AT 101 SOC 2 Type 2

Independent Service Auditor’s Report on Management’s Description of a Service Organization’s System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security

April 1, 2013 through March 31, 2014
# Table of Contents

## I. Independent Service Auditor’s Report
- Independent Service Auditor’s Report ................................................................. 3

## II. Information Provided by MARQUIS
- Management Assertions Letter .............................................................................. 7
- Description of MARQUIS’ Information Technology and Application Development System .................................................. 10
  - Company Overview ............................................................................................ 10
  - MARQUIS’ Products and Services Overview .................................................... 10
  - System Description ............................................................................................ 14
  - Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Information and Communication .................................................................................... 20

## III. Information Provided by Auditwerx
- Security Principle ................................................................................................. 29
  - Control Objective 1 – Policies ........................................................................... 29
  - Control Objective 2 – Communications .............................................................. 33
  - Control Objective 3 – Procedures ....................................................................... 35
  - Control Objective 4 – Monitoring ....................................................................... 46
I. Independent Service Auditor’s Report
INDEPENDENT SERVICE AUDITOR’S REPORT

Jeff Kassing
President
MARQUIS Software Solutions, Inc.
5160 Tennyson Pkwy, Suite 100E
Plano, TX 75024

Scope

We have examined the description titled “Description of MARQUIS’ Information Technology and Application Development System Throughout the Period April 1, 2013 through March 31, 2014” (“the description”) and the suitability of the design and operating effectiveness of controls to meet the criteria for the security principle set forth in TSP Section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids) (applicable trust services criteria), throughout the period April 1, 2013 through March 31, 2014. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of MARQUIS’ (“MARQUIS” or “the Company”) controls are suitably designed and operating effectively along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

MARQUIS’ Responsibilities

In Section II, the Company has provided an assertion regarding the fair presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the applicable trust services criteria throughout the period April 1, 2013 through March 31, 2014. MARQUIS is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Auditwerx’ Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in MARQUIS’ assertion and on the suitability of the design and operating effectiveness of the controls to meeting the applicable trust services criteria, based on our examination. We conducted our examination 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, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period from April 1, 2013 through March 31, 2014.
Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

**Inherent Limitations**

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

**Opinion**

In our opinion, in all material respects, based on the description criteria identified in MARQUIS’ assertion and the applicable trust services criteria:

a. The description fairly presents the system that was designed and implemented throughout the period April 1, 2013 through March 31, 2014.

b. The controls stated in the description were suitably designed to provide reasonable assurance that the trust services criteria would be met if the controls operated effectively throughout the period April 1, 2013 through March 31, 2014, and user entities applied the complementary user entity controls contemplated in the design of the MARQUIS’ controls throughout the period April 1, 2013 through March 31, 2014.

c. The controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period April 1, 2013 through March 31, 2014.

**Description of Tests of Controls**

The specific controls we tested and the nature, timing, and results of our tests are presented in the section of our report titled “Description of Test of Controls and Results Thereof.”

**Restricted Use**

This report and the description of tests of controls and results thereof in Section III of this report are intended solely for the information and use of MARQUIS; user entities of MARQUIS’ Information Technology and Application Development system during some or all of the period April 1, 2013 through March 31, 2014; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Company
- How the Company’s system interacts with user entities, subservice organizations, or other parties
- Internal control and its limitations
• Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
• The applicable trust services criteria
• The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

Auditwerx

Auditwerx

April 14, 2014
Tampa, Florida
II. Information Provided by MARQUIS
We have prepared the description titled “Description of MARQUIS’ Information Technology and Application Development System Throughout the Period April 1, 2013 through March 31, 2014” (“the description”), based on the criteria in items (a)(i) – (ii) below, which are the criteria for a description of a service organization’s system in Paragraphs 1.34-35 of the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2SM) (the description criteria). The description is intended to provide users with information about the Information Technology and Application Development system, particularly system controls intended to meet the criteria for the security principle set forth in TSP Section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that:

a. The description fairly presents the Information Technology and Application Development system throughout the period April 1, 2013 through March 31, 2014, based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided

(2) The components of the system used to provide the services, which are the following:

- **Infrastructure** – The physical and hardware components of a system (facilities, equipment, and networks).
- **Software** – The programs and operating software of a system (systems, applications, and utilities).
- **People** – The personnel involved in the operation and use of a system (developers, operators, users, and managers).
- **Procedures** – The automated and manual procedures involved in the operation of a system.
- **Data** – The information used and supported by a system (transaction streams, files, databases, and tables).

(3) The boundaries or aspects of the system covered by the description

(4) How the system captures and addresses significant events and conditions

(5) The process used to prepare and deliver reports and other information to user entities and other parties

(6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization or other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls

(7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization’s system

(8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with
controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria; and for privacy, the types of activities that the subservice organization would need to perform to comply with our privacy commitments

(9) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons therefore

(10) Other aspects of the service organization’s control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria

(11) Relevant details of changes to the service organization’s system during the period covered by the description

ii. The description does not omit or distort information relevant to the service organization’s system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. The controls stated in the description were suitably designed throughout the specified period to meet the applicable trust services criteria.

c. The controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.

d. MARQUIS does not use subservice organizations or other parties to operate its statement of scope system. Accordingly, our description does not address the criteria in items (a)(i)(6) and (a)(i)(8).

By: /S/ Jeff Kassing

Jeff Kassing
President

April 14, 2014
DESCRIPTION OF MARQUIS’ INFORMATION TECHNOLOGY AND APPLICATION DEVELOPMENT SYSTEM

Company Overview

MARQUIS was founded in the mid-1980s, providing software, outsourcing, consulting services, and direct mail fulfillment specifically for banks and credit unions. They provide solutions through marketing and sales tools, compliance management and consulting. As an organization that serves financial institutions worldwide, they adhere to the security policies demanded by the industry and regulators.

MARQUIS’ Products and Services Overview

Products and Services Offered by MARQUIS Include:

- Marketing Solutions
- Compliance Solutions
- Consulting Solutions

Marketing Solutions

MarketTrax

MarketTrax provides a Marketing Customer Information File (MCIF) application for first time users. MarketTrax is a complete MCIF solution, some of the features include:

- Target and measure marketing campaigns
- Increase customer retention
- Increase customer loyalty
- Increase profitability
- Reduce mailing costs
- Cross-sell intelligently
- Increase renewals of maturing accounts
- Measure sales performance
- Create client messaging for home banking

ExecuTrax

ExecuTrax is a more advanced MCIF than MarketTrax. This is the next generation in MCIF technology and strategic marketing information management. ExecuTrax delivers updated client information nightly so that clients can drive their marketing based on real-time client events.

The MCIF is refreshed more than just once per month so client information is reliable and current. Customers receive information from the client within days, instead of weeks or months. The client can utilize their institution’s Web site to respond with relevant marketing to all of these inquiries with the use of MCIF. Fundamentally, the features and benefits of ExecuTrax mirror that of MarketTrax, except for the nightly update and thin client architecture.
OnTrax Marketing Services provides the client intelligence needed to drive both strategic and tactical marketing efforts. Benefits of utilizing OnTrax include:

- Understanding the information the client will get and taking specific action
- Knowing which relationships deliver a profit
- Anticipating what products the client’s customers are likely to buy next
- Deciphering which direct mail campaign will produce results
- Enhance marketing with tactical projects that will deliver real life return on investment (ROI).

