The Seibels Group, Inc.

Independent Service Auditor's Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy on the Insurance Servicing Operations and Supporting Information Technology General Control System (SOC 3)

For the period January 1, 2019 to November 30, 2019

An Independent Service Auditor Report issued by
Dixon Hughes Goodman LLP

table of contents

This report, including the description of tests of controls and results thereof, is intended solely for the information and use of the Company; user entities of the Company's system during some or all of the specified period and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding. This report is not intended to be, and should not be, used by anyone other than these specified parties.

DIXON HUGHES GOODMAN LLP

section I: independent service auditor's report

To: Management of Seibels
Columbia, South Carolina

Scope

We have examined Seibels' accompanying assertion titled "Management's Assertion" (assertion) that the controls within its Insurance Servicing Operations and Supporting Information Technology General Control system (system) were effective throughout the period January 1, 2019, to November 30, 2019, to provide reasonable assurance that Seibels' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

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

Seibels uses subservice organizations to provide certain hosting and information technology functions. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Seibels, to achieve Seibels' service commitments and system requirements based on the applicable trust services criteria. The description presents Seibels' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Seibels' controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Seibels is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Seibels' service commitments and system requirements were achieved. Seibels has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Seibels is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

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

DIXON HUGHES GOODMAN LLP

Our examination included:

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

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

Inherent Limitations

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

Opinion

In our opinion, management's assertion that the controls within Seibels' Insurance Servicing Operations and Supporting Information Technology General Control system (system) were effective throughout the period January 1, 2019, to November 30, 2019, to provide reasonable assurance that Seibels' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Dixon Hughes Goodman LLP

Greenville, South Carolina

January 31, 2020

section II: management's assertion

Seibels' Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Seibels' Insurance Servicing Operations and Supporting Information Technology General Control system (system) throughout the period January 1, 2019, to November 30, 2019, to provide reasonable assurance that Seibels' service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented in Section Three and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2019, to November 30, 2019, to provide reasonable assurance that Seibels' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria). Seibels' objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section Three.

Seibels uses subservice organizations to provide certain information technology and data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Seibels, to achieve Seibels' service commitments and system requirements based on the applicable trust services criteria. The description presents Seibels' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Seibels' controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Seibels, to achieve Seibels' service commitments and system requirements based on the applicable trust services criteria. The description presents Seibels' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Seibels' controls.

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

We assert that the controls within the system were effective throughout the period January 1, 2019, to November 30, 2019, to provide reasonable assurance that Seibels' service commitments and system requirements were achieved based on the applicable trust services criteria.

The Seibels Group, Inc.

section III: management's description of its system and controls

Overview of Operations

Profile

Seibels (or the "Company") is a provider of processing, technology, and claims solutions to the property and casualty insurance industry. Tracing its roots to 1869, Seibels understands the value of insurance management services. Bolstered by its heritage, stability, innovative technologies, experienced insurance professionals, and customer focus, Seibels strives to meet and exceed clients' expectations.

Products and Services

Seibels is a leading insurance services provider of managed processing solutions, including Business Process Outsourcing, Information Technology Outsourcing, Claims Services, and Professional Services. Through its subsidiaries, Seibels conducts its operations from service centers located in Columbia, South Carolina and Altamonte Springs, Florida.

Seibels Processing Solutions, Inc.

With decades of experience in providing Business Process Outsourcing and application services, Seibels has developed specialized knowledge and skills that enable the identification and implementation of new ideas and technologies specifically suited to clients' needs. Seibels is committed to fostering a culture of partnership and flexibility in client relationships. With a combination of insurance experience and technology expertise, Seibels provides the following tailored Business Process Outsourcing solutions:

- Policy Administration
- Rating and Underwriting
- Billing and Collections
- Accounting and Reporting
- Financial Services
- Marketing Assistance
- Customer Service Centers with bilingual English and Spanish speaking staff available 24/7

Seibels Technology Solutions, Inc.

