented incident response plans for specific scenarios, which could impact security. Security incidents which arise are notified to the Lexer Information Security Officer (ISO). The ISO is appointed as manager of the incident management process and will involve adequate resources to resolve the incident as quickly as possible. Incidents are recorded in the Incident Management Register and if relevant, and not customer sensitive, the status page in the Lexer platform is also updated to communicate any relevant breaches, incidents and threats.

Post Incident Reviews: If the incident was categorized as a major security incident, the Information Security Officer will conduct a Post Incident Review. The main purpose of the Post Incident Review is to evaluate the response to an incident and derive learnings from it. Any major security incidents are raised and discussed with the ELT.

Audit Logging & Monitoring
Logging and monitoring software is used to collect data from in-scope systems to monitor system performance, potential security threats and vulnerabilities, and resource utilization; and to detect unusual system activity or service requests. Logs are reviewed as required to investigate issues and also as part of a formalised weekly health check. Any issued identified via audit log review are logged and tracked through to resolution.

Anti-Virus Software
Antivirus Software is installed across in–scope systems which are commonly susceptible to computer virus, malicious code, and unauthorized software.

CHANGE MANAGEMENT

Overview
Lexer follows an agile development process that includes being able to iteratively roll out functional and non-functional changes while targeting both high quality and high applicability. Management has documented system acquisition, change and release management policies and processes to communicate management's expectations in regards to performing changes to the production environment. These policies and processes apply to all changes to the production environment and convey the change control process including assessing the impact of changes, testing, rollback procedures, approval requirements, and change communication to relevant stakeholders. In addition, change management personnel involved in the change management process agree on their meeting cadence (usually this is daily during a stand up meeting) to discuss the prioritization of current and proposed changes.

Change Request Initiation And Control
Infrastructure Changes: Infrastructure changes (such as new servers, server patches, firewall rule changes, configuration changes, global changes to the hypervisor, network or storage components etc.) are raised through the Asana task management system. Requests are fielded by the Information Technology Leadership team (Chief Technology Officer and Team Leads) who will form an implementation plan.

System Changes: The Information Technology Leadership team have created a Global Product Roadmap which details the projects expected to be undertaken for the next 6-12 months and provides visibility to the business around what is planned. The projects are then placed onto a priority listing, which forms the basis of upcoming work. The Leadership team meet regularly to assess upcoming work for scope, resourcing and effort required, and reprioritise if required. The roadmap is reviewed periodically and posted on the entity intranet. Planned developments impacting external users are communicated as required.

When changes are identified, the change requestor creates a ticket in the Asana task management system to track the change through implementation to ensure the change control procedures are followed. Relevant stakeholders are notified when a change is identified and kept informed of all changes through the task management system. Change stakeholders populate key fields on the ticket, including the change request

description, desired outcomes, and importance to the business.

For larger projects, the project details are defined within a project poster, which includes details of the impact to users, problem being solved and the solution design. Potential risks, including impacts on security, privacy, access and performance, are considered as a part of the project planning process and regularly during the project lifecycle. Chief Technology Officer approval and sign off is required for all larger projects.

Impact Assessment
Developers work in a separate developer environment and merge their changes once all local tests are passed. They will initiate a pull request within the Software Development tool used for version control, which requires another developer to perform a code review. Once the code review is completed, the change is integrated into a staging environment. Further regression and user acceptance testing is performed. Once completed the release is merged into a production like environment (live-stage) to ensure stability. Before the change is released, it is reviewed by a member of the Information Technology Leadership Team to assess impact and risks and any communication required. Once assessed, the change is released into Production. Access to the different environment utilised in the change management process is logically restricted to provide segregation.

Control of Changes & Monitoring
Lexer uses continuous integration software to manage, track and provide control over versions of source code for releases. Development personnel check out source code and store it locally on their computer. Once the team are ready to update the code repository, they check the code back in and it is assigned a different version number. This allows users to roll back code to previous versions when necessary. The ability to merge and pull down source code during development from the version control software is restricted to relevant Information Technology team members.

The release of compiled builds is managed by a release management system. Before a migration to production can occur a manual approval step by a designated approver is enforced. Key activities which occur during the change and release process are automatically logged which includes details about the change, timestamp and user information. Teams are also notified automatically of key changes, which occur to their project through the collaboration messaging system, which is integrated with the release management software.

The Product Management Team works with Development Teams to schedule releases and confirm all testing, QA and documentation review for the release has been performed.

Emergency Changes & Rollbacks
Multiple historic release versions are retained and mapped in the Continuous Integration application. This, along with the version control tool, allows for any changes or releases, which cause unexpected behaviour to be efficiently rolled back to the last, stable release.

Additional Criteria for Confidentiality

1. DATA CLASSIFICATION AND DATA ACCESS CONTROL

Lexer assets and information are documented in the Asset and Risk Register and the asset value classified as High/Medium/Low, along with the risk probability classified as Certain/Likely/Possible/Unlikely/Rare. The Information Security Officer is responsible for the classification of the assets and the requisite level of protection. The classification enables personnel to determine what types of information can be disclosed, as well as the sensitivity of the information.

Personnel requesting access to Restricted Information as part of their work are required to sign a Red Zone Access Approval form, which is approved by the Information Security Officer and the Chief Technology Officer.

Personnel connecting to the Production environment network require mobile phone two factor authentication. There are separate environments for development, testing, staging and production. Production data is housed only in the Production environment.

Lexer performs quarterly user access reviews. During the review, the Chief Technology Officer reviews user accounts in order to ensure that all access is appropriate and has been approved. If any account is found to be violating Lexer's Access Management Policy, the respective accounts are disabled.

2. DATA ENCRYPTION

Web sessions are encrypted between the customer's browser and Lexer's servers using industry-standard encryption. Communication between Lexer's data centre environments is over encrypted VPNs. During storage all production data is encrypted using industry-standard encryption.