These services include accepting the client’s raw data files, cleaning the account data to ensure effective match rates and accuracy, calculating profitability (which will balance to the general ledger), house holding accounts into common rooftops, and then producing reports and analysis.

In addition, MARQUIS will provide specific guidance on what should be done to enhance and retain existing relationships and to find high value new relationships.

CallTrax was designed exclusively to help financial institutions easily manage and monitor their formal sales and service CRM initiatives. CallTrax enables the client to embrace and manage a formal sales program. Clients can track their sales activity and performance with existing customers, prospects, third-party partners, and affiliates. Clients can manage time-sensitive offer calling activity, post and track internal referral action, manage customer support information, as well as view sales and management reports for activity, performance, and incentives all through one integrated solution.

CallTrax delivers client intelligence that is updated nightly to their entire sales team. Everyone at the client’s institution can know what every customer is up to, what they want/need, and who is going to call and follow up with them to drive loyalty, retention, and revenue growth.

referralTrax automates the referral process at user financial institutions. Users have access to the status of every referral in their institution at any time.

In addition, referralTrax provides a complete view of a financial institution’s customer relationships. referralTrax allows the entire organization to see the value of their individual relationships, targeted one-to-one messaging, the next product their customers are likely to want next, as well as automating the referral tracking process. This allows the client to move away from the paper-based referral process that may exist within their institution today. referralTrax will not only automatically track the referrals but allow for user staff to see all referral activity by product, officer, branch, etc.

referralTrax is a browser-based solution that enables secure access to customer data 24x7x365 via the client’s secure Intranet server.
Q-Trax is MARQUIS’ entry-level CRM solution. If the client is still using paper to track referrals, tasks, and pipeline activity, Q-Trax can manage all of these in one easy-to-use browser-based system.

Q-Trax includes several reports that provide the client with an analysis of each type of activity by office, employee, product, task type, and more. All of the reports are saved into a worksheet that is easy for the client to modify and enhance.

Q-Trax uses browser technology. Users merely need to load Q-Trax onto their server, and access can be granted from any PC or smart phone (e.g., Blackberry, iPhone, etc.). Client officers in the field can enter a task for a customer and have it completed by someone else before they leave the customer’s office.

Q-Trax also includes a referral entry App for client tellers that can be integrated with the client teller platform system.

CenTrax is the Windows-based Community Reinvestment Act, Home Mortgage Disclosure Act, and Fair Lending software solution that comes standard to comply with applicable regulations. CenTrax includes the following capabilities to assist with compliance:

- Geo-coding
- HMDA Loan Application Register (LAR) and CRA Loan Register (LR) Wizards
- Examiner charts
- Comprehensive reporting
- Mapping and graphing to visually communicate performance
- Aggregate data for CRA and HMDA peer performance comparison
- Easy filtering to see only the segments/markets requested
- Optional Fair Lending features to monitor Fair Lending processes

Fair Lending is a completely integrated option to the CenTrax software.

FastTrax is an online geo-coding system that provides immediate census tract and demographic information associated with a borrower’s address. FastTrax allows users to capture census tract numbers up front during the application process and to understand important demographic characteristics of the applicant. FastTrax assists with data integrity, geo-coding accuracy, and by allowing the client to maximize lending opportunities in their markets.

c/dTrax enables the client to collect and report Community Development activities such as:

- CD Loans
- Services
- Investments
c/dTrax supports the compliance officer at CRA exam time by providing an easier way to provide reporting and results. c/dTrax features the automation that enables everyone within the client organization to enter their own data, which in turn makes it easier at CRA exam time.

Compliance Solutions

MARQUIS provides many outsourced services to financial institutions of all sizes. MARQUIS offers the following Compliance Service options for managing Compliance:

- CRA Services
- Home Mortgage Disclosure Act Services (HMDA)
- Geo-coding
- Mapping

Community Reinvestment Act (CRA) Services

MARQUIS has developed packaged reports that help prepare and guide banks, thrifts, and credit unions through their CRA exam. MARQUIS also offers CRA Loan Register (LR) filing. This service enables MARQUIS to take the client’s small business/small farm information and prepare the data for submission.

CRA Manager – MARQUIS’ Comprehensive CRA Exam Reporting/Mapping assists users in preparing for their CRA exams. MARQUIS will produce the CRA Exam Tables, provide mapping of performance in the client’s Assessment Area, geo-code their records, and then compile the user data in the required format.

Home Mortgage Disclosure Act Services

Collecting and reporting home mortgage activity is a requirement of any lender with greater than $35 million in assets that receives applications within Metropolitan Statistical Areas (MSAs). MARQUIS assists users in collecting, scrubbing, geo-coding, edit checking, verifying, and submitting this data in the form and fashion outlined by regulators.

HMDA Loan Application Register (LAR) Filing – MARQUIS’ HMDA service takes raw data and at the end delivers the required submission to regulators.

Geo-Coding

At the heart of the analysis and submission for CRA, HMDA, and Fair Lending is geo-coding. Without accurate and reliable geo-coding, the client’s analysis and annual HMDA and CRA submissions will be flawed. MARQUIS guarantees a 90% match rate on all valid address records using the regulatory required address and zip code match.

Geo-Coding Services – Clients send their account addresses to MARQUIS via secure file transfer protocol (FTP), and MARQUIS returns a processed geo-coded file to the client in the same manner.

Mapping

Presenting information in a map overlay format allows users to make more effective presentations. MARQUIS makes it easy for users to document their performance with Mapping Services.
Consulting Solutions

Compliance

MARQUIS’ Professional Compliance Consulting team can reduce the user workload of compliance with federal and state examining agencies.

- *For HMDA:* MARQUIS’ professional HMDA services range from performing the HMDA work for the client, analyzing their HMDA lending patterns vs. peers, and up to full-scale file review.

- *For CRA:* MARQUIS’ consulting staff can perform a complete CRA performance evaluation (PE) on the client’s institution. MARQUIS can guide the client through the regulatory changes and requirements to file the required CRA LR or perform a detailed CRA file review.

- *Fair Lending:* Fair Lending monitoring is not optional for any bank of any size. MARQUIS offers expertise in Fair Lending compliance and reporting.

Marketing

MARQUIS offers Professional Marketing Consulting, utilizing the services of MARQUIS Approved Consultants (MACs). MARQUIS offers:

- Direct mail creation
- Branding
- Strategic planning
- Competitive market analysis
- Sales training
- Loan/deposit development

System Description

The System is comprised of the following components:

- Departments/People (functional areas, operators, users, and managers)
- Infrastructure (facilities, equipment, and networks)
- Systems/Software (overview, key components, applications, and utilities)
- Procedures (automated, manual procedures involved in the operation of the system)
- Data (transaction streams, files, databases, and tables)

The following sections of this description define each of these five components above that comprise the entire System.

Departments/People

All employees of MARQUIS are obligated to respect and protect confidential data. A background check is required by individuals before being hired by MARQUIS. As part of the New Hire package all employees are given the Employee Handbook and required to sign that it has been read and pledge to agree to follow all MARQUIS policies and procedures including security policies. Continued education is performed throughout the year through staff and department meetings.
IT personnel provide the following core support services for the components of MARQUIS’ IT Environment:

- Systems and Network Monitoring
- Security
- Database Administration
- Backup Operations
- Network Management
- Application Change Management
- Infrastructure Change Management

Infrastructure

MARQUIS headquarters is located in a secure, modern office building developed to meet the needs of a high-tech firm. The building is monitored inside and out for security purposes. Controlled access to the building is maintained by using card readers to grant access to the areas based on individual permission rights. On-site security guards are used to monitor the building after business hours. The server room can only be accessed by system administrators and staff based on job responsibilities. Fire Detection and Suppression Systems are used as an early detection to limit loss due to fire. Fire detection systems are tailored to the building needs and engineered to meet all county fire codes.