Seibels' information technology outsourcing instantly raises a company's IT level, helps reduce costs, and provides access to new technology. Seibels provides Managed Application Hosting, Corporate Web Hosting, and delivers Remote Application Support, all of which are hosted in a secure data center. Managed systems include web-based policy and claims administration, First Notice of Loss (FNOL) reporting, and claims management.

Seibels develops web-based, scalable systems based on modern technology platforms. Systems are engineered in compliance with industry standards and supported by a secure infrastructure. Seibels Technology Solutions provides full policy-life-cycle support, efficient installation capabilities, and a base system complete with Policy Administration, Billing, Claims Management, Agent Portal, and Reporting. Systems include: IPX Enterprise Insurance Suite, iSeries SIPS, UnderwritingXpert, Claims Processing Xpert (CPX) Claims Management System, Guidewire Suite, and FNOL software.

From comprehensive product maintenance and support to assistance in managing processing environments, Seibels also offers an array of Professional Services designed to meet customer's needs. Founded on proven methodologies, Seibels' Professional Services include:

- Planning
- Integration
- Installation
- Testing
- Modification
- Training

Seibels Claims Solutions, Inc.

Seibels' full-service claims organization offers the property and casualty insurance industry total claims administration. Seibels Claims Solutions works to simplify the claims handling experience, improve loss ratios and customer service, and decrease loss adjusting expenses. Seibels Claims Solutions provides the following services:

- Business Process Outsourcing
- Third Party Administration
- First Notice of Loss Call Center Services
- Catastrophe (CAT) Management
- SIU/Subro/Salvage Services
- Litigation Services
- Re-inspection Services

Seibels' Claims Administration Services are customizable based on a company's needs. From FNOL to full claims administration, Seibels provides companies with a tailored solution. Claims Administration Services include centralized claim intake twenty-four hours a day, seven days a week. Upon notification by phone, fax, or email, claim assignments are quickly processed and electronically routed to the appropriate adjuster or mitigation service. The total claim management program coordinates call intake and claim triage, field assignment and management of the claim process, and review of field work. Claims services also provides complete tracking, review and reporting of reserves, payments, expenses, salvage, and subrogation activities. In the case of a catastrophe, Seibels also provides CAT Management services including planning and preparation, FNOL services, file examination, and a network of CAT adjusting companies.

Organizational Structure

Seibels operates under the direction of its President and Chief Executive Officer, along with senior executives that serve as heads of the business units described above. All areas are led by capable, experienced and well-qualified individuals with years of experience applicable to their respective job responsibilities. Executives provide oversight of business units and are directly involved in Seibels operations.

The Accounting Department is comprised of four primary units: Payment Processing, Receivable Accounting, Client Accounting, and Seibels Accounting Services. While each of these units has its own specific functions, there are several duties that are shared between them.

The Premium Processing department is responsible for processing all cash received into the systems, reviewing premium refunds prior to mailing, preparing deposits for delivery to the bank and ensuring that corresponding journal entry sheets are submitted for general ledger entry in a timely manner. The unit is also responsible for daily cash balancing routines, as well as, the processing of not sufficient funds (NSF) checks, voids, and stop payment requests. In addition, the unit performs a significant amount of customer service type duties that involve periodic communication with agents and insureds.

The Receivable Accounting department manages the reconciliation of and controls over premium receivables, including maintenance and management of bad debt reserves, and the monthly agent commission reporting process. These duties also extend to include certain customer service functions, requiring direct communication with insureds and agents. This unit also serves as Seibels subrogation and related collections department and assists SCS with adjuster invoice entry in CPX and the systems, along with the associated reconciliation of adjuster expense with contractual catastrophe override commissions.

The Client Accounting Services department (CAS) is responsible for the accounting and reporting of its customers, in accordance with both Statutory Accounting Principles and Generally Accepted Accounting Principles. This includes the accounting and reporting for the statistical operations of the insurance companies, accounting for and reporting on the provisions of in force and runoff reinsurance treaties and preparing quarterly and annual financial statements. This unit prepares all premium tax and municipal returns, as well as a variety of state and industry reports for the National Association of Insurance Commissioner (NAIC) and state departments of insurance.