Restricted Information is encrypted in transit and at rest. Hardware-based full disk encryption is enabled for all staff workstations as part of the initial setup.

The Cryptographic Control Policy specifies the expected levels of cryptographic control.

3. CONFIDENTIALITY ENABLERS

The Information Security Officer is responsible for changes to confidentiality practices and commitments, which are communicated to relevant internal and external stakeholders as required.

Lexer Security Policies and acceptable standards as per the employee handbook are communicated to personnel when joining. With the acceptance of the employment offer, the employee acknowledges that they will abide by the policies communicated by the HR Team. All new hires undergo induction within the first month of employment which includes introductory sessions from the Information Security Officer and Chief Technology Officer around information security and its importance to Lexer.

Lexer ensures that it has applicable clauses relating to confidentiality and non-disclosure in service agreements with vendors, as well as in its agreements with its Customers.

As part of on-boarding a Customer, Lexer performs a gap analysis between client confidentiality requirements and internal policies. Client requirements which a more onerous than existing Lexer policy requirements are reviewed for incorporation into Lexer Policy or logged for management on an as needed basis.

Lexer disposes of Customer data in accordance with requirements of the Customer contract being terminated.

The entity creates test data using data masking software that replaces confidential information with test information prior to the creation of test databases; no real customer data is allowed to be used for testing / development without proper management authorisation.

Significant Events and conditions; other than transactions

If significant events and conditions arise, Lexer has Disaster Recovery Plans designed to ensure the systems continue to provide customers with the services covered by the report.

Controls at Subservice Organisations

Lexer uses AWS as a subservice organisations to provide services, which form part of the Lexer Identify service to be used by Lexer's customers, including: Identity and Access Management (IAM), cloud computing (EC2), Elastic Block Storage (EBS) and electronic storage (S3).

The description, Section V, includes controls and related control objectives of Lexer as well as the control objectives and related controls of the service organisations providing the aforementioned services. Controls of subservice organisations providing the aforementioned services have been clearly identified within the description for the benefit of Lexer's Customers, however were not subject to audit by our independent Auditor as outlined in their report in Section III. Where Lexer has established monitoring controls over the operating effectiveness of controls at subservice organisations these have been included within the controls examined.

As the controls related to the following Control Objectives are fully outsourced to AWS the following Control Objectives have been carved-out of scope:

- CC5.5 - Physical access to facilities housing the system (for example, data centres, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and confidentiality.

Lexer has an established monitoring program over controls which have been outsourced to subservice organisations. Assessment of these activities has been performed in relation to Control Objective "CC4.0 - Common Criteria Related to Monitoring of Controls".

Complementary Customer Control Considerations

The controls described in this document cover only a portion of the overall internal controls for each customer of Lexer. Achievement of each of the control objectives set out in Appendix B may be dependent on controls performed by Lexer customers as well as controls performed by Lexer. Therefore, each customer's internal controls should be evaluated in conjunction with the controls and testing results summarised in Section VI of this report.

This section highlights customer internal control responsibilities that Lexer has considered in developing the list of controls described in this report. Customers should evaluate their own systems of internal control to determine if the following controls, at a minimum, are in place. This list does not purport to be and is not a complete listing of the control activities, which provide a basis for the assertions underlying customer financial statements and control environment, with respect to the scope of this audit.

Lexer customers are responsible for Customer Portal user access management for all their personnel. This includes:

- ensuring that access is granted with appropriate data and functional access and revoked in a timely manner.
- reviewing the access rights assigned to their personnel within the Customer Portal.
- review of audit logs to identify potential security incidents.

SECTION VI: CONTROL OBJECTIVES, RELATED CONTROLS AND RESULTS FROM PWC'S TESTS OF DESIGN EFFECTIVENESS AND IMPLEMENTATION

Introduction

The following description of control objectives and control procedures is applicable to the CCH Integrator Service as at 13 December 2018. Each control objective has been specified by Lexer Management and is followed by the corresponding control procedures that have been agreed by Lexer Management. Included as part of the description of the control procedures is a summary of exceptions noted as part of the test procedures performed by PricewaterhouseCoopers.