MARQUIS servers are protected from outside intrusion through the use of an enterprise class firewall and monitored for access attempt failures by a gateway monitoring system. MARQUIS has also deployed a filtering function in the firewall to add an additional layer of protection for corporate systems. MARQUIS servers are protected from electronic intrusion and utilize vulnerability & penetration testing to analyze potential threats. MARQUIS uses anti-virus and anti-spyware software to protect systems from malicious code such as viruses, worms, and Trojans.

MARQUIS uses the technique of NAT on the main Internet router to provide hidden Internet addresses to internal Company computers. This effectively mitigates the possibility of external sources finding the addresses of internal Company computers.

Network Address Translation (NAT) allows computers on a private network to access the Internet through an intermediary called the Network Address Translator. The Network Address Translator examines all packets destined for the Internet, removes the private IP address from the IP header, substitutes the address of the NAT public interface, and forwards it to the destination. When the resource at the destination IP address responds to the request, the Network Address Translator receives it, checks its internal table to see which client the packet belongs to, and forwards it to the proper client.

MARQUIS utilizes intrusion detection and prevention technology at the perimeter of its network to detect unauthorized access attempts and the presence of malicious code. Company administrators manage and monitor the system. Alerting is configured to notify administrators if predefined thresholds are met or exceeded.

MARQUIS uses Virtual Private Networking (VPN) to allow remote users to access certain segments of the Company’s internal network. Remote connections are authorized and configured on a case by case basis by management and reviewed periodically. The connections are integrated into monitoring systems. For remote user connections, users authenticate with the VPN concentrator and then authenticate with the Windows domain to gain access to network resources. Two levels of access rights are implemented based on the type of users accessing the network. Strong VPN authentication and encryption protocols are in use.
Network Diagram

The following diagram shows the basic layout of MARQUIS’ network.

![Network Diagram](image)

**Systems/Software**

MARQUIS applications are developed using a standard software development life cycle that ensure changes to platforms and new implementations are performed in a logical systematic manner. The Company provides software for deployment in an on-premises client model as well as providing application hosting from the corporate IT facility.

Logical access to MARQUIS’ systems, applications, and data is limited to properly authorized individuals, and user rights are kept to a minimum based on job responsibility. System administrators at the direction of management control network and server passwords. All user account authentication to the network is managed via Microsoft Active Directory. System passwords are managed by the Systems Administrator who follows a strict password policy. The VP, Product Development is responsible for maintaining data integrity and for determining end-user access rights. All access granted to systems, applications, and data is password protected using role-based security.
MARQUIS uses server and workstation operating system software is based on the Microsoft Windows platform. Microsoft Active Directory and Group Policy have been implemented to provide administrative security boundaries for MARQUIS’ staff. All workstations are members of the MARQUIS domain and have policies enforced that restrict user rights to authorized business needs. Patch management software is utilized to manage the server operating systems and supporting software with regular deployment of security patches. MARQUIS maintains rapid response support agreements with all critical hardware and software vendors.

MARQUIS maintains copies of files and data on backup media. Backups include programs, scripts, client data, etc. Backups at each location are automated and run at predefined schedules. All exceptions to a successful backup will generate alerts to appropriate personnel who monitor these processes. Backup media is rotated and secured by the system administrator.

Procedures

MARQUIS has several policies in place that ensure procedures are documented to manage known and expected processes. The Acceptable Use Policy sets essential guidelines for the appropriate use of hardware to perform duties as employees of MARQUIS. It is important to have clear guidelines for acceptable use of computers that prevent the risk of creating system or network issues that would compromise network systems by allowing access by predators of business systems. The Password Policy defines the internal network password policies in regards to password characteristics, length, complexity and procedures to reset password if needed. The Client Security Policy insures the integrity of MARQUIS’ Business Information. This policy focuses on the computers that run their operating system, other basic services like file storage and print queues detailing how these systems connect to MARQUIS’ networks. The purpose of their Encryption Policy is to provide guidance for the use of encryption concerning the handling of client data utilizing FTP, Email, shipping and storage. The Data Backup Policy ensures that both data & software are regularly and securely backed-up from each MARQUIS server. This policy is essential to protect against the loss of data & software and to facilitate a rapid recovery from any IT failure.

The Disaster Recovery Policy is enhanced from time to time, in response to tests performed that mimic a real-life disaster scenario. The Disaster Recovery Plan outlines the process, procedures and management actions to be taken if a disaster causing an extended outage to the MARQUIS Information Technology Infrastructure. MARQUIS uses the Incident Response Policy to manage and investigate incidents that meet all levels of computer incident criteria or any other incident that compromises the security of MARQUIS. The scope of this policy is to identify what qualifies as an incident, define the process to resolve the incident and coordinate efforts to prevent another incident from occurring. It is each employee’s responsibility to follow these guidelines and know these polices.

Client Implementation

MARQUIS has procedures and standards in place for implementing clients. The procedures cover the implementation phases such as:

- CRM consultation
- General information
- Data section
- Data files
- Balancing
- CRM customization
- Baseline review
- Kick-off presentation
- Training
- Implementation
MARQUIS is equipped to customize or adapt systems to any number of configurations. MARQUIS employs a team that designs and verifies system configurations. Once the platform-specific configuration guidelines have been met, systems are built to the clients’ previously agreed-upon implementation details. Once implemented, the systems can be fully managed and supported by MARQUIS’ support staff. All implementations are approved by the client and MARQUIS’ integration managers in a transition meeting prior to being placed into support status.

**Support Operations**

MARQUIS uses software for tracking support issues and maintaining historical records. MARQUIS has configured the application with multiple queues for each specialized group. Customers can submit work orders and receive a response from the support group for follow up. Customers can also email directly or call in during regular business hours.

Client Support receives customer problem reports via MARQUIS’ application, email, or telephone and utilizes an online problem tracking and reporting system to assist in:

- Logging the problem report (ticketing)
- Ticket tracking
- Routing and documenting all actions taken

The incoming ticket queue is monitored by support staff on a rotating basis. Tickets are triaged by the on-call staff member and troubleshooting steps taken. The ticket follows an escalation path to development should the first level not find a resolution.

**Data**

Maintaining the integrity and confidentiality of Customer Data is MARQUIS’ highest responsibility. To fulfill this responsibility, MARQUIS has several policies which cover Client Implementation, Data Transfer, Data Storage, Data Destruction and Data Transit.

Before MARQUIS will receive any data from a customer, MARQUIS must receive a signed Software or Services Agreement along with a signed Privacy Addendum. These agreements provide the baseline for the transfer of data in a safe and secure manner.

Data may be sent to MARQUIS by a client various times throughout an Agreement, using a variety of methods. MARQUIS’ client can send information to MARQUIS using one of three methods including Secure FTP (preferred), Email, or Secure Physical Delivery. Regardless of the method chosen, MARQUIS’ client is instructed to make every effort to encrypt, password protect, and otherwise secure its data prior to delivery to MARQUIS. When MARQUIS returns data back to the client, it is always encrypted, and compressed into a password protected “zip” file for security.