This unit is also responsible for the maintenance of a relational database general ledger system, preparation of monthly account reconciliation notebooks, and monthly consolidating internal financial statements. Additional responsibilities include the administration of accounts payable, bank reconciliations, fixed asset accounting, and certain treasury processes, as requested.

Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Information and Communication

Management and the Board of Directors instill a philosophy that enables all employees to share in Seibels successes and ultimate growth. The Board of Directors is responsible for determining a strategic vision and direction for the Company and management is charged with operating the Company to achieve those goals. Seibels' management team is comprised of a well-skilled and diverse group of individuals who interact regularly. Management is also responsible for establishing corporate policy and addressing all operational, financial, cultural, and social aspects of the Company. Employees function as vital components in the building and shaping of the Company, and along with management, are always expected to exhibit high ethical standards .

Control Environment

The control environment sets a tone throughout the organization, influencing the control consciousness of its people. It is the foundation for all other components of the internal control structure, providing discipline and structure.

Ethical Values

Seibels' fundamental principles and ethical values are documented in its Employee Handbook and communicated to all employees through Company-wide meetings hosted by the President, as well as, departmental meetings between employees and supervisors. All employees are required to read and comply with the Employee Handbook, which is available 24x7x52 on the Company's intranet.

Hiring

The Human Resources department is primarily responsible for the recruiting and hiring process. Consistent and thorough hiring standards are adhered to throughout all levels of the organization. All personnel are subject to various background checks (e.g., reference checks, work history checks, credit checks, criminal history checks, and drug tests). Written performance reviews are performed at 90 days for new employees and on an annual basis thereafter. In addition, various in-house training programs are offered to supplement current knowledge levels.

Risk Assessment

Seibels recognizes that risk management is a critical component of internal controls affecting all levels of the organization. Management regularly assesses the risks of internal fraud and has taken measures to deter and prevent such actions from occurring. Management is also aware of the risks related to its information technology (IT) infrastructure, such as security, network operations, and disaster recovery.

A risk assessment is performed annually to ensure that data is accurately classified, vendors are adequately managed, and systems are secured appropriately.

Information and Communication

Management is committed to maintaining an environment of open communication with all employees. Updates on Company performance and other relevant matters are communicated in various ways, such as the Company's intranet, electronic mail distribution, meetings with managers, and other postings throughout the Company.

Confidentiality/Privacy

Documented policies exist pertaining to the confidentiality and privacy of customer data. During the course of business, Seibels collects and processes PII which is used for verification purposes. This includes, but is not limited to: SSN, DOB, DL#, and banking information. Seibels' Information Security Program (ISP) committees ensure user compliance by monitoring the handling of all customer and company confidential data according to ISP policies. DLP rules and secure email ensure data is transmitted securely. Remote access is encrypted as well as all data transmissions. Seibels ISP policies also require all paper documents be shredded when no longer needed or locked away securely when not in use. All system security access is role-based to ensure only authorized personnel have access to customer data.

Seibels Privacy Policy is posted on our company website and is updated as necessary. It provides our customers information regarding data collection, protection, and methods for modification or removal as well as contact information should they have concerns about how their PII data is handled. Note, there were no customer PII complaints in 2019. Seibels upholds our customers and vendors to the same privacy and confidentiality standards as our employees. Privacy commitments are outlined between Seibels and their customers through contractual agreement. Our vendors and contractors are vetted and obligated to sign NDAs.

As part of Seibels confidentiality and privacy compliance, employees and contractors undergo ISP training as part of their onboarding process and annual renewal is required as part of our users continuing education. Security Tips and notification emails are periodically sent to our staff as part of our ongoing ISP training, along with any phishing/malicious email alerts to make sure our users are vigilant in protecting our customers' data.

Monitoring

Seibels utilizes several monitoring techniques for effectively monitoring operational activities. Seibels maintains automated monitoring systems to ensure the system is operational and that adequate free disk storage is available. SQL Server automated maintenance jobs are used to regularly check database integrity, maintain indexes, and perform transaction log backups. All critical processing is monitored, and notification is sent to IT on-call personnel in the event of failure or message waiting status. There is IT staff on call 24x7x52 and any issues encountered are attended to and resolved as quickly as possible.