Control ID	Control Procedure	PwC Design and Implementation Test Result
CC1.0 - Common Criteria Related to Organization and Management		
CC1.1 - The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security and confidentiality.		
CN01	Lexer's organisational structure, reporting lines / relationships, authorities and responsibilities are evaluated and reviewed at least annually by the ELT; changes are communicated to personnel.	No Exceptions Noted
CN02	Job descriptions are in place and communicated to define roles and responsibilities, skills, knowledge levels and required competence across staff levels with the technical tools and knowledge resources required to perform assigned tasks provided.	No Exceptions Noted
CC1.2 - Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security and confidentiality		
CN01	Lexer's organisational structure, reporting lines / relationships, authorities and responsibilities are evaluated and reviewed at least annually by the ELT; changes are communicated to personnel.	No Exceptions Noted
CN02	Job descriptions are in place and communicated to define roles and responsibilities, skills, knowledge levels and required competence across staff levels with the technical tools and knowledge resources required to perform assigned tasks provided.	No Exceptions Noted
CC1.3 - The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and confidentiality and provides resources necessary for personnel to fulfil their responsibilities.		
CN02	Job descriptions are in place and communicated to define roles and responsibilities, skills, knowledge levels and required competence across staff levels with the technical tools and knowledge resources required to perform assigned tasks provided.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CN06	The human resources team performs background checks as well as employee experience / training evaluations for all candidates as part of the new hire process.	No Exceptions Noted
CN07	Information security and awareness training is conducted for new hires and at least annually for Lexer personnel with Red Zone access, to communicate security and confidentiality obligations.	No Exceptions Noted
CC1.4 - The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security and confidentiality.		
CN04	Changes to Lexer's policies and standards are reviewed and approved by the ELT before being communicated to personnel; revised policies are then available on the intranet.	No Exceptions Noted
CN05	The Human Resources Policy defines terms and conditions of employment, requirements for information security awareness, education and training, termination or change of employment and pre-employment checks.	No Exceptions Noted
CN06	The human resources team performs background checks as well as employee experience / training evaluations for all candidates as part of the new hire process.	No Exceptions Noted
CN08	Upon execution of their Employment Agreement, new hires receive an employee handbook and have access to Lexer's online knowledgebox where documents defining personnel's responsibilities for information security can be located. New hires must read and acknowledge their understanding of Lexer's security policy and team handbook.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CC2.0 - Common Criteria Related to Communications		
CC2.1 - Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.		
CN08	Upon execution of their Employment Agreement, new hires receive an employee handbook and have access to Lexer's online knowledgebox where documents defining personnel's responsibilities for information security can be located. New hires must read and acknowledge their understanding of Lexer's security policy and team handbook.	No Exceptions Noted
CN09	A description of Lexer's service which defines its boundaries, relevant key system components, purpose and design of the system is available to internal and external personnel.	No Exceptions Noted
CN10	Lexer's security commitments (including security obligations, terms, conditions and responsibilities) are documented, along with the responsibilities of external users, in third party contracts and non-disclosure agreements.	No Exceptions Noted
CC2.2 - The entity's security and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.		
CN03	IT Security Policies are documented and reviewed at least annually by the ELT.	No Exceptions Noted
CN04	Changes to Lexer's policies and standards are reviewed and approved by the ELT before being communicated to personnel; revised policies are then available on the intranet.	No Exceptions Noted
CN07	Information security and awareness training is conducted for new hires and at least annually for Lexer personnel with Red Zone access, to communicate security and confidentiality obligations.	No Exceptions Noted
CN08	Upon execution of their Employment Agreement, new hires receive an employee handbook and have access to Lexer's online knowledgebox where documents defining personnel's responsibilities for information security can be located. New hires must read and acknowledge their understanding of Lexer's security policy and team handbook.	No Exceptions Noted
CN09	A description of Lexer's service which defines its boundaries, relevant key system components, purpose and design of the system is available to internal and external personnel.	No Exceptions Noted
CN10	Lexer's security commitments (including security obligations, terms, conditions and responsibilities) are documented, along with the responsibilities of external users, in third party contracts and non-disclosure agreements.	No Exceptions Noted
CC2.3 - The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.		
CN03	IT Security Policies are documented and reviewed at least annually by the ELT.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CN04	Changes to Lexer's policies and standards are reviewed and approved by the ELT before being communicated to personnel; revised policies are then available on the intranet.	No Exceptions Noted
CN07	Information security and awareness training is conducted for new hires and at least annually for Lexer personnel with Red Zone access, to communicate security and confidentiality obligations.	No Exceptions Noted
CN08	Upon execution of their Employment Agreement, new hires receive an employee handbook and have access to Lexer's online knowledgebox where documents defining personnel's responsibilities for information security can be located. New hires must read and acknowledge their understanding of Lexer's security policy and team handbook.	No Exceptions Noted
CN09	A description of Lexer's service which defines its boundaries, relevant key system components, purpose and design of the system is available to internal and external personnel.	No Exceptions Noted
CN10	Lexer's security commitments (including security obligations, terms, conditions and responsibilities) are documented, along with the responsibilities of external users, in third party contracts and non-disclosure agreements.	No Exceptions Noted
CN13	The Information Security Function performs periodic internal assessment to review the design and operating effectiveness of internal controls related to Security and Confidentiality. The results of these reviews are reported to the ELT with response plans developed in relation to material deficiencies.	No Exceptions Noted
CN31	The Lexer status page is kept up to date to inform external users of relevant breaches, incidents and threats.	No Exceptions Noted
CC2.4 - Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and confidentiality of the system, is provided to personnel to carry out their responsibilities.		
CN03	IT Security Policies are documented and reviewed at least annually by the ELT.	No Exceptions Noted
CN04	Changes to Lexer's policies and standards are reviewed and approved by the ELT before being communicated to personnel; revised policies are then available on the intranet.	No Exceptions Noted
CN07	Information security and awareness training is conducted for new hires and at least annually for Lexer personnel with Red Zone access, to communicate security and confidentiality obligations.	No Exceptions Noted
CN13	The Information Security Function performs periodic internal assessment to review the design and operating effectiveness of internal controls related to Security and Confidentiality. The results of these reviews are reported to the ELT with response plans developed in relation to material deficiencies.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CN32	The ISO reviews the design and operational of outsourced controls via third party attestation reports for major subservice providers to ensure they meet organisational Security and Confidentiality requirements; Issues are logged and tracked though to resolution.	No Exceptions Noted
CC2.5 - Internal and external users have been provided with information on how to report security and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.		
CN03	IT Security Policies are documented and reviewed at least annually by the ELT.	No Exceptions Noted
CN04	Changes to Lexer's policies and standards are reviewed and approved by the ELT before being communicated to personnel; revised policies are then available on the intranet.	No Exceptions Noted
CN07	Information security and awareness training is conducted for new hires and at least annually for Lexer personnel with Red Zone access, to communicate security and confidentiality obligations.	No Exceptions Noted
CN10	Lexer's security commitments (including security obligations, terms, conditions and responsibilities) are documented, along with the responsibilities of external users, in third party contracts and non-disclosure agreements.	No Exceptions Noted
CN30	Security incidents are logged and responded to with constant effort until resolved.	No Exceptions Noted
CN31	The Lexer status page is kept up to date to inform external users of relevant breaches, incidents and threats.	No Exceptions Noted
CC2.6 - System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and confidentiality are communicated to those users in a timely manner.		
CN01	Lexer's organisational structure, reporting lines / relationships, authorities and responsibilities are evaluated and reviewed at least annually by the ELT; changes are communicated to personnel.	No Exceptions Noted
CN02	Job descriptions are in place and communicated to define roles and responsibilities, skills, knowledge levels and required competence across staff levels with the technical tools and knowledge resources required to perform assigned tasks provided.	No Exceptions Noted
CN03	IT Security Policies are documented and reviewed at least annually by the ELT.	No Exceptions Noted
CN04	Changes to Lexer's policies and standards are reviewed and approved by the ELT before being communicated to personnel; revised policies are then available on the intranet.	No Exceptions Noted
CN31	The Lexer status page is kept up to date to inform external users of relevant breaches, incidents and threats.	No Exceptions Noted
CN39	Project team members collaborate regularly during the project lifecycle to determine the potential effect of proposed changes on security and confidentiality commitments and system requirements.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CN40	A product roadmap that describes upcoming product developments is formalised, reviewed periodically by the ISMS Executive Committee and posted on the intranet. Developments impacting external users are communicated on a monthly basis, and when required.	No Exceptions Noted