Encryption of data is an essential means of ensuring information is not intercepted as it is transferred from source to destination. MARQUIS has established an Encryption Policy to provide guidance on the standards and methods to be used for data transmissions. MARQUIS uses a number of encryption programs to ensure secure communications. A secure sockets layer (SSL) connection via MARQUIS’ secure FTP site is the preferred method of data exchange. MARQUIS also supports Pretty Good Privacy (PGP).

During the course of a contracted project, which includes the setup phase for new clients, all of a client’s data is stored on a secure network. The secure network is organized by task and business line so that only employees involved in the processing of an institution’s data may have access to that institution’s data.
Access to client confidential data is only granted to those MARQUIS employees who are directly responsible for a task or project licensed by client. Even authorized individuals may use confidential records only for authorized purposes. The Information Security program provides guidelines for external connections, for data communications, for connecting devices to a network, and for adding new software to systems. As part of the program, the responsibility and accountability for its implementation must be established.

Once MARQUIS has completed the contracted project all original media provided to MARQUIS and all files generated by MARQUIS for the customer will be destroyed. Additionally, all reports will be deleted or shredded for the client’s protection. MARQUIS utilizes a credited destruction service. Proof of destruction will be provided upon client’s request.
Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Information and Communication

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The control environment has a pervasive influence on the structure of business activities, establishment of objectives, and assessment of risks. It influences control activities, information and communication systems, and monitoring procedures. The control environment is influenced by an entity’s history and managerial culture. Effectively controlled entities strive to have competent personnel, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive corporate direction. These entities establish appropriate controls that foster shared values and teamwork in pursuit of the organization’s objectives.

Control environment elements include the following, and the extent to which each element is addressed at MARQUIS is described below:

- Management Controls, Philosophy, and Operating Style
- Integrity and Ethical Values
- Organizational Structure
- Assignment of Authority and Responsibility
- Standard Operating Controls
- Audit
- Risk Assessment
- Monitoring

Management Controls, Philosophy, and Operating Style

Management is responsible for directing and controlling operations; establishing, communicating, and monitoring control policies and procedures; and setting the tone for the organization. Importance is placed on accuracy and integrity, maintaining written and updated procedures, security and privacy, and establishing and maintaining sound internal controls over all functional aspects of operations.

Management’s philosophy and operating style affect the way the entity is managed, including the kinds of business risks accepted. MARQUIS places a great deal of importance on working to ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in daily operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in customer support and transaction processing.

Formal job descriptions and regular departmental/divisional meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operate under MARQUIS policies and procedures, including confidentiality agreements and security policies. Periodic training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring customer base for trends, changes, and anomalies.

Competence should reflect the knowledge and skills needed to accomplish tasks that define an individual’s job. Through consideration of an entity’s objectives and the strategies and plans for achievement of those objectives, management must determine how well these tasks need to be accomplished. Management has identified the competence levels for particular jobs and translated those levels into requisite knowledge and skills.
Integrity and Ethical Values

Maintaining a climate that demands integrity and ethical values is critical to the establishment and maintenance of an effectively controlled organization. The effectiveness of internal controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. MARQUIS has programs and policies designed to promote and ensure integrity and ethical values in its environment.

MARQUIS desires to maintain a safe, pleasant, and cooperative working environment and expects employees to have high standards of performance, integrity, productivity, and professionalism. MARQUIS has developed professional conduct policies that set forth policies of importance to all employees relating to ethics, values, and conduct. All employees are expected to know and adhere to these standards, as well as to generally accepted norms of conduct and courtesy at all times. While managers are responsible for understanding, communicating, and enforcing MARQUIS policies, this does not override or diminish an employee’s individual responsibility to be aware of and adhere to these policies. Violations of these policies or other forms of misconduct may lead to disciplinary or corrective action up to and including dismissal.

Standards of Conduct

The Company has implemented standards of conduct to guide all employee and contractor behavior. Management monitors behavior closely, and exceptions to these standards lead to immediate corrective action as defined by Human Resources (HR) policies and procedures. Additionally, all employees must sign confidentiality agreements prior to employment. Any employee found to have violated the Company’s ethics policy may be subject to disciplinary action, up to and including termination of employment.

Commitment to Competence

The Company has formal job descriptions that define roles and responsibilities and the experience and background required to perform jobs in a professional and competent fashion. The Company determines the knowledge and skills needed to perform job duties and responsibilities and hires for that skill set and job requirements. Management monitors and formally evaluates employee and contractor performance on a periodic basis to determine that performance meets or exceeds Company standards.

Organizational Structure

An entity’s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Significant aspects of establishing a relevant organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. Significant cross-training between management positions and between staff positions exists to help ensure smooth operations and maintenance of controls during staff or management absence.

Assignment of Authority and Responsibility

The extent to which individuals recognize that they are held accountable influences the control environment. This holds true for everyone who has ultimate responsibility for activities within an entity, including the internal control system. This includes assignment of authority and responsibility for operating activities, and establishment of reporting relationships and authorization protocols. MARQUIS’ management encourages individuals and teams to use initiative in addressing issues and resolving problems. Policies describing appropriate business practices, knowledge and experience of key personnel, and available resources are provided to employees in order to assist them in carrying out their duties.
MARQUIS is led by a team of senior executives that assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments. Such assignments commonly relate to achieving corporate objectives, oversight of operating functions, and any compliance with applicable regulatory requirements. Open dialogue and individual initiative are encouraged as fundamental parts of the Company’s goal to deliver client service.

**Roles and Responsibilities**

*The following organizational chart depicts MARQUIS’ corporate structure.*

Led by Executive Management, MARQUIS is segregated into the following 12 distinct and separate departments:

- Go MARQUIS
- DM Sales
- Creative Department
- Compliance Sales
- Compliance Consulting
- Marketing Sales
- Marketing Consulting
- Administration
- Support Services
- Product Development
- Systems Administrator
- Client Services

Executive Management is responsible for developing and establishing organizational goals, strategic vision, organizational direction, client strategy, client acquisition, market positioning, internal controls, and Company growth.
**Go MARQUIS** – This department is responsible for the overall client relationship. This includes initial contact, managing the software setup process, high level usage of the product, uncovering referrals and training opportunities, managing customer satisfaction ratings, as well as software renewals.

**DM Sales** – MARQUIS’ DM Sales managers are responsible for calling on banks and credit unions with a focus on the direct mail programs. Principle contacts depend upon the size of the institution and include, but are not limited to, the President, EVP, and Marketing Director.

**Creative Department** – The Creative Department functions as a full service creative agency, which includes a print fulfillment operation.

**Compliance Sales** – MARQUIS’ Compliance Sales managers are responsible for calling on banks. Principle contacts depend upon the size of the institution and include, but are not limited to, the President, EVP, and Compliance officer.

**Compliance Consulting** – MARQUIS’ Compliance consultants serve as subject matter experts and trusted advisors to help clients satisfy the expectations of regulators and their boards. They form a partnership with clients and draw on their full range of experience and success. They develop specific and proven recommendations to help clients meet and comply with regulatory standards.

**Marketing Sales** – MARQUIS’ Marketing Sales managers are responsible for calling on banks and credit unions. Principle contacts depend upon the size of the institution and include, but are not limited to, the President, EVP, and Marketing Director.