Relevant Applications

IPX

Supported Business Processes: Policy data is entered by agents, customers, or Company personnel, and subsequent transactional activity is generated and stored within IPX on a Windows operating environment. Transactional statistical data is also stored within IPX. During daily and monthly processing, summary reports are generated to ensure data integrity. If the summary reports do not balance, detail reports are utilized to identify the anomalies in the data.

Inbound Data Feeds: IPX data entry is real-time. Manual entry is entered by employees, customers, and agents daily. IPX automated nightly processing generates summary reports used to ensure data integrity.

Outbound Data Feeds: Outbound feeds are automated and run nightly. Databases are updated instantaneously, daily reports are generated, and data is sent using SFTP, email, etc. to Seibels' customers, agents, and third-party vendors.

Security: The system is administered by Seibels Technology Services (STS) under the direction of the business owner. End users gain access using standardized provisioning controls such as service request forms authorized by their manager for employees. Agent access is granted through their Insurance Marketing Department. IPX users have their own security and each user is assigned their own unique user ID which further defines their access through predefined teams and security groups. Segregation of duties is maintained between Application Development and Technology Services. User access is periodically reviewed for appropriateness.

Platform: IPX is a centralized computing system operating on a Microsoft Windows operating system. The primary system resides in the main Seibels' data center with replication to a cloud DR solution. The system is supported by Microsoft Windows using remote sessions. No other remote access is available on the system.

Software Architecture: IPX is an in-house maintained system written in .Net programing language. The system is maintained by Seibels' developers. Application additions and changes are moved from test environments to production using Visual Studio, a third-party software package.

SIPS

Supported Business Processes: Policy and claims data are entered by agents, customers, or Company personnel, and subsequent transactional activity is generated and stored within SIPS on the iSeries. Transactional statistical data is also stored within SIPS. During daily and monthly processing, summary reports are generated to ensure data integrity. If the summary reports do not balance, detail reports are utilized to identify the anomalies in

the data.

Inbound Data Feeds: SIPS data entry is both manual and automated. Manual entry is entered by employees daily. SIPS automated nightly processing uploads the data that were manually entered that day in other systems.

Outbound Data Feeds: Outbound feeds are automated and run nightly. Databases are updated, daily reports are generated, and data is sent using SFTP, email, etc. to Seibels' customers, agents, and third-party vendors.

Security: The system is administered by STS under the direction of the business owner. End users gain access using standardized provisioning controls such as service request forms authorized by their manager. There are several layers of security: SIPS has its own menu security and each user is assigned their own unique user ID which further defines their access through authorization and library lists. Segregation of duties is maintained between Application Development and Technology Services. User access is periodically reviewed for appropriateness. Remote access is available via VPN.

Platform: SIPS is a centralized computing system housed on the IBM iSeries, with OS400 as the operating system. The primary system resides in the main Seibels' data center with another IBM iSeries located at the Company's co-located data center in Spartanburg, SC. The system is supported by IBM using remote sessions. No other remote access is available on the system.

Software Architecture: SIPS is an in-house maintained system written in CL, COBOL, and RPG programing language. The system is maintained by Seibels' developers. Application additions and changes are moved from test environments to production using Implementer, a third-party software package.

Claims Processing Xpert (CPX)

Supported Business Processes: CPX manages the claims processing lifecycle, including first notice of loss, claims information gathering, communications, reserve, and payment requests. CPX interfaces with several other systems, including the policy administration module of the systems (SIPS and IPX) to retrieve and store policy coverage information, the document management system to store and retrieve policy and/or claims related documents, and to the systems to set reserves and make payments.

Inbound Data Feeds: Inbound data feeds are SIPS, IPX, manual input, ISO Web Service, Call Center Web Service, CSC, IA SFTP Docs, and Imaging System.