CN41	Changes are initiated, logged, developed, assessed, tested, peer-reviewed by Management with external parties notified where applicable.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CC3.0 - Common Criteria Related to Risk Management and Design and Implementation of Controls		
CC3.1 - The entity: (1) identifies potential threats that could impair system security and confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyses the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.		
CN11	Lexer has a formalised Risk Management process which maintains a Global Risk Register tracking key risks to the organization, including information security risks. The Register is owned by the Information Security Officer with oversight by the ELT.	No Exceptions Noted
CN12	During risk assessments, management identifies changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and updates the potential threats to system objectives. In response to the identification of such risks, management updates its policies, procedures, processes, and controls, as needed.	No Exceptions Noted
CN14	Lexer personnel responsible for the organisation's ability to meet its security and confidentiality requirements subscribe to newsletters and attend relevant forums to inform them of changes to the environmental, regulatory, technological landscape.	No Exceptions Noted
CN15	Vulnerability assessments and penetration tests are completed by Lexer's development team and third party vendors to identify weaknesses in system operation that would impair system security and confidentiality commitments.	No Exceptions Noted
CN16	Vulnerabilities identified during risk and vulnerability assessments are logged and tracked through to resolution. All vulnerabilities identified are reviewed and assessed to determine the expected remediation timeline, dependent on the assigned risk rating.	No Exceptions Noted
CN26	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems; to monitor system performance, potential security threats and vulnerabilities, and resource utilization; and to detect unusual system activity or service requests. Logs are reviewed on a periodic basis with any issues identified logged and tracked through to resolution.	No Exceptions Noted
CN32	The ISO reviews the design and operational of outsourced controls via third party attestation reports for major subservice providers to ensure they meet organisational Security and Confidentiality requirements; Issues are logged and tracked though to resolution.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CC3.2 - The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.		
CN03	IT Security Policies are documented and reviewed at least annually by the ELT.	No Exceptions Noted
CN04	Changes to Lexer's policies and standards are reviewed and approved by the ELT before being communicated to personnel; revised policies are then available on the intranet.	No Exceptions Noted
CN11	Lexer has a formalised Risk Management process which maintains a Global Risk Register tracking key risks to the organization, including information security risks. The Register is owned by the Information Security Officer with oversight by the ELT.	No Exceptions Noted
CN12	During risk assessments, management identifies changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and updates the potential threats to system objectives. In response to the identification of such risks, management updates its policies, procedures, processes, and controls, as needed.	No Exceptions Noted
CN13	The Information Security Function performs periodic internal assessment to review the design and operating effectiveness of internal controls related to Security and Confidentiality. The results of these reviews are reported to the ELT with response plans developed in relation to material deficiencies.	No Exceptions Noted
CN14	Lexer personnel responsible for the organisation's ability to meet its security and confidentiality requirements subscribe to newsletters and attend relevant forums to inform them of changes to the environmental, regulatory, technological landscape.	No Exceptions Noted
CN15	Vulnerability assessments and penetration tests are completed by Lexer's development team and third party vendors to identify weaknesses in system operation that would impair system security and confidentiality commitments.	No Exceptions Noted
CN16	Vulnerabilities identified during risk and vulnerability assessments are logged and tracked through to resolution. All vulnerabilities identified are reviewed and assessed to determine the expected remediation timeline, dependent on the assigned risk rating.	No Exceptions Noted
CN33	Formalised Business Continuity and Disaster Recovery plans, which include details on disaster recovery and business recovery requirements and procedures, are in place and tested on a periodic basis.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CC4.0 - Common Criteria Related to Monitoring of Controls		
CC4.1 - The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and confidentiality, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.		
CN13	The Information Security Function performs periodic internal assessment to review the design and operating effectiveness of internal controls related to Security and Confidentiality. The results of these reviews are reported to the ELT with response plans developed in relation to material deficiencies.	No Exceptions Noted
CN14	Lexer personnel responsible for the organisation's ability to meet its security and confidentiality requirements subscribe to newsletters and attend relevant forums to inform them of changes to the environmental, regulatory, technological landscape.	No Exceptions Noted
CN15	Vulnerability assessments and penetration tests are completed by Lexer's development team and third party vendors to identify weaknesses in system operation that would impair system security and confidentiality commitments.	No Exceptions Noted
CN16	Vulnerabilities identified during risk and vulnerability assessments are logged and tracked through to resolution. All vulnerabilities identified are reviewed and assessed to determine the expected remediation timeline, dependent on the assigned risk rating.	No Exceptions Noted
CN32	The ISO reviews the design and operational of outsourced controls via third party attestation reports for major subservice providers to ensure they meet organisational Security and Confidentiality requirements; Issues are logged and tracked though to resolution.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CC5.0 - Common Criteria Related to Logical and Physical Access Controls		
CC5.1 - Logical access security software, infrastructure, and architectures have been implemented to support: (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and confidentiality.		
CN03	IT Security Policies are documented and reviewed at least annually by the ELT.	No Exceptions Noted
CN15	Vulnerability assessments and penetration tests are completed by Lexer's development team and third party vendors to identify weaknesses in system operation that would impair system security and confidentiality commitments.	No Exceptions Noted
CN16	Vulnerabilities identified during risk and vulnerability assessments are logged and tracked through to resolution. All vulnerabilities identified are reviewed and assessed to determine the expected remediation timeline, dependent on the assigned risk rating.	No Exceptions Noted
CN17	Lexer has defined and documented Access Control Policies that governed the processes for identification and authentication of authorised users, restriction of user access to authorised system components and prevention and detection of unauthorised system access.	No Exceptions Noted
CN18	Formal role-based access controls are enforced by the access control systems, where configurable.	No Exceptions Noted
CN19	Access to Red Zone, Code Versioning and Release Management Systems is only provisioned to Lexer personnel following authorisation by Management.	No Exceptions Noted
CN20	Administrative access, for management of Customer personnel user access to the Customer Portal, is only provisioned to the Authorised Customer Representative following execution of a client agreement.	No Exceptions Noted
CN21	Code Versioning and Release Management Systems and the Customer Portal enforce minimum required password settings in accordance with policy, where configurable.	No Exceptions Noted
CN22	Red Zone IT Systems enforce minimum required password settings, multi-factor authentication.	No Exceptions Noted
CN23	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are revoked on a timely basis following notification from HR Team regarding termination of employment.	No Exceptions Noted
CN24	Administrative access, for management of Customer personnel user access to the Customer Portal, is revoked following termination of a client agreement.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CN25	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are reviewed on at least quarterly to confirm access provisioned remains commensurate with business requirements	No Exceptions Noted
CN28	Intrusion detection and prevention systems are utilised to analyse and report network events and are configured to send automated alerts which are then addressed in a timely manner.	No Exceptions Noted
CN43	Segregated development, test and production environments are in place with access to these environments logically restricted.	No Exceptions Noted
CC5.2 - New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
CN17	Lexer has defined and documented Access Control Policies that governed the processes for identification and authentication of authorised users, restriction of user access to authorised system components and prevention and detection of unauthorised system access.	No Exceptions Noted
CN18	Formal role-based access controls are enforced by the access control systems, where configurable.	No Exceptions Noted
CN19	Access to Red Zone, Code Versioning and Release Management Systems is only provisioned to Lexer personnel following authorisation by Management.	No Exceptions Noted
CN20	Administrative access, for management of Customer personnel user access to the Customer Portal, is only provisioned to the Authorised Customer Representative following execution of a client agreement.	No Exceptions Noted
CN21	Code Versioning and Release Management Systems and the Customer Portal enforce minimum required password settings in accordance with policy, where configurable.	No Exceptions Noted
CN22	Red Zone IT Systems enforce minimum required password settings, multi-factor authentication.	No Exceptions Noted
CN23	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are revoked on a timely basis following notification from HR Team regarding termination of employment.	No Exceptions Noted
CN24	Administrative access, for management of Customer personnel user access to the Customer Portal, is revoked following termination of a client agreement.	No Exceptions Noted