**Marketing Consulting** – MARQUIS’ Marketing consultants serve as subject matter experts and trusted advisors in the areas of financial marketing. They form a partnership with clients and draw on their full range of experience and successes. They develop specific and proven recommendations to help clients achieve their strategic business objectives.

**Administration** – This department has two distinct sub-departments:

- **Human Resources** – This department is responsible for providing a quality workforce by aiding all departments in the selection and retention of qualified employees as well as providing a safe and comfortable work environment for all Company employees. Human Resources is responsible for all personnel functions including:
  - Employee hiring procedures that include background and credit checks
  - Employee benefit administration
  - Payroll auditing, reporting, and processing
  - Compliance with external and internal regulatory and policy requirements
  - All recordkeeping as it relates to Human Resources
  - Creation and interpretation of personnel policies and procedures
  - Implementation and ongoing responsibility for employee orientation, education, and employee competency training programs
  - Maintenance of a system of employee performance evaluations
  - The recruitment process, which includes employee qualifications, testing, and selection

Written job descriptions for employees are maintained by the Director of Human Resources. The descriptions are reviewed annually and revised as necessary.
• **Accounting** – This department is responsible for managing accounting functions, preparation of reports and statistics detailing financial results, as well as establishing and maintaining accounting practices to ensure accurate and reliable data necessary for business operations is provided and safeguarded. This department oversees accounts receivable, accounts payable, payroll, and budget.

**Support Services** – This department is responsible for helping all clients in need of assistance with any MARQUIS usage, implementation, upgrades, and various PC or server technology questions.

**Product Development** – This department is responsible for writing original and modifying existing software programs to provide new application functionality and fix inappropriate application behavior. Product Development interacts with senior staff and customers to develop extended knowledge of software changes requested as well as to test the results of the work performed for conformance to assignment expectations. The development process covers all disciplines of project management, software development, and software quality assurance.

**System Administration** – This department is responsible for infrastructure support, network security, disaster recovery readiness, client-server applications, cable/fiber installation, desktop support, and helpdesk operations. This department oversees the installation of new servers, troubleshooting/repair of all hardware-related issues, and maintains and analyzes all networking equipment. A main function of this department is server room administration, which includes design, implementation, expansion, and 24x7x365 operational support. This department is responsible for IT security.

**Client Services** – This department is responsible for handling all new client software setups along with processing the outsourced client data each month.

**Standard Operating Controls**

MARQUIS’ management sends guidance to employees regarding expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluation, counseling, promotion, compensation, and remedial actions.

MARQUIS has hiring practices that are designed to help ensure that new employees are qualified for their job responsibilities. All applicants pass through an interview process that assesses their qualifications related to the expected responsibility level of the individual. MARQUIS conducts pre-employment reference checks from information provided on the employment application. Additionally, HR conducts pre-hire background investigations relating to past employment history, credit history, and criminal activity in accordance with the Fair Credit Reporting Act (FCRA).

MARQUIS invests significant resources in employee development by providing on-the-job training and other learning opportunities. New employees participate in an orientation program that acquaints them with the Company’s organization, its affiliated companies, functions, values, products, and selected policies. Thereafter, development activities include providing more challenging assignments, job rotation, training programs, seminars, and continuing education programs. Additionally, employees are provided with measurable objectives and are subject to periodic performance reviews to help ensure competence.

**Security Awareness**

MARQUIS conducts security training programs for all employees in the areas of physical safety and security. Each member of MARQUIS is made aware of the security implications that revolve around their functions and actions. Approaching security as an organization has a more profound effect than relying solely on a single group. This process begins with providing individuals with the understanding and knowledge needed to help secure them and
their data within established policies. Security awareness programs include the message that individual users can have a significant impact on the overall security of an organization.

Managers oversee the training and awareness of the topics contained in the Employee Handbook and the Client Security Policy:

- Computer and Email Usage
- Use of Telephones
- Use of Equipment
- Internet Usage Summary Policy
- Computer Software
- Personal Use of Company Property
- Property and Equipment Care
- Restricted Areas
- Return of Company Property
- Safety Rules
- Security Violations of Policies

Audit

MARQUIS' management performs periodic audits of procedures and holds scheduled compliance meetings with staff to review current and new procedures. Auditing is implemented on all systems, where possible, to track a variety of events including but not limited to security access violations and database access.

Risk Assessment

MARQUIS has a cross functional risk assessment process that utilizes management, as well as staff, to identify risks that could affect the MARQUIS’ ability to meet its contractual obligations. Risk assessment efforts include analyses of threats, probabilities of occurrence, potential business impacts, and associated mitigation plans. Risk mitigation strategies include prevention and elimination through the implementation of internal controls and transference through commercial general and umbrella policies. Management maintains risk plans and updates them at least annually.

Team leaders are required to identify significant risks related to their areas of responsibility and implement measures to mitigate those risks. The management team, including the Chief Executive Officer, Chief Operating Officer, and the Vice President of Information Systems, meets regularly to identify any risks and develop corrective steps to minimize the impact of these risks. The Company employs numerous methods to assess and manage risk, including policies, procedures, team structure, recurring meetings, and automated error detection controls. The Company strives to identify and prevent risks at an early stage through policy and procedure adherence in addition to mitigating relevant risks as discovered either through team structure, meetings, or notifications.

The Company maintains security policies and communicates them to staff to ensure that individuals utilizing Company resources understand their responsibility in reducing the risk of compromise and exercise appropriate security measures to protect systems and data.

Monitoring

Management monitors internal controls as part of normal business operations. MARQUIS uses a series of management reports and processes to monitor the results of the various business processes. The management team regularly reviews the reports and logs, records, and resolves all exceptions to normal processing activities.
The Company uses software to track user and customer requests, which are maintained in a system and tracked until completion. Management performs regular reviews of tasks assigned to their departments/divisions units. Tasks that are not addressed in a timely manner are manually escalated and resolved.

The Company’s Information Technology team regularly monitors the network for capacity, performance, and hardware failure. Overall system health and capacity planning are monitored daily to ensure the system will meet the needs of the Company’s clients. Administrators monitor security access violations, including server logs and reports.

Monitoring policies and procedures are utilized for addressing issues relating to outages of critical services or other issues needing immediate action. These procedures vary based on the defined severity level of the problem.

Company administrators use several monitoring tools to identify and provide alerts to the following conditions:

- A managed system has exceeded a predefined performance or load threshold.
- A managed system has suffered an error condition.
- A managed system has detected a hardware element that is expected to fail in the near future.
- A managed system is no longer in communication with the monitoring infrastructure.
- A managed system has entered a condition previously specified by Company administrators as operating outside of a threshold.

Systems Administration utilizes a Web-based resource for performing external vulnerability testing. The assessment includes testing for current and recent known threats against the Company’s external-facing Internet firewalls. The testing verifies the configuration of the security policy on the firewall. Detailed reports are delivered upon completion for administrators to act upon if a vulnerability is discovered.

Information and Communication

MARQUIS uses a variety of methods for communication to ensure that significant events and issues are conveyed in a timely manner and that staff understand their role and responsibility over service and controls. These methods include the following: new hire training, ongoing training, policy and process updates, weekly departmental meetings summarizing events and changes, use of email and paging to communicate time sensitive information, and the documentation and storage of historical data in internal repositories for business and support activities. The Company maintains systems that manage the flow of information and facilitate communication with its customers.

