LoanPro®

Service and Organization Controls (*SOC 3®*) Report

Management's Report on Its Assertions on the Effectiveness of Its Controls Over the LoanPro Loan Management System Based on the Trust Services Criteria for Security

January 1, 2021 to June 30, 2021

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations
™

Table of Contents

LoanPro®

SQUIRE
HIGHER PERSPECTIVE

Independent Service Auditor's Report

To Management of
LoanPro Software, LLC

Scope

We have examined LoanPro Software, LLC's (LoanPro) accompanying assertion titled "Assertion of LoanPro's Management" (assertion) that the controls within LoanPro's Loan Management System (system) were effective throughout the period January 1, 2021 to June 30, 2021, to provide reasonable assurance that LoanPro's service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Service Organization's Responsibilities

LoanPro 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 LoanPro's service commitments and system requirements were achieved. LoanPro has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, LoanPro is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve LoanPro's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve LoanPro's service commitments and system requirements based the applicable trust services criteria.

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

Inherent Limitations

There are inherent limitations in 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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management’s assertion that the controls within LoanPro’s Loan Management System were effective throughout the period January 1, 2021 to June 30, 2021, to provide reasonable assurance that LoanPro’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Squire + Company, PC

Orem, Utah
July 28, 2021

LoanPro

Assertion of LoanPro Software, LLC's Management

We are responsible for designing, implementing, operating, and maintaining effective controls within LoanPro Software, LLC's (LoanPro) Loan Management System (system) throughout the period January 1, 2021 to June 30, 2021 to provide reasonable assurance that LoanPro's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2021 to June 30, 2021 to provide reasonable assurance that LoanPro's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

LoanPro'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 attachment B.

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

We assert that the controls within the system were effective throughout the period January 1, 2021 to June 30, 2021, to provide reasonable assurance that LoanPro's service commitments and system requirements were achieved based on the applicable trust services criteria.

Rhett Roberts (Jul 28, 2021 10:18 MDT)

Rhett Roberts
LoanPro Software, LLC
July 28, 2021

Attachment A: LoanPro Software, LLC's Description of the Boundaries of its Loan Management System

The LoanPro Loan Management System (LMS) was created to offer lenders in United States and Canada a modern, cloud-based solution for managing and servicing loans. LoanPro is offered under a subscription-based model. The LoanPro application programming interface (API) allows users to integrate LoanPro's LMS with a lender's existing applications.

Services Provided

The services provided by the LMS include the following:

- Providing customizable features and loan calculators that can be configured for multiple loan types.
- Providing day-to-day, accurate information for loan balances, balances past due, payoff quotes, etc.
- Providing customizable advanced communication, allowing lenders to automate routine loan-servicing communication tasks.
- Providing a website where a customer's borrowers can log in, view their loan data and make payments to their loans.
- Providing transaction history reports, including operational, management and ad hoc reports in a variety of formats.
- Providing onboarding, customer service, custom programming, and account management services to enterprise customers.
- Providing a highly customizable interface and an API that allows lenders to integrate the full set of LoanPro features with their existing backend services.

Infrastructure

The LoanPro LMS is hosted at Amazon Web Servers (AWS) data centers, using the AWS infrastructure as a service offering (IaaS). The various services making up the runtime and provisioning systems for the LoanPro LMS are deployed in AWS region: us-east-1 (North Virginia). When possible, LoanPro's infrastructure is hosted in multiple availability zones.

Servers are divided into topics, keeping them single purpose for both performance and security reasons. Some topics are grouped in load balancers (such as Web/API servers). Additionally, servers are placed in one of three types of subnet groups: private (no inbound and outbound connections), protected (only outbound connections) or public (inbound and outbound connections). Security groups have been established for each subnet. A cloud security agent is installed on all outward-facing web/API servers which provide additional security including firewalls, intrusion prevention and detection (IPS/IDS), file integrity monitoring anti-malware, log inspection and content filtering.

The LoanPro LMS is a multi-tenant application, where tenancy is defined at the database layer (each tenant has their own database in one of the available database servers, or in a non-shared database server, if requested). LoanPro uses Amazon's Aurora database engine; databases containing customer data are stored within volumes. The primary Aurora instance is replicated across multiple availability zones for reliability. Database fields containing confidential data (social security numbers, passwords, birthdates, driver's license numbers) are encrypted at rest. Aurora database clusters reside in the private network, with no public connectivity allowed.

The LoanPro LMS utilizes AWS' S3 to store documents. Storage is segregated by tenant using a unique identifier, which relates the customer to the attachment stored in S3.

Laptops with access to AWS that serve as information assets are subject to LoanPro's Acceptable Use Policy, which prohibits the installation of unauthorized software. Laptops are also required to have anti-malware and data loss prevention software enabled.