Outbound Data Feeds: Outbound data feeds are SIPS (automated night processing), IPX, manual input, ISO Web Service, Call Center Web Service, CSC, IA SFTP Docs, Imaging System, and Seibels' WebMail Web Service.

Security: The system uses a built-in role-based security and Microsoft Active Directory to present an appropriate user interface to the claims examiner, adjuster, supervisor, or customer that is logged into CPX.

Platform: CPX server components are housed on Windows Server 2003 and SQL 2005 servers residing in the main Seibels' data center. The CPX user interface runs on users' Windows 7 PCs. All CPX programs are developed to run on the Microsoft .NET Framework.

Software Architecture: CPX is an in-house developed application.

Guidewire Claims Processing

Supported Business Processes: Guidewire Claims manages the claims processing lifecycle, including first notice of loss (FNOL), claims information gathering, communications, reserve, and payment requests. Claim center includes loss-report intake, adjudication processes and management, and operational reporting. Guidewire Claims interfaces with several other systems, including the policy administration module of the Systems (SIPS and IPX) to

retrieve and store policy coverage information, the document management system (DMS) to store and retrieve policy and/or claims related documents, and to systems to set reserves and make payments.

Inbound Data Feeds: Inbound data feeds are IPX, manual input, ISO Web Service, Call Center Web Service, CSC, IA SFTP Docs, and Imaging System.

Outbound Data Feeds: Outbound data feeds are SIPS (automated night processing), IPX, manual input, ISO Web Service, Call Center Web Service, CSC, IA SFTP Docs, Imaging System, and Seibels' WebMail Web Service.

Security: The system uses a built-in role-based security and Microsoft Active Directory to present an appropriate user interface to the claims examiner, adjuster, supervisor, or customer that is logged into Guidewire Claims.

Platform: Guidewire Claims server components are housed on Windows Server 2012 and SQL 2012 servers residing in the main Seibels' data center. The Guidewire Claims user interface runs on users' Windows 7 & 10 PCs. All Guidewire Claim's programs are developed to run on the Microsoft .NET Framework & JAVA platforms.

Software Architecture: Guidewire Claims runs on the Guidewire Claims Version 8 system.

Guidewire

Supported Business Processes: Guidewire InsuranceSuite provides a single source for customer policy, transactional, and financial data. Policy Center is an underwriting, policy, and product management system supporting underwriters as they serve agents and policy holders. Billing Center is a billing and cash management system designed to enable insurers to deliver superior customer service, improve workflows and operational performance, and reduce total cost of operations. DataHub and InfoCenter provide consumable information for business intelligence, analysis, and enhanced decision-making. Consumer Portal allows customers to self-manage policy, claims, and personal information. ProducerEngage gives agents access to self-services tools and current policy, billing, and claims information so they can foster productive relationships with insurance carriers.

Inbound Data Feeds: Inbound data feeds originate from third party vendors, manual input, and web applications.

Outbound Data Feeds: Outbound data feeds include Guidewire Claims Center, OnBase, automated nightly jobs, and daily reports. Data is sent using SFTP, email, etc. to Seibels' customers, agents, and third-party vendors.

Security: The system uses built-in role-based security. Single Sign on is being designed for use with existing customer website and account security.

Platform: Guidewire server components are housed on Linux servers on a Kubernetes platform residing in the main Seibels' data center. The Guidewire user interface is web based.

Software Architecture: Guidewire runs on the Guidewire Insurance Suite Version 9 system.

Guidewire GWLive!

Supported Business Processes: Guidewire GWLive! is a cloud-based data warehousing solution for both Claim and Policy Center giving our customers the ability to slice data into segments making sense to day to day claim and policy management.

Inbound Data Feeds: Inbound data feeds are Claim Center, IPX, Policy Center, and SIPS.

Outbound Data Feeds: Outbound data feed is only to Guidewire GWLive!. Since this is a cloud-based data warehousing solution, no personally identifiable information is sent to Guidewire.

Security: For inbound feeds, the system uses a built-in role-based security and Microsoft Active Directory to securely extract data from customer systems into a staging database. For outbound feeds, it utilizes IP restriction

along with separate secure SFTP logins for each customer's data. Once in GWLive!, customer data is specifically limited to the roles granted to individual customers and secured via Guidewire's integration processes.