MARQUIS has implemented various methods of communication to help ensure that employees understand their individual roles and responsibilities over processing and controls and communicate significant events in a timely manner. Employee manuals are provided upon hire that communicate all relevant policies and procedures concerning employee conduct. Security of the physical premises and logical security of systems is reinforced by training and through awareness programs. The communication system between senior management and operations staff includes the use of the office email system, written memos when appropriate, and weekly meetings. Periodic department meetings between each manager and their staff are held to discuss new Company policies and procedures and other business issues. Monthly staff and training meetings are utilized to inform staff of new policy and technology updates. Communication is encouraged at all levels to promote the operating efficiency of MARQUIS.

Trust Services Criteria and Related Controls

The Company’s trust services criteria and related control activities are included in Section III of this report to eliminate the redundancy that would result from listing them here in Section II and repeating them in Section III.
Although the trust services criteria and related control activities are included in Section III, they are, nevertheless, an integral part of Company’s description of controls.

User Control Considerations

The Company’s applications are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report.

This section describes additional controls that should be in operation at user organizations to complement the controls at the Company. User auditors should consider whether or not the following controls have been placed in operation at the user organizations:

- Controls are in place for user organizations to ensure compliance with contractual requirements.
- Controls are in place to ensure that user organizations adopt strong operating system and application password management procedures, including using passwords that cannot be easily compromised and require to change on a regular basis.
- Controls are in place to provide reasonable assurance of the compatibility of software not provided by Company.
- Controls to provide reasonable assurance that the customer has procedures in place for developing, maintaining and testing their own business continuity plans (BCP).
- Controls to provide reasonable assurance that Company IT is notified in advance of any equipment or other shipments they will be sending or receiving.
- Controls to provide reasonable assurance of the transmission and receipt of information not provided by Company.
- Controls for approving the telecommunications infrastructure between itself and Company.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Processing of transactions for customers by Company covers only a portion of the overall internal control structure of each customer. The Company products and services were not designed to be the only control component in the internal control environment. Additional control procedures are required to be implemented at the customer level. It is not feasible for all of the control objectives relating to the processing of transactions to be completely achieved by Company. Therefore, each customer’s system of internal controls must be evaluated in conjunction with the internal control structure described in this report.
III. Information Provided by Auditwerx
## Security Principle

### Control Objective 1 – Policies

**CO1 – MARQUIS defines and documents its policies for the security of its systems.**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>MARQUIS’ security policies are established and periodically reviewed and approved by a designated individual or group.</td>
<td>MARQUIS’ information security policy addresses both IT and physical security, and it is reviewed and approved annually by the Systems Administrator, Vice President, and President.</td>
<td>Inspected the security policies to ascertain that procedures governing IT and physical security for the in-scope technology and locations were included.</td>
</tr>
<tr>
<td>1.2</td>
<td>MARQUIS’ security policies include, but may not be limited to, the following matters:</td>
<td>MARQUIS’ security policies address the following:</td>
<td>Inspected documentation for annual IT and physical security review by the Systems Administrator, Vice President, and President.</td>
</tr>
<tr>
<td>a.</td>
<td>Identifying and documenting the security requirements of authorized users.</td>
<td>Identifying and documenting the security requirements of authorized users.</td>
<td>Inspected the security policies to ascertain they included the matters specified.</td>
</tr>
<tr>
<td>b.</td>
<td>Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements.</td>
<td>Classifying data based on its criticality and sensitivity and using the assigned classification to define protection requirements, access rights and access restrictions, and retention and destruction requirements.</td>
<td>Inspected the security policies to ascertain they included the matters specified.</td>
</tr>
</tbody>
</table>
Control Objective 1 – Policies (Continued)

CO1 – MARQUIS defines and documents its policies for the security of its systems.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Assessing risks on a periodic basis.</td>
<td>Assessing risk on a periodic basis.</td>
<td>Inspected the security policies to ascertain they included the matters specified.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>d. Preventing unauthorized access.</td>
<td>Preventing unauthorized access.</td>
<td>Inspected the security policies to ascertain they included the matters specified.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access.</td>
<td>Adding new users, modifying the access levels of existing users, and removing users who no longer need access.</td>
<td>Inspected the security policies to ascertain they included the matters specified.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>f. Assigning responsibility and accountability for system security.</td>
<td>Assigning responsibility and accountability for confidentiality and related security.</td>
<td>Inspected the security policies to ascertain they included the matters specified.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>g. Assigning responsibility and accountability for system changes and maintenance.</td>
<td>Assigning responsibility and accountability for system changes and maintenance.</td>
<td>Inspected the security policies to ascertain they included the matters specified.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>h. Testing, evaluating, and authorizing system components before implementation.</td>
<td>Testing, evaluating, and authorizing system components before implementation.</td>
<td>Inspected the security policies to ascertain they included the matters specified.</td>
<td>No exceptions noted.</td>
</tr>
</tbody>
</table>
### Control Objective 1 – Policies (Continued)

**CO1 – MARQUIS defines and documents its policies for the security of its systems.**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2 i. Addressing how complaints and requests relating to security issues are resolved.</td>
<td>Addressing how complaints and requests relating to confidentiality and related security issues are resolved.</td>
<td>Inspected the security policies to ascertain they included the matters specified.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>j. Identifying and mitigating security breaches and other incidents.</td>
<td>Handling confidentiality and related security breaches and other incidents.</td>
<td>Inspected the security policies to ascertain they included the matters specified.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>k. Providing for training and other resources to support its system security policies.</td>
<td>Providing for training and other resources to support its system confidentiality and related security policies.</td>
<td>Inspected the security policies to ascertain they included the matters specified.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>l. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.</td>
<td>Providing for the handling of exceptions and situations not specifically addressed in its system security policies.</td>
<td>Inspected the security policies to ascertain they included the matters specified.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>m. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.</td>
<td>Providing for the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.</td>
<td>Inspected the security policies to ascertain they included the matters specified.</td>
<td>No exceptions noted.</td>
</tr>
</tbody>
</table>
Control Objective 1 – Policies (Continued)

CO1 – MARQUIS defines and documents its policies for the security of its systems.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>n. Providing for sharing information with third parties.</td>
<td>Providing for sharing information with third parties.</td>
<td>Inspected the security policies to ascertain they included the matters specified.</td>
</tr>
<tr>
<td>1.3</td>
<td>Responsibility and accountability for developing and maintaining MARQUIS’ system security policies, and changes and updates to those policies, are assigned.</td>
<td>MARQUIS assigns responsibility and accountability for developing and maintaining system security policies to the Security Officer.</td>
<td>Inspected the job descriptions for members of the security administration team to determine whether the description identified the responsibilities of the security administration team for the maintenance and enforcement of the organization’s security policy.</td>
</tr>
</tbody>
</table>
## Control Objective 2 – Communications