CN25	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are reviewed on at least quarterly to confirm access provisioned remains commensurate with business requirements	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CC5.3 - Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and confidentiality.		
CN05	The Human Resources Policy defines terms and conditions of employment, requirements for information security awareness, education and training, termination or change of employment and pre-employment checks.	No Exceptions Noted
CN18	Formal role-based access controls are enforced by the access control systems, where configurable.	No Exceptions Noted
CN19	Access to Red Zone, Code Versioning and Release Management Systems is only provisioned to Lexer personnel following authorisation by Management.	No Exceptions Noted
CN20	Administrative access, for management of Customer personnel user access to the Customer Portal, is only provisioned to the Authorised Customer Representative following execution of a client agreement.	No Exceptions Noted
CN21	Code Versioning and Release Management Systems and the Customer Portal enforce minimum required password settings in accordance with policy, where configurable.	No Exceptions Noted
CN22	Red Zone IT Systems enforce minimum required password settings, multi-factor authentication.	No Exceptions Noted
CN23	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are revoked on a timely basis following notification from HR Team regarding termination of employment.	No Exceptions Noted
CN24	Administrative access, for management of Customer personnel user access to the Customer Portal, is revoked following termination of a client agreement.	No Exceptions Noted
CN25	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are reviewed on at least quarterly to confirm access provisioned remains commensurate with business requirements	No Exceptions Noted
CN29	Data (including backups, storage for workstations and laptops) is encrypted at rest and for all public networks transfers, including web communication sessions.	No Exceptions Noted
CN43	Segregated development, test and production environments are in place with access to these environments logically restricted.	No Exceptions Noted
CC5.4 - Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and confidentiality.		
CN05	The Human Resources Policy defines terms and conditions of employment, requirements for information security awareness, education and training, termination or change of employment and pre-employment checks.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CN18	Formal role-based access controls are enforced by the access control systems, where configurable.	No Exceptions Noted
CN19	Access to Red Zone, Code Versioning and Release Management Systems is only provisioned to Lexer personnel following authorisation by Management.	No Exceptions Noted
CN20	Administrative access, for management of Customer personnel user access to the Customer Portal, is only provisioned to the Authorised Customer Representative following execution of a client agreement.	No Exceptions Noted
CN21	Code Versioning and Release Management Systems and the Customer Portal enforce minimum required password settings in accordance with policy, where configurable.	No Exceptions Noted
CN22	Red Zone IT Systems enforce minimum required password settings, multi-factor authentication.	No Exceptions Noted
CN23	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are revoked on a timely basis following notification from HR Team regarding termination of employment.	No Exceptions Noted
CN24	Administrative access, for management of Customer personnel user access to the Customer Portal, is revoked following termination of a client agreement.	No Exceptions Noted
CN25	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are reviewed on at least quarterly to confirm access provisioned remains commensurate with business requirements	No Exceptions Noted
CN29	Data (including backups, storage for workstations and laptops) is encrypted at rest and for all public networks transfers, including web communication sessions.	No Exceptions Noted
CN43	Segregated development, test and production environments are in place with access to these environments logically restricted.	No Exceptions Noted
CC5.6 - Logical access security measures have been implemented to protect against security and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.		
CN15	Vulnerability assessments and penetration tests are completed by Lexer's development team and third party vendors to identify weaknesses in system operation that would impair system security and confidentiality commitments.	No Exceptions Noted
CN16	Vulnerabilities identified during risk and vulnerability assessments are logged and tracked through to resolution. All vulnerabilities identified are reviewed and assessed to determine the expected remediation timeline, dependent on the assigned risk rating.	No Exceptions Noted
CN27	Firewalls limit incoming connections based on defined rules which are reviewed periodically or after significant changes to the environment.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CN28	Intrusion detection and prevention systems are utilised to analyse and report network events and are configured to send automated alerts which are then addressed in a timely manner.	No Exceptions Noted
CN29	Data (including backups, storage for workstations and laptops) is encrypted at rest and for all public networks transfers, including web communication sessions.	No Exceptions Noted
CN35	Personal information (both public and sensitive information) involved in business processes, systems, and third-party involvement is clearly identified and classified based on severity and risk within data management policies and procedures.	No Exceptions Noted
CC5.7 - The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and confidentiality.		
CN27	Firewalls limit incoming connections based on defined rules which are reviewed periodically or after significant changes to the environment.	No Exceptions Noted
CN28	Intrusion detection and prevention systems are utilised to analyse and report network events and are configured to send automated alerts which are then addressed in a timely manner.	No Exceptions Noted
CN29	Data (including backups, storage for workstations and laptops) is encrypted at rest and for all public networks transfers, including web communication sessions.	No Exceptions Noted
CN35	Personal information (both public and sensitive information) involved in business processes, systems, and third-party involvement is clearly identified and classified based on severity and risk within data management policies and procedures.	No Exceptions Noted
CC5.8 - Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security and confidentiality.		
CN07	Information security and awareness training is conducted for new hires and at least annually for Lexer personnel with Red Zone access, to communicate security and confidentiality obligations.	No Exceptions Noted
CN19	Access to Red Zone, Code Versioning and Release Management Systems is only provisioned to Lexer personnel following authorisation by Management.	No Exceptions Noted
CN20	Administrative access, for management of Customer personnel user access to the Customer Portal, is only provisioned to the Authorised Customer Representative following execution of a client agreement.	No Exceptions Noted
CN23	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are revoked on a timely basis following notification from HR Team regarding termination of employment.	No Exceptions Noted
CN24	Administrative access, for management of Customer personnel user access to the Customer Portal, is revoked following termination of a client agreement.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CN25	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are reviewed on at least quarterly to confirm access provisioned remains commensurate with business requirements	No Exceptions Noted
CN26	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems; to monitor system performance, potential security threats and vulnerabilities, and resource utilization; and to detect unusual system activity or service requests. Logs are reviewed on a periodic basis with any issues identified logged and tracked through to resolution.	No Exceptions Noted
CN28	Intrusion detection and prevention systems are utilised to analyse and report network events and are configured to send automated alerts which are then addressed in a timely manner.	No Exceptions Noted
CN48	Antivirus Software is installed across in–scope systems which are commonly susceptible to computer virus, malicious code, and unauthorized software.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CC6.0 - Common Criteria Related to System Operations		
CC6.1 - Vulnerabilities of system components to security and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security and confidentiality.		
CN11	Lexer has a formalised Risk Management process which maintains a Global Risk Register tracking key risks to the organization, including information security risks. The Register is owned by the Information Security Officer with oversight by the ELT.	No Exceptions Noted
CN12	During risk assessments, management identifies changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and updates the potential threats to system objectives. In response to the identification of such risks, management updates its policies, procedures, processes, and controls, as needed.	No Exceptions Noted
CN15	Vulnerability assessments and penetration tests are completed by Lexer's development team and third party vendors to identify weaknesses in system operation that would impair system security and confidentiality commitments.	No Exceptions Noted
CN16	Vulnerabilities identified during risk and vulnerability assessments are logged and tracked through to resolution. All vulnerabilities identified are reviewed and assessed to determine the expected remediation timeline, dependent on the assigned risk rating.	No Exceptions Noted
CN26	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems; to monitor system performance, potential security threats and vulnerabilities, and resource utilization; and to detect unusual system activity or service requests. Logs are reviewed on a periodic basis with any issues identified logged and tracked through to resolution.	No Exceptions Noted
CN27	Firewalls limit incoming connections based on defined rules which are reviewed periodically or after significant changes to the environment.	No Exceptions Noted
CN28	Intrusion detection and prevention systems are utilised to analyse and report network events and are configured to send automated alerts which are then addressed in a timely manner.	No Exceptions Noted
CN34	Lexer has defined and documented Data Management policies that govern the performance of data backups and data restoration.	No Exceptions Noted
CN36	Automated backup systems are deployed to perform scheduled backups of production data and systems at predefined intervals; Notification for failed backups are automatically generated and resolved via the incident management process.	No Exceptions Noted
CN37	Restorability and integrity of backup files is validated on a periodical basis.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CC6.2 - Security and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.		