Employees access the LoanPro application via a unique username and password to enforce accountability within the system. Employees accessing the system remotely are required to use MFA protocols. Access to sensitive system components maintained in the protected and private subnets require elevated credentials.

Software

The LMS application is developed and maintained by LoanPro. Software updates are released on a quarterly basis using continuous integration and continuous delivery (CI/CD) through AWS' CodePipeline. Prior to releasing software updates to the production environment, LoanPro provides release notes to customers explaining the changes in the software update.

LoanPro has a formalized change management process in place, which requires the identification, documentation, assessment of risk and potential impact of changes, approval of changes, and testing of changes to verify operational functionality.

The development environment within AWS is segregated within the VPC and includes a beta and staging environment.

LoanPro uses an agile development methodology. Developers are assigned tasks which are organized into four-week "sprints." Phabricator is utilized to monitor the progress of changes, tasks within sprints and the status of proposed changes to the system. A "Voice of the Customer" (VOC) process is used to identify customer-requested changes to features within the LMS application. VOC Channels and/or VOC weekly meetings are held by the Product Management team to determine the criticality of the issue before it is scheduled/assigned to a sprint.

Operations personnel are responsible for deploying all code to the production environment and may do so only after the necessary testing. Final code is published to the master branch within AWS.

All production servers are built according to established and documented hardening processes. "Vanilla" images are provided by AWS, and an automated hardening process is applied before servers are allowed to serve any traffic. All production images have built-in security provided by a cloud security agent. The image-creation process is defined with infrastructure as code so it can be put into version control. Any changes are reviewed and monitored.

LoanPro's operating procedures dictate patch management processes. New vulnerabilities are reviewed every week, and a log is maintained with the patched and unpatched vulnerabilities. All non-critical vulnerabilities are patched on a monthly basis, while critical vulnerabilities are patched immediately.

Servers are not patched directly in production; rather, new images are created with all applicable patches applied, and live servers are substituted with new servers created from the patched images. Servers are monitored on a quarterly basis with both an internal scan (using AWS Inspector with all available rule definitions) and an external scan using a third-party provider.

LoanPro has the ability to initiate a roll-back to an earlier image of the LMS in the event the deployment of a new version of the software contains significant unintended consequences.

In addition, the following software, services, and tools support the LoanPro control environment:

- SumoLogic monitors the application environment and provides log monitoring and reporting.
- AWS' CodeDeploy provides automated code deployment to the LoanPro production environment. AWS' CodePipeline automates the software deployment process.
- A cloud security agent provides additional security to outward facing servers and includes firewalls, intrusion prevention (IPS), file integrity monitoring, anti-malware, log inspection and content filtering.
- AWS' Inspector Agent provides internal vulnerability scanning.
- Systems Manager/Secrets Manager
- Identity and Access Management (IAM) provides identity and access management through AWS
- Phabricator is used as a ticketing system for incident management, user access provisioning, and change management processes.
- NewRelic monitors web application traffic.
- Pingdom provides website monitoring for the LoanPro LMS.
- Clam Antivirus monitors and protects LoanPro information assets against viruses and malware.

People

LoanPro has approximately 65 employees organized in the following teams:

Administration – The management team is responsible for managing human resources, vendor management, and facilities. The Chief Executive Officer (CEO) and Chief Operating Officer (COO) are responsible for the overall security of the LoanPro LMS.

Finance - The management team is responsible for managing legal, finance, accounting and billing with the direction of the Chief Financial Officer (CFO).

Software and Development – The software and development team are responsible for developing new products and new features to existing products. The Chief Technology Officer (CTO) is also responsible for the overall security of the LoanPro LMS.

Software Support and Operations – The software support and operations team is responsible for monitoring system stability and tasks related infrastructure and software for existing products.

Processes and Policy Development – The processes and policy development team is responsible for creating, implementing, monitoring and updating company policies, processes, and procedures.

Customer Onboarding – The customer onboarding team works with newly-signed customers on configuring the LoanPro LMS according to the customer's business rules and practices.

Support Team– The Support team is responsible for providing ongoing customer support and consulting to onboarded customers.

Data

Data within the LoanPro LMS and the greater LoanPro infrastructure is carefully guarded. Data is always encrypted in transit using current TLS standards. Depending on the sensitivity of data, it may also be encrypted at rest.

LoanPro has created various input and data validation rules to assist customers in identifying errors and incomplete data fields prior to activating a loan. LoanPro has defined all data fields used in the LMS, consisting of required data fields (fields which are necessary to calculate a loan) and non-required fields (fields that may be applicable to a loan but are not necessary to calculate a loan). There are three ways to import and activate loans within the LoanPro LMS.