**CO2 – MARQUIS communicates its defined system security policies to responsible parties and authorized users.**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1  MARQUIS has prepared an objective description of the system and its boundaries and communicated such description to authorized users.</td>
<td>MARQUIS provides a description of its system, system boundaries, and system processes that includes infrastructure, software, people, and procedures to those people who request it.</td>
<td>Inspected published descriptions of MARQUIS’ system, system boundaries, and system processes to determine whether the description addressed infrastructure, software, people, procedures, and data for the in-scope technology and locations.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>2.2   The security obligations of users and MARQUIS’ security commitments to users are communicated to authorized users.</td>
<td>MARQUIS provides ongoing security training to its employees through department meetings and/or emailed instructions. The Company’s IT employees are required to annually sign and acknowledge their review of the information security policy. The Company’s policies relating to security are reviewed with new employees as part of their orientation, and new employees are required to sign and acknowledge their review of the employee handbook.</td>
<td>Inspected sample of the security meeting minutes to determine whether employees received ongoing security training. For a sample of IT employees, inspected their employee acknowledgements to determine the employees acknowledged their review of the information security policy. For a sample of newly hired employees, inspected the new hire employee acknowledgement forms to determine they signed and acknowledged their review of the employee manual, which included the security policies.</td>
<td>No exceptions noted. No exceptions noted. No exceptions noted.</td>
</tr>
</tbody>
</table>
**Control Objective 2 – Communications (Continued)**

**CO2 – MARQUIS communicates its defined system security policies to responsible parties and authorized users.**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3 Responsibility and accountability for MARQUIS’ system security policies and changes and updates to those policies are communicated to Company personnel responsible for implementing them.</td>
<td>Written job descriptions have been defined and communicated to the security administration team.</td>
<td>Inspected the job descriptions for the members of the security administration team to determine the description indicated that the security administration team was responsible for the custody and maintenance of the organization’s security policy.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>2.4 The process for informing MARQUIS about breaches of the system security and for submitting complaints is communicated to authorized users.</td>
<td>MARQUIS’ security awareness program trains employees how to identify and report possible security breaches.</td>
<td>Inspected the security training meeting minutes and determined whether that material described how to identify and report possible security breaches.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>System alerts, including planned outages and known issues, are communicated via email.</td>
<td>Inspected a selected system alert email to determine system alerts are communicated to system users.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>2.5 Changes that may affect system security are communicated to management and users who will be affected.</td>
<td>Planned changes to system components are reviewed, scheduled, and communicated to management as part of the weekly IT maintenance process.</td>
<td>Inspected a sample of weekly IT maintenance schedules and communications to determine planned system changes were included and reviewed and signed off by IT management.</td>
<td>No exceptions noted.</td>
</tr>
</tbody>
</table>
Control Objective 3 – Procedures

**CO3 – MARQUIS placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
</table>
| 3.1 Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. | A Company-wide risk assessment is performed annually by management includes the following:  
- Determining business objectives including security commitments  
- Evaluating the effect of environmental, regulatory, and technological changes on MARQUIS’ system security  
- Identifying threats to operations, including security threats, using information technology asset records  
- Analyzing risks associated with the threats  
- Determining a risk mitigation strategy  
- Developing or modifying and deploying controls consistent with the risk mitigation strategy | Inspected the annual risk assessment documentation to determine it included the specified procedures. | No exceptions noted. |
| 3.2 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: | Access to MARQUIS’ Network is restricted through the use of defined application and database user roles.  
Access granted to users is authorized by the department manager, VP of Product Development or Executive Team. | Inspected user access for a sample of users and determined access was authorized and consistent with their role.  
Inspected Active Directory administrative access granted to authorized individuals. | No exceptions noted. |
| a. Logical access security measures to restrict access to information resources not deemed to be public. | | | |
Control Objective 3 – Procedures (Continued)

CO3 – MARQUIS placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2 a. Logical access security measures to restrict access to information resources not deemed to be public. (Continued)</td>
<td>MARQUIS user role assignments are reviewed by department manager, VP of Product Development or Executive Team monthly.</td>
<td>Inspected a sample of user access reviews noting the review was performed monthly.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>3.2 b. Identification and authentication of users.</td>
<td>Unique user identification numbers, names, and passwords are required to authenticate all users to MARQUIS’ network. Password parameters consist of the following:  - Passwords have a minimum of eight characters including one nonalphanumeric character.  - Passwords expire every 120 days.  - Logon sessions terminate after five failed attempts.  - An expired password cannot be recycled for twelve (12) months.</td>
<td>Inspected the password parameters for the system to determine the password parameters were configured with the following specifications:  - Passwords have a minimum of eight characters including one nonalphanumeric character.  - Passwords expire every 120 days  - Logon sessions terminate after five failed attempts.  - The passwords cannot be reused for twelve (12) months.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>3.2 c. Registration and authorization of new users.</td>
<td>In order for the MARQUIS’ employees to obtain network access, the department manager must submit a help desk ticket authorizing such access. Proper segregation of duties is considered in granting access privileges based on the user’s job role.</td>
<td>Inspected the user access requests for a sample of employees requiring access to the system to determine whether access was authorized and provided for the proper segregation of duties.</td>
<td>No exceptions noted.</td>
</tr>
</tbody>
</table>
Control Objective 3 – Procedures (Continued)

CO3 – MARQUIS placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>d. The process to make changes and updates to user profiles.</td>
<td>Only authorized Company personnel are able to create or modify user access and user access privileges. The human resources department provides IT personnel with a termination checklist after termination. IT reconciles the report against current system privileges to determine if access has been appropriately removed or disabled.</td>
<td>Inspected a report identifying individuals with access to create or modify user access privileges to determine the access was limited to authorized personnel. Inspected a sample of termination checklists and user accounts to determine user access was appropriately removed or disabled.</td>
</tr>
<tr>
<td>e. Distribution of output restricted to authorized users.</td>
<td>Clients accessing the client FTP portal can only view reports for their assigned directory. Administrative access to FTP portal is restricted to authorized personnel.</td>
<td>Inspected FTP system configuration to determine that user access is restricted to assigned directories and administrative access to assign user privileges is restricted to authorized personnel.</td>
<td>No exceptions noted.</td>
</tr>
</tbody>
</table>
Control Objective 3 – Procedures (Continued)

CO3 – MARQUIS placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>f. Restriction of access to offline storage, backup data, systems, and media.</td>
<td>The Company restricts access to offline storage, backup data, systems, and media to authorized individuals. Data and media are backed up to an encrypted hard drive that is password protected and secured in a locked case offsite.</td>
<td>Inspected the backup encryption configuration to determine access to data is restricted to authorized individuals.</td>
</tr>
<tr>
<td></td>
<td>g. Restriction of access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (e.g., firewalls).</td>
<td>Administrative access to the MARQUIS’ firewall is restricted to the System Administrator. All firewall configuration changes are logged by the Company’s security incident and event management (SIEM) utility and are reviewed by the security administration team. Administrative access to Active Directory servers and databases is restricted to authorized personnel. A list of all master passwords is maintained in a password-encrypted database.</td>
<td>Inspected the firewall system configuration and access listing to determine access was restricted to authorized personnel and changes were logged. Inspected the Active Directory and servers’ access listings to determine access was restricted to authorized personnel. Inspected the database configurations to determine master passwords were maintained in an encrypted database.</td>
</tr>
</tbody>
</table>
Control Objective 3 – Procedures (Continued)

CO3 – MARQUIS placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3</td>
<td>Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.</td>
<td>Physical access to the data centers that house the MARQUIS’ IT resources, servers, backup media, and related hardware, such as firewalls and routers, is restricted to authorized individuals by card key systems. Requests for physical access privileges to the Company’s computer facilities require approval from authorized IT management personnel. Documented procedures exist for the identification and escalation of potential physical security breaches.</td>
<td>Inspected key card system user listing to the data center to determine key card systems restricted access to authorized individuals. There were no new users granted access during the audit period. Inspected written security policies and ascertained the policies addressed the identification and escalation of potential physical security breaches.</td>
</tr>
</tbody>
</table>
### Control Objective 3 – Procedures (Continued)

**CO3 – MARQUIS placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4</td>
<td>Procedures exist to protect against unauthorized access to system resources.</td>
<td>Virtual private networking (VPN) software is used to restrict remote access. Users are authenticated by the VPN server through user identification names, and passwords, and a preshared key. &lt;br&gt; MARQUIS uses firewalls to prevent unauthorized network access. &lt;br&gt; The Company contracts with third-party security providers to conduct quarterly security reviews and vulnerability assessments. Results and recommendations are communicated to and addressed by management.</td>
<td>Inspected the VPN configurations to determine user identification numbers, names, and passwords were required. &lt;br&gt; Inspected the network diagram to determine the design of the system included firewalls to prevent unauthorized network access. &lt;br&gt; For a sample of months, inspected the security review and vulnerability assessment reports to determine the assessments were performed and communicated.</td>
</tr>
<tr>
<td>3.5</td>
<td>Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.</td>
<td>MARQUIS uses anti-virus software on all Windows-based desktops, laptops, and servers. These systems are configured to query the anti-virus repository daily to retrieve the latest antivirus definitions. &lt;br&gt; The Company uses a SIEM utility to identify and record any computer viruses identified on the Company’s network.</td>
<td>Inspected the anti-virus software configurations to determine the software was configured to retrieve the latest anti-virus definitions on a daily basis. &lt;br&gt; Observed the SIEM utility to determine management had recorded any identified computer viruses.</td>
</tr>
</tbody>
</table>
Control Objective 3 – Procedures (Continued)

CO3 – MARQUIS placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.6</td>
<td>Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.</td>
<td>MARQUIS’ employees have the ability to encrypt email attachments using a secure WinZip or PGP encryption. The MARQUIS’ remote access VPN uses Layer 2 Tunneling Protocol and Internet Protocol Security (L2TP IPSec) to encrypt all remote sessions.</td>
<td>Inspected system setting on the email server to determine emails could be encrypted when required. Inspected the VPN configurations to determine Layer 2 Tunneling Protocol and Internet Protocol Security (L2TP IPSec) encryption was used.</td>
</tr>
</tbody>
</table>

Criteria related to execution and incident management used to achieve objectives

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7</td>
<td>Procedures exist to identify, report, and act upon system security breaches and other incidents.</td>
<td>User entities are provided with instructions for communicating potential security breaches to the information security team. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures.</td>
<td>Inspected the instructions provided to user entities to determine they included protocols for communicating potential security breaches. Inspected the written incident management procedures to determine whether the procedures included a process for handling the security incident.</td>
</tr>
</tbody>
</table>
Control Objective 3 – Procedures (Continued)

CO3 – MARQUIS placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3.8</strong></td>
<td>Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.</td>
<td>MARQUIS has a defined information classification scheme for the labeling and handling of data. The Company classifies data into two levels: Public and Sensitive Data.</td>
<td>Inspected the data classification policy to determine there was a documented classification scheme for labeling and handling data.</td>
</tr>
<tr>
<td><strong>3.9</strong></td>
<td>Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.</td>
<td>Security incidents are reported to Executive Team and follow the Incident Response Policy. Employees found to be in violation of MARQUIS’ information security policy are subject to disciplinary action up to and including termination of employment.</td>
<td>There were no security incidents during the audit period. Inspected the security policy to determine the policy included procedures for employees in violation of the policy.</td>
</tr>
<tr>
<td><strong>3.10</strong></td>
<td>Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.</td>
<td>MARQUIS has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.</td>
<td>Inspected the security and systems development methodology policy to determine it included project planning, design, testing, implementation, maintenance, and disposal or decommissioning.</td>
</tr>
</tbody>
</table>
Control Objective 3 – Procedures (Continued)

**CO3** – **MARQUIS placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.11</td>
<td>Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.</td>
<td>MARQUIS has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions. Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the candidate’s credentials are commensurate with the position. New personnel are offered employment subject to background checks.</td>
<td>For a sample of positions, inspected written job descriptions to determine the job descriptions included responsibilities and academic and professional requirements. For a sample of new employees, inspected the results of background checks to determine a background check was performed.</td>
</tr>
</tbody>
</table>

No exceptions noted.
Control Objective 3 – Procedures (Continued)

**CO3** – MARQUIS placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change management-related criteria applicable to the system's security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.12</td>
<td>Procedures exist to maintain system components, including configurations consistent with the defined system security policies.</td>
<td>MARQUIS maintains a documented change management and patch management process. Servers are reviewed monthly by the security administration team to determine if required vendor security patches have been applied. The Company contracts with third parties to conduct quarterly security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management. Management develops a plan for action for each recommendation and follows up on open recommendations on a regular basis.</td>
<td>Inspected the change and patch management policies to determine there were documented procedures. For a sample of months, inspected management’s server review documentation to determine the security patches were applied. For a sample of months, inspected the security review and vulnerability assessment reports to determine the assessments were performed, communicated, and addressed by management.</td>
</tr>
</tbody>
</table>
Control Objective 3 – Procedures (Continued)

CO3 – MARQUIS placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.13  Procedures exist to provide that only authorized, tested, and documented changes are made to the system.</td>
<td>MARQUIS maintains a formally documented change management process. Changes to hardware, operating system, and system software are authorized, tested (when applicable), and approved by appropriate personnel prior to implementation. Changes in system infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments.</td>
<td>Inspected the change management policy for hardware, operating system, and system software to determine procedures were documented to include authorization, tested (when applicable), and approved prior to implementation. Inspected documentation of the system infrastructure architecture to determine a separate development or test environment existed from the production environment. Inspected the access list to the change management tools to determine access to migrate changes to production was appropriate based on job responsibilities and that developers did not have the ability to migrate changes into production.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>3.14  Procedures exist to provide that emergency changes are documented and authorized timely.</td>
<td>Emergency changes follow the standard change management process, but at an accelerated timeline. Prior to initiating an emergency change, all necessary approvals are obtained and documented.</td>
<td>There were no emergency changes during the audit period.</td>
<td>No testing performed.</td>
</tr>
</tbody>
</table>
**Control Objective 4 – Monitoring**

*CO4 – MARQUIS monitors the system and takes action to maintain compliance with its defined system security policies.*

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Tests Performed</th>
<th>Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>MARQUIS’ system security is periodically reviewed and compared with the defined system security policies.</td>
<td>External vulnerability assessments are performed on a monthly basis, and management initiates corrective actions for identified vulnerabilities. MARQUIS performs monthly user access reviews.</td>
<td>Inspected a sample of vulnerability assessments noting monthly performance. Obtained a sample of monthly user access reviews, noting review by management.</td>
</tr>
</tbody>
</table>
| 4.2      | There is a process to identify and address potential impairments to MARQUIS’ ongoing ability to achieve its objectives in accordance with its defined system security policies. | MARQUIS uses a SIEM utility to capture the following critical security events:  
- Daily intrusion detection system (IDS) or intrusion prevention system (IPS) attacks  
- Critical IDS or IPS alerts  
- Servers not reporting in the past 15 minutes  
- Firewall configuration changes  
Reports are logged and reviewed by the systems administrator. | Selected a sample of SIEM logs, noting capture of critical security events and monitoring reports are available to systems administrator. | No exceptions noted. |