



**Lentra AI Pvt. Ltd.  
Service Organization Control  
SOC 3 Report**

**April 1, 2021 - March 31, 2022**

# Table of contents

SECTION I: INDEPENDENT SERVICE AUDITOR'S REPORT ..... 2

SECTION II: MANAGEMENT'S ASSERTION ..... 5

SECTION III: DESCRIPTION OF THE BOUNDARIES OF THE LENTRA SYSTEM ..... 6

SECTION IV: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS ..... 8

# Section I: Independent Service Auditor's Report

Lentra AI Pvt. Ltd.  
8th floor, Kalpataru Infinia,  
21, Old Mumbai - Pune Hwy,  
Wakadewadi, Bhamburda,  
Pune, Maharashtra 411005

## Scope

We have examined Lentra accompanying description of "Software Development and Support Processes" (SDSP) throughout the period 1-04-2021 to 31- 03-2022, (description) based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period 1-04-2021 to 31- 03-2022, to provide reasonable assurance that Lentra service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Lentra' s uses Softcell Technologies Global Private Limited (Softcell) and ST Telemedia Global Data Centre (STT) subservice organization for its data center services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Lentra to achieve Lentra service commitments and system requirements based on the applicable trust services criteria. The description presents Lentra controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Lentra controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Lentra, to achieve Lentra service commitments and system requirements based on the applicable trust services criteria. The description presents Lentra controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Lentra controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

## Service Organization's Responsibilities

Lentra is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Lentra service commitments and system requirements were achieved. Lentra has provided the accompanying assertion titled "Management Assertion" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Lentra is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

  
DK

### **Service Auditor's Responsibilities**

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

### **Service Auditor's Independence and Quality Control**

We have complied with the independence and other ethical requirements of the *Code of Professional Conduct* established by the AICPA. We applied the statements on quality control standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

### **Inherent Limitations**

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

  
DK

**Opinion**

In our opinion, management's assertion that the controls within the Service Organization's system were effective throughout the period April 1, 2021, to March 31, 2022, to provide reasonable assurance that Lentra's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

**For Sudit K. Parekh & Co.**  
**Chartered Accountants**

Signature: Durgaprasad Khatri  
Durgaprasad Khatri (Jun 18, 2022 11:17 GMT+5.5)

Email: durgaprasad.khatri@skparekh.com

**Durgaprasad Khatri**  
**Partner**

Membership No: 016316

PCAOB Registrant No: 2767

Date: 01-04-2022

Place: Mumbai

## Section II: Management's Assertion

### *Lentra 's Management Assertion*

We are responsible for designing, implementing, operating, and maintaining effective controls within Lentra AI Pvt Ltd ), "Software Development and Support Processes" (SDSP) throughout the period April 1, 2021, to March 31, 2022<sup>3</sup>, to provide reasonable assurance that Lentra 's service commitments and system requirements relevant to security, availability, processing integrity, and confidentiality were achieved. Our description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2021 to March 31, 2022, to provide reasonable assurance that Lentra 's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality ("applicable trust services criteria")<sup>4</sup> set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Lentra 's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section IV.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2021, to March 31, 2022, to provide reasonable assurance that Lentra 's service commitments and system requirements were achieved based on the applicable trust services criteria.

# Section III: Description of the Boundaries of the Lenra System

## **Background and Overview of Services**

Lenra was formed in 2019 with the objective to transform retail lending. Our vision is to be the lending platform of choice for all retail lenders in the world. Our mission in the foreseeable future is to service at least 100 of the retail lenders in India and deliver delight to them in doing so. Based in Pune, Lenra deliver the solutions to the customers as a Software service (SaaS).

## **Significant Changes during the Review Period**

Following significant changes happened during the audit period.

As a result of the move to work from home office along with the recent COVID-19 pandemic, all employees work from home/remotely. Business operations are reviewed regularly, and necessary operational changes are made where necessary to ensure a strong control environment. This was implemented from 19-3-2020 as a part of our investor's global directive and later reinforced by our government's guidance.

## **Impact of Covid and Changes to our Controls**

Due to COVID-19 pandemic in order to ensure business continuity and employee safety, Lenra initiated a secure work-from-home method in March 2020. Employees are given VPN access on a case-by-case basis after being reviewed by the CISO team. Employees are also provided with Lenra's laptops running Ubuntu OS that have been hardened by the IT team.

Employees connect to various IT systems directly from home. For accessing production infrastructure for administration purposes, selected employees connect to the office via VPN client and then connect to production servers via a PIM/PAM software and such sessions are fully recorded for a potential audit later.

## **Subservice Organizations**

Lenra utilizes the following subservice providers for data center services that are not included within the scope of this examination. However, Lenra's responsibilities for the applications and services run at these hosting provider services are covered as part of the audit and in scope. Responsibility matrix is defined as part of the SLA and agreements with these sub service organizations.