Platform: Guidewire GWLive! server components are housed on Windows Server 2012 and SQL 2012 servers residing in the main Seibels' data center. The Guidewire GWLive! user interface is web based since it is a cloud-based data warehousing system. All Guidewire GWLive! outbound components are Claim's programs are developed to run on the Microsoft .NET Framework & JAVA platforms.

Software Architecture: Guidewire GWLive! Claims runs on the Guidewire Claims Version 8 system; Policy Center runs on the Guidewire Policy Center Version 9 system.

UnderwritingXpert

Supported Business Processes: Once a policy is bound within the individual company web sites, UnderwritingXpert manages the underwriting process workflow. This system provides interfaces to manage a number of underwriting activities, including: underwriting referral processing, policy approval and declination, inspection ordering, loss history review and communications with agents and policy holders.

Inbound Data Feeds: Inbound data feeds are the Systems, manual input, imaging system, and web applications.

Outbound Data Feeds: Outbound data feeds are the Systems, manual input, and imaging system.

Security: The system uses a built-in role-based security and Microsoft Active Directory to present an appropriate user interface to the underwriter, supervisor, customer, or customer service representative (CSR) that is logged into UnderwritingXpert.

Platform: UnderwritingXpert server components are housed on Windows Server 2003 and SQL 2005 servers residing in the main Seibels' data center. The UnderwritingXpert user interface runs on users' individual Windows 7 PCs. All UnderwritingXpert components are developed to run on the Microsoft .NET Framework.

Software Architecture: UnderwritingXpert is an in-house developed application.

OnBase

Supported Business Processes: OnBase is Seibels' enterprise information platform used to manage all documents related to a customer policy. Workflows are designed to manage daily processing, approvals, and monitoring. The system is also used to manage all accounts payable workflow including invoice approval.

Inbound Data Feeds: Inbound data feeds are pulled from Email (Outlook and automated feeds), SFTP, Printer scans, and Windows file shares.

Outbound Data Feeds: There are no outbound data feeds, however IPX and Guidewire reference OnBase for all policy-related documentation.

Security: OnBase is integrated with Windows AD and has its own built-in security. Authority is granted and restricted through the System Manager based upon authority defined when user IDs are initially created. Accounts Payable invoice approval authority is limited to the manager level.

Platform: The system resides on Windows Servers 2012r2 and SQL 2012sp2 cu5 and is in the main Seibels' data center.

Software Architecture: OnBase is a third-party developed application.

Epicor

Supported Business Processes: Epicor is the Company's SQL-based general ledger system with real- time processing modules. Reconciliations and reporting are performed monthly to ensure data integrity.

Inbound Data Feeds: Inbound data feeds are the Systems manual input, Excel import files, and CSV import files (SFTP files from banking institutions).

Outbound Data Feeds: Outbound data feeds are Excel, Crystal Reports, and FRX.

Security: Epicor has its own built-in security. Authority is granted and restricted through the System Manager based upon authority defined when user IDs are initially created. Posting authority is limited to the manager level.

Platform: The system resides on a Windows Server 2012r2 and SQL 2012sp2 cu5 and is in the main Seibels' data center.

Software Architecture: Epicor is a third-party developed application.

Description of Relevant Controls

Governance Controls

Seibels' human resource policies and practices relate to employee hiring, orientation, evaluation, compensation, disciplinary activities, and (in some cases) third party vendor management.

Personnel Administration

New Employee Hiring Process

When a position is available, the supervisor submits a requisition to their manager and to human resources (HR) for approval. HR will place the job announcement on the Seibels' intranet and the Company website. HR will, if needed, run advertisements utilizing internet job websites, newspaper, and employment agencies. To be considered as a candidate for employment, the individual must provide a resume and/or complete an application for employment outlining employment history, education, references, position sought, and approval to run background checks. Applicants offered a position must submit to drug testing, criminal background check, and as applicable, a credit check. To assist in the hiring process, Seibels utilizes an orientation checklist to ensure all necessary steps in the application process are completed. Note that the results of the drug testing are kept separate from the personnel file if that applicant is ultimately hired.