CN15	Vulnerability assessments and penetration tests are completed by Lexer's development team and third party vendors to identify weaknesses in system operation that would impair system security and confidentiality commitments.	No Exceptions Noted
CN16	Vulnerabilities identified during risk and vulnerability assessments are logged and tracked through to resolution. All vulnerabilities identified are reviewed and assessed to determine the expected remediation timeline, dependent on the assigned risk rating.	No Exceptions Noted
CN26	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems; to monitor system performance, potential security threats and vulnerabilities, and resource utilization; and to detect unusual system activity or service requests. Logs are reviewed on a periodic basis with any issues identified logged and tracked through to resolution.	No Exceptions Noted
CN30	Security incidents are logged and responded to with constant effort until resolved.	No Exceptions Noted
CN31	The Lexer status page is kept up to date to inform external users of relevant breaches, incidents and threats.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CC7.0 - Common Criteria Related to Change Management		
CC7.1 - The entity's commitments and system requirements, as they relate to security and confidentiality, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.		
CN38	Lexer has defined and documented policies that govern system acquisition, development, maintenance, release and deployment.	No Exceptions Noted
CN39	Project team members collaborate regularly during the project lifecycle to determine the potential effect of proposed changes on security and confidentiality commitments and system requirements.	No Exceptions Noted
CN41	Changes are initiated, logged, developed, assessed, tested, peer-reviewed by Management with external parties notified where applicable.	No Exceptions Noted
CC7.2 - Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and confidentiality.		
CN03	IT Security Policies are documented and reviewed at least annually by the ELT.	No Exceptions Noted
CN04	Changes to Lexer's policies and standards are reviewed and approved by the ELT before being communicated to personnel; revised policies are then available on the intranet.	No Exceptions Noted
CN11	Lexer has a formalised Risk Management process which maintains a Global Risk Register tracking key risks to the organization, including information security risks. The Register is owned by the Information Security Officer with oversight by the ELT.	No Exceptions Noted
CN12	During risk assessments, management identifies changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and updates the potential threats to system objectives. In response to the identification of such risks, management updates its policies, procedures, processes, and controls, as needed.	No Exceptions Noted
CN16	Vulnerabilities identified during risk and vulnerability assessments are logged and tracked through to resolution. All vulnerabilities identified are reviewed and assessed to determine the expected remediation timeline, dependent on the assigned risk rating.	No Exceptions Noted
CC7.3 - Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and confidentiality.		
CN13	The Information Security Function performs periodic internal assessment to review the design and operating effectiveness of internal controls related to Security and Confidentiality. The results of these reviews are reported to the ELT with response plans developed in relation to material deficiencies.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CN16	Vulnerabilities identified during risk and vulnerability assessments are logged and tracked through to resolution. All vulnerabilities identified are reviewed and assessed to determine the expected remediation timeline, dependent on the assigned risk rating.	No Exceptions Noted
CN30	Security incidents are logged and responded to with constant effort until resolved.	No Exceptions Noted
CC7.4 - Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and confidentiality commitments and system requirements.		
CN15	Vulnerability assessments and penetration tests are completed by Lexer's development team and third party vendors to identify weaknesses in system operation that would impair system security and confidentiality commitments.	No Exceptions Noted
CN16	Vulnerabilities identified during risk and vulnerability assessments are logged and tracked through to resolution. All vulnerabilities identified are reviewed and assessed to determine the expected remediation timeline, dependent on the assigned risk rating.	No Exceptions Noted
CN18	Formal role-based access controls are enforced by the access control systems, where configurable.	No Exceptions Noted
CN19	Access to Red Zone, Code Versioning and Release Management Systems is only provisioned to Lexer personnel following authorisation by Management.	No Exceptions Noted
CN20	Administrative access, for management of Customer personnel user access to the Customer Portal, is only provisioned to the Authorised Customer Representative following execution of a client agreement.	No Exceptions Noted
CN23	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are revoked on a timely basis following notification from HR Team regarding termination of employment.	No Exceptions Noted
CN24	Administrative access, for management of Customer personnel user access to the Customer Portal, is revoked following termination of a client agreement.	No Exceptions Noted
CN25	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are reviewed on at least quarterly to confirm access provisioned remains commensurate with business requirements	No Exceptions Noted
CN38	Lexer has defined and documented policies that govern system acquisition, development, maintenance, release and deployment.	No Exceptions Noted
CN41	Changes are initiated, logged, developed, assessed, tested, peer-reviewed by Management with external parties notified where applicable.	No Exceptions Noted
CN42	Code development is managed via an automated version control system which also provides the ability to roll back to the previous stable version in the event of a failed change.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CN43	Segregated development, test and production environments are in place with access to these environments logically restricted.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
Additional Criteria for Confidentiality		
C1.1 - Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.		
CN35	Personal information (both public and sensitive information) involved in business processes, systems, and third-party involvement is clearly identified and classified based on severity and risk within data management policies and procedures.	No Exceptions Noted
CN41	Changes are initiated, logged, developed, assessed, tested, peer-reviewed by Management with external parties notified where applicable.	No Exceptions Noted
CN44	Test data is created using data masking software that replaces confidential information with test information prior to the creation of test databases. No real customer data is allowed to be used for testing / development without prior authorisation from Executive Management.	No Exceptions Noted
C1.2 - Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.		
CN07	Information security and awareness training is conducted for new hires and at least annually for Lexer personnel with Red Zone access, to communicate security and confidentiality obligations.	No Exceptions Noted
CN18	Formal role-based access controls are enforced by the access control systems, where configurable.	No Exceptions Noted
CN19	Access to Red Zone, Code Versioning and Release Management Systems is only provisioned to Lexer personnel following authorisation by Management.	No Exceptions Noted
CN20	Administrative access, for management of Customer personnel user access to the Customer Portal, is only provisioned to the Authorised Customer Representative following execution of a client agreement.	No Exceptions Noted
CN23	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are revoked on a timely basis following notification from HR Team regarding termination of employment.	No Exceptions Noted
CN24	Administrative access, for management of Customer personnel user access to the Customer Portal, is revoked following termination of a client agreement.	No Exceptions Noted
CN25	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are reviewed on at least quarterly to confirm access provisioned remains commensurate with business requirements	No Exceptions Noted
CN35	Personal information (both public and sensitive information) involved in business processes, systems, and third-party involvement is clearly identified and classified based on severity and risk within data management policies and procedures.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
CN41	Changes are initiated, logged, developed, assessed, tested, peer-reviewed by Management with external parties notified where applicable.	No Exceptions Noted
CN44	Test data is created using data masking software that replaces confidential information with test information prior to the creation of test databases. No real customer data is allowed to be used for testing / development without prior authorisation from Executive Management.	No Exceptions Noted
C1.3 - Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.		
CN08	Upon execution of their Employment Agreement, new hires receive an employee handbook and have access to Lexer's online knowledgebox where documents defining personnel's responsibilities for information security can be located. New hires must read and acknowledge their understanding of Lexer's security policy and team handbook.	No Exceptions Noted
CN18	Formal role-based access controls are enforced by the access control systems, where configurable.	No Exceptions Noted
CN19	Access to Red Zone, Code Versioning and Release Management Systems is only provisioned to Lexer personnel following authorisation by Management.	No Exceptions Noted
CN20	Administrative access, for management of Customer personnel user access to the Customer Portal, is only provisioned to the Authorised Customer Representative following execution of a client agreement.	No Exceptions Noted
CN23	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are revoked on a timely basis following notification from HR Team regarding termination of employment.	No Exceptions Noted
CN24	Administrative access, for management of Customer personnel user access to the Customer Portal, is revoked following termination of a client agreement.	No Exceptions Noted
CN25	Access rights to Red Zone, Code Versioning and Release Management Systems held by Lexer personnel are reviewed on at least quarterly to confirm access provisioned remains commensurate with business requirements	No Exceptions Noted
CN29	Data (including backups, storage for workstations and laptops) is encrypted at rest and for all public networks transfers, including web communication sessions.	No Exceptions Noted
CN35	Personal information (both public and sensitive information) involved in business processes, systems, and third-party involvement is clearly identified and classified based on severity and risk within data management policies and procedures.	No Exceptions Noted

Control ID	Control Procedure	PwC Design and Implementation Test Result
C1.4 - The entity obtains confidentiality commitments that are consistent with the entity's confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.		
CN10	Lexer's security commitments (including security obligations, terms, conditions and responsibilities) are documented, along with the responsibilities of external users, in third party contracts and non-disclosure agreements.	No Exceptions Noted
C1.5 - Compliance with the entity's confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.		
CN32	The ISO reviews the design and operational of outsourced controls via third party attestation reports for major subservice providers to ensure they meet organisational Security and Confidentiality requirements; Issues are logged and tracked though to resolution.	No Exceptions Noted
C1.6 - Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.		
CN10	Lexer's security commitments (including security obligations, terms, conditions and responsibilities) are documented, along with the responsibilities of external users, in third party contracts and non-disclosure agreements.	No Exceptions Noted
CN32	The ISO reviews the design and operational of outsourced controls via third party attestation reports for major subservice providers to ensure they meet organisational Security and Confidentiality requirements; Issues are logged and tracked though to resolution.	No Exceptions Noted
CN45	The Information Security Officer is responsible for changes to confidentiality practices and commitments. A formal process is used to communicate these changes to users, related parties, and vendors.	Control did not operate. Unable to assess implementation.
C1.7 - The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.		
CN35	Personal information (both public and sensitive information) involved in business processes, systems, and third-party involvement is clearly identified and classified based on severity and risk within data management policies and procedures.	No Exceptions Noted
CN46	As part of on-boarding a Customer, Lexer performs a gap analysis between client confidentiality requirements and internal policies. Client requirements which a more onerous than existing Lexer policy requirements are reviewed for incorporation into Lexer Policy or logged for management on an as needed basis.	No Exceptions Noted
C1.8 - The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.		
CN47	Lexer disposes of Customer data in accordance with requirements of the Customer contract being terminated.	No Exceptions Noted

APPENDIX A: MANAGEMENT RESPONSE TO FINDINGS

No reportable exceptions were identified as part of PwC independent testing of control design and implementation.

APPENDIX B: LIST OF CRITERIA

Criteria Common to All Security and Confidentiality Principles	
CC1.0	**Common Criteria Related to Organization and Management**
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to Security and Confidentiality.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to Security and Confidentiality.
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting Security and Confidentiality and provides resources necessary for personnel to fulfil their responsibilities.
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to Security and Confidentiality.
CC2.0	**Common Criteria Related to Communications**
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.
CC2.2	The entity's Security and Confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the Security and Confidentiality of the system, is provided to personnel to carry out their responsibilities.
CC2.5	Internal and external users have been provided with information on how to report Security and Confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to Security and Confidentiality are communicated to those users in a timely manner.
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**
CC3.1	The entity (1) identifies potential threats that could impair system Security and Confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyses the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.
CC4.0	**Common Criteria Related to Monitoring of Controls**
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to Security and Confidentiality, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to Security and Confidentiality.
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to Security and Confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

Criteria Common to All Security and Confidentiality Principles	
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to Security and Confidentiality.
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to Security and Confidentiality.
CC5.5	Physical access to facilities housing the system (for example, data centres, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to Security and Confidentiality.
CC5.6	Logical access security measures have been implemented to protect against Security and Confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to Security and Confidentiality.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to Security and Confidentiality.
CC6.0	**Common Criteria Related to System Operations**
CC6.1	Vulnerabilities of system components to Security and Confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to Security and Confidentiality.
CC6.2	Security and Confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.
CC7.0	**Common Criteria Related to Change Management**
CC7.1	The entity's commitments and system requirements, as they relate to Security and Confidentiality, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to Security and Confidentiality.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to Security and Confidentiality.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's Security and Confidentiality commitments and system requirements.
Additional Criteria for Confidentiality	
C1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.
C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.
C1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.
C1.4	The entity obtains confidentiality commitments that are consistent with the entity's confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.
C1.5	Compliance with the entity's confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.
C1.6	Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.
C1.7	The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.
C1.8	The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.