1) Customers can manually input data using the user interface (UI) in multiple screens and modules within the LMS. Various error messages occur when data fields either contain a type of data that is not accepted by field format or a required field contains an error or is incomplete. After remediation for all required fields, a list of nonrequired fields appear on a transaction warning pop-up that the customer must accept. In addition, once a loan is submitted and accepted, another pop-up warns the customer that the terms and settings of the loan are locked.
2) Large data sets can be imported into the LoanPro LMS using a .csv file template that can be accessed within the application. This import feature allows customers to import data sets containing different types of transactions and actions. Batches are either accepted or rejected. If the batch is rejected, the LMS identifies the particular data fields that need to be corrected.
3) Customers can create middleware that imports data automatically via the LoanPro API. The customer's website can also be accessed by borrowers to add payments and update personal or insurance information.

Additional rules identify whether a duplicate loan has previously been submitted, the first payment date is prior to the loan contract date, etc.

Payment transactions are also governed by validation controls built within the LMS. A payment import transaction template (.csv) can be accessed and used by customers to ingest payment information into the LMS. A UI for uploading payment information ingests the import and reports the percentage of records validated, percentage of records imported, and number of records updated. Validation controls also screen import data for improper values based on payment type, payments on non-existent loans, etc.

Payment transactions are only processed if data imports are successful. Payment requests are transmitted by the LoanPro LMS to Secure Payments to the customer's payment processor or financial institution and are based on the customer's requirements. At the completion of the transmission, the payment processor or financial institution relay a status back to the LoanPro LMS using a call-back URL to capture data sent about transactions by payment processors. When updated status information is received, statuses are changed in near real-time.

Customers can access reports available on the user interface (UI) of the LoanPro “reports” section. Templated reports have been created by LoanPro; however, customers may request additional report templates.

Customers also can create output comma-delimited value (.csv) files from varying parts of the application. The LoanPro LMS can provide API outputs that are consumed by customer systems. Reporting problems or errors identified by customers should be communicated to the LoanPro Support team. Issues and problems that cannot be resolved immediately are tracked. Resolution timelines are governed by service legal agreements based on the customer’s subscription level.

Report queries can be manually or automatically set and are available for download for 24 hours and are stored within AWS’ S3. Report downloads are encrypted using TLS 1.2. Reports generated for loan balances, payment statuses and interest use all available near real-time data held within the LMS.

Modification of report templates follow established change management processes and procedures. Report servers are clustered and secured in the protected subnet and are also protected by a cloud security agent.

Processes and Procedures

LoanPro’s management has developed and communicated processes and procedures to address key security lifecycle areas. Policies and operating processes and procedures are available to employees on an internal network repository. Every policy has a policy owner who is responsible for managing the risk in the policy’s objective. Policies and operating processes and procedures are reviewed semiannually or annually by the policy owner (based on risk) and are approved by senior management. Key process and procedures documents include the following:

- Information asset classification/data classification (data at rest, in transit, and output)
- System and software development procedures
- Business impact analysis
- Data encryption and encryption key management
- Selection, documentation and implementation of security controls
- Performance of annual management self-assessments regarding security controls
- Monitoring security controls
- Management of access and roles
- Security of data backups and offline storage
- Incident response and business continuity
- Maintenance of restricted access to system configurations, super user functionality, passwords, powerful utilities, and security devices
- Internal team policies, processes and procedures (i.e. administration, customer relations, etc.)

Relevant Aspects of the Control Environment

LoanPro’s control environment has been established by senior management’s awareness of the need of a strong control environment with emphasis on appropriate controls. Controls are included in process and policy documents, and through the actions of the owners and senior management of the company. The elements of the control environment include commitment to integrity and ethical values, oversight responsibility, assignment of authority and responsibility, and a commitment to competence.

Commitment to integrity and ethical values

LoanPro has developed organizational policy statements that include the acceptable use of information assets provided to employees, behavioral standards, code of conduct and other documents which communicate LoanPro's values.

New employees are required to sign copies of these documents during the onboarding process. Ongoing employees are required to sign documents annually.

Oversight of the Management Board

A five-person Management Board has been established by the equity owners of LoanPro. In addition, LoanPro has established an Adviser's Council consisting of experts in compliance, financial technology, industry and regulatory matters. These individuals assist the Management Board in determining initiatives and strategic goals, identifying issues in the external environment, and other issues that may affect the business as a whole. The Management Board and Adviser's Council meet semiannually.

Assignment of Authority and Responsibility

LoanPro's organizational structure provides the framework within which activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed by LoanPro. This organizational structure is based, in part, on the size and the nature of its activities. Assignment of authority and responsibility for operating activities is based on alignment of specific business processes related to the security of the LMS. These activities include establishing policies and procedures related to appropriate business practices, knowledge and experience of key personnel, and resources available for carrying out duties and responsibilities.

Commitment to Competence

LoanPro's commitment to employee competence is supported by human resources policies and procedures. Hiring processes include an evaluation of a candidate's education, experience, and/or skillsets required based on a job posting. Candidates are required to undergo screening and background checks. During the onboarding process, new employees are required to sign acknowledgement forms indicating acceptance of code of conduct principles described in the employee handbook, training on security topics, the asset policy, visitor's policy, removable media policy and information asset policy prior to gaining access to the system.

Employees undergo a formal evaluation process annually which evaluates the employee's competencies against the employee's job description. Employees are also required to participate in security awareness training annually, and specialized positions require additional training in security topics.

Accountability

Internal policies and procedures outline specific internal control responsibilities to be performed by employees. In addition, internal control responsibilities are documented in job descriptions. These documents provide a basis in which individuals are held accountable for performing their internal control responsibilities. Policy and procedures documents are maintained in an internal network repository and are available to all employees. Internal evaluations are conducted on an ongoing basis to ensure employees in compliance with security controls.

Information and Communication

Internal Communication

LoanPro's internal communicates regularly with its employees via emails and newsletters. Information systems supporting communication within work groups include a slack channel and the use of Phabricator. Communication of infrastructure, application and security exceptions are communicated to appropriate personnel via alerts.

External Communication

Customers have the ability to access information through LoanPro's portal. The portal also includes a status page where system issues are posted, a help documents section outlining instructions on how to operate the system, instructions on submitting a ticket and release notes for quarterly software updates. Information on how to contact LoanPro via email or phone call are also included on the portal.

Security Practices

LoanPro has a suite of policies, procedures and practices that encompass functions related to security, safety and business continuity for internal operations and its delivery of services to customers. Security practices have been developed and designed to provide protection of customer data as well as LoanPro's proprietary data. LoanPro is continually working to improve security controls and practices.

Data Classification

LoanPro's Terms and Conditions and Privacy Policy statements are publicly available on its website and include how personal data is handled and describes the conditions under which LoanPro may access, collect and/or use data in a customer's development, test, or production environments.

Risk Assessment

The risk assessment process consists of the following:

- *LoanPro LMS IT Risk Assessment*. The LoanPro LMS IT risk assessment is reviewed on a semi-annual basis or as needed for changes in the security and technology environment. This risk assessment addresses identified and/or potential risks. Risks are ranked as to likelihood and impact. Risk mitigation plans or control activities are in place to address high-level IT risks related to the LoanPro application.

- *Business Risk Assessment*. The business risk assessment is conducted at least annually and is updated as necessary for significant changes identified by senior management and the Adviser's Council to respond to LoanPro's operational, compliance and reporting risks. Risks are ranked as to likelihood and impact. High-level risks are evaluated for appropriate control activities and risk mitigation plans/activities.

Monitoring

In addition to the daily oversight conducted by the Software Support and Operations team (log monitoring, internal vulnerability assessments and report review), the Software Support and Operations team conduct periodic reviews of the LMS on a weekly, monthly, quarterly, semi-annual and annual basis to ensure controls related to the security of the system are being assessed for effectiveness.

The Process and Policy Director evaluates the operating effectiveness of controls on an ongoing basis and during the annual business risk assessment and policy review process.

Complementary User Entity Controls (CUECS)

Security is a shared responsibility between an application service provider and its customers. The LoanPro LMS has been designed with the assumption that certain controls will be implemented by user entities (customers). Certain requirements can only be met if CUECS are suitably designed and operating effectively, along with related controls at LoanPro.

Attachment B: LoanPro Software, LLC's Principal Service Commitments and System Requirements

LoanPro has designed processes and procedures related to its LMS to meet the service, security, operational and compliance objectives established by LoanPro. Security and compliance commitments are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Providing commercially reasonable efforts to safeguard the security of the LoanPro LMS.
- Designing the LoanPro LMS to permit system users to access the information they need based on their role, while restricting users from access to information not necessary for their role.
- Providing database structures that permit end users to access their company's customer data while restricting access to any other company's data.
- Providing data encryption to protect customer data in transit and at rest.
- Maintaining incident management policies and procedures.
- Maintaining data backup policies, vulnerability tracking, patch management and other procedures to ensure the accuracy, completeness and security of customer data residing in the LoanPro LMS.

Security and other system requirements are documented in LoanPro's policies and procedures, system design documentation and in contracts with customers. Security policies include an organization-wide approach to how systems and data are protected. Standard operating procedures have also been designed and documented for employees to carry out specific manual and automated processes required in the operation and development of the LoanPro LMS.