## **In scope Product and Service:**

The following products are covered in scope for this report:

<b>Category</b>	<b>Name</b>	<b>Description</b>
<b>Product</b>	<b>MultiBureau</b>	The product sits between a bank's loan origination system (LOS) and the four Credit information bureaus (CIB) as a middleware. This system receives the input fields from the LOS, submits it to the CIB and hands back the retrieved report from the CIB to the LOS. This process is automated at scale and speed with reports and MIS dashboards to all concerned.
<b>Product</b>	<b>GoGetr</b>	This product is like MultiBureau except that it sits between the LOS and any/all data sources external to the bank. The solution helps automate the process of fetching data from sources that are external to the bank, that the bank wants to fetch and use in the process of making a credit risk assessment.
<b>Product</b>	<b>GoNoGo</b>	This is a loan origination software system. This loan workflow automation software begins a journey from establishing the identity of an individual and typically ends with a decision whether the bank approves or rejects a loan application. Significantly, GoNoGo depends on eKYC, MultiBureau, GoGetr, BREx, GoTrust and peripheral other modules in executing its objectives.

<b>Category</b>	<b>Name</b>	<b>Description</b>
<b>Product</b>	<b>LMS (Loan Management System)</b>	Account opening and account maintenance software encompassing the essential elements including KYC records, mandates, a general ledger and reports. The system of records, it may be noted, is a statutory requirement for each folio and is an integral part of this system.
<b>Product</b>	<b>BREx (earlier referred to as SoBRE):</b>	This is the business rule engine that helps a credit risk team establish all rules, criteria, policy and scoring mechanisms in a software system. This system acts to take inputs that are fed into the LOS and spews a decision output based on the rules set. The system also has score calculators and other mechanisms to compute eligibility, look up a table of deviations (exceptions) and other tools of the underwriter's trade.
<b>Infrastructure</b>	<b>Network</b>	<ul style="list-style-type: none"> <li>• The network is segregated into VLANs and separate Network Zones which control access to specific subnets. There are multiple layers of security controls prior to a user accessing the data.</li> <li>• All data access is governed by the Application Products of Lenra for a customer.</li> <li>• All other data access to the Virtual Machines is governed by VPN and Privilege Identity and Access Management tools.</li> <li>• There is no other remote access provided. Lenra networks do not access any Customer/ Third Party networks.</li> <li>• Lenra protects information involved in application services passing over public networks from security threats and unauthorized disclosure or modification.</li> <li>• Network security controls are implemented to ensure that only authorized users are allowed to access the applications.</li> </ul>
<b>Infrastructure</b>	<b>Datacenter</b>	<p>STT is used for hosting of production environment. STT Mumbai, India is used as production environment and the DR site is at STT, Pune, India. The STT data centers are accredited for ISO 27001, TIA 942, PCI-DSS, ISO 20000, ISO 14001, SOC1 Type II. More details can be found at <a href="https://www.sttelemidiagdc.in/awards-accreditation">https://www.sttelemidiagdc.in/awards-accreditation</a></p> <p>The Criteria that relate to controls at the subservice organizations included all criteria related to the Trust Service Principles of Security, Confidentiality and Availability. The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Lenra include:</p> <ul style="list-style-type: none"> <li>▪ The Software Development and related support processes are protected against unauthorized access (both physical and logical).</li> <li>▪ The Software Development and related support processes is available for operation and use and in the capacities as committed or agreed.</li> <li>▪ Policies and procedures exist related to security and availability and are implemented and followed.</li> </ul>
<b>Infrastructure</b>	<b>Server</b>	Nutanix is used for providing production support for the IT infrastructure and virtualization of servers. Nutanix is SOC 2 attested company.
<b>Infrastructure</b>	<b>Third party vendor</b>	Softcell is a third party that provides managed Security incidents, firewalls, management of virtual servers, backups and other private cloud administration. Softcell is ISO 27001:2013 certified company. Softcell, manage our IP block (APNIC announcements), DNS (on Cloudflare) and perimeter devices relating to anti-DDOS, Internet uplink routing and gateway firewall



# Section IV: Principal Service Commitments and System Requirements

Lentra makes service commitments to its customers and has established system requirements as part of the product service. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. Lentra is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Lentra 's service commitments are achieved.

Service commitments include, but are not limited to, the following:

- **Security:** Lentra has made commitments related to securing customer data and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, physical security and other relevant security controls.
- **Availability:** Lentra has made commitments related to percentage uptime and connectivity for applications as well as commitments related to service credits for instances of downtime.
- **Confidentiality:** Lentra has made commitments related to maintaining the confidentiality of customers' data through data classification policies, data encryption and other relevant security controls.

Lentra has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Lentra 's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of various Lentra services and offerings. Lentra 's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality.






# Lentra SOC 3 310322

Final Audit Report

2022-06-18

Created:	2022-06-17
By:	Krishnanand N. Bhat (knbhat@nexdigm.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAARWZzl7XcsEEfY0p5t4brR3OP4sKNcyeq

## "Lentra SOC 3 310322" History

-  Document created by Krishnanand N. Bhat (knbhat@nexdigm.com)  
2022-06-17 - 12:53:36 PM GMT- IP address: 103.94.187.2
-  Document emailed to Durgaprasad Khatri (durgaprasad.khatri@skparekh.com) for signature  
2022-06-17 - 12:54:50 PM GMT
-  Email viewed by Durgaprasad Khatri (durgaprasad.khatri@skparekh.com)  
2022-06-18 - 5:23:59 AM GMT- IP address: 104.47.74.190
-  Document e-signed by Durgaprasad Khatri (durgaprasad.khatri@skparekh.com)  
Signature Date: 2022-06-18 - 5:47:39 AM GMT - Time Source: server- IP address: 103.94.187.2
-  Agreement completed.  
2022-06-18 - 5:47:39 AM GMT