After the application process, a formal offer letter is sent to the potential employee outlining the job being offered, the salary or wage as applicable, and any negotiated benefits. The applicant is typically asked to respond on or before five days following the date of the offer letter. Following acceptance of the offer, the new employee will then come to HR for general orientation. As part of this training, the new employee must review the employee handbook and sign a form acknowledging he or she received the handbook and agrees to comply with the rules and regulations contained within. They must also complete Information Security Program (ISP) training, and at the end of that training, they must sign a form acknowledging they received the training.

Employee Performance Evaluation

Most employees receive an annual performance evaluation, which is maintained in the Paylocity performance system. The evaluation is completed by the employee's direct manager or supervisor. Prior to the administration of the performance evaluation, it is typically reviewed by a second level manager and HR and is either approved or returned for correction. During the evaluation, the employee may add feedback/comments on the review. Upon

completion of the performance evaluation, it is electronically signed by the employee, the employee's direct manager or supervisor, the employee's second level manager, and HR.

Disciplinary Measures or Termination of Employment

Supervisors/managers are asked to discuss employee issues with an HR representative to determine the level of discipline needed. If a written document needs to be presented to an employee, the supervisors/managers are asked to submit the documentation through the Paylocity performance system to HR for review prior to discussing with the employee. Once approved by HR, the documentation is discussed with the employee outlining issues of concern and expectations for improvement going forward. The employee is asked to electronically sign the documentation acknowledging that it was discussed, and a copy of the document is given to the employee. In the event an employee refuses to electronically sign the document, the supervisor/manager notes it, and electronically signs it. Employees may submit a rebuttal to the document in the system. Depending upon the content of the rebuttal, additional discussions may occur between the employee and the supervisor/manager.

Involuntary terminations must be approved by the Director of HR. If a situation is so egregious (for example, violent behavior that could affect the safety of others), a manager may terminate the employee on the spot; however, this is only done in the event the situation needs an immediate action.

Third-Party Service Agreements

Seibels typically reviews third party service agreements annually prior to renewing. When they decide to put the service agreement out for proposal, Seibels requests proposals from at least two other service providers in addition to the existing service provider. As part of the proposal process, Seibels considers price, services to be provided, references, experience, quality of the proposal, and overall review of the company. A Microsoft Excel spreadsheet is prepared comparing the proposals and then a final decision is made based on the required criteria.

Organization and Administration

The IT department is divided into separate organizational elements to help verify business processes are executed in an efficient and effective manner and to maintain an adequate segregation of duties within organizational elements. Management has implemented a division of roles and responsibilities that limit the possibility for a single individual to subvert critical processes. There are policies and procedures in place to verify personnel perform only those duties related to their positions.

Management verifies position descriptions are used to delineate employee responsibilities. Authorities are established and updated as needed.

Communications

The customer service function is managed as a shared task within Technology Services using a dedicated phone system to receive and route incoming customer calls. All customer support personnel have dedicated monitors to identify and track calls to ensure minimal wait time. All calls are converted to trouble tickets using the Seibels Service Request application that routes tickets to the appropriate technical support personnel. All tickets are tracked through to proper resolution. Technology Services utilizes a suite of monitoring tools to provide proactive incident identification and response services.

General Information Technology Controls

Software and Infrastructure Changes

Systems development and maintenance, along with all change management activities, are enacted through a formal process in accordance with established change management policies. Hardware and software changes to existing systems must be approved by management and must align with the Company's business objectives and technology requirements. All infrastructure changes follow a process in which additions are logged using the Seibels Service Request (SR) system. All additions are inventoried and tagged with unique codes. Changes are tested where applicable prior to wide-spread deployment. Change Advisory Board (CAB) reviews are required for all production change approvals.

A software development lifecycle (SDLC) methodology is used to manage all application software changes. The methodology is used for large-scale projects, system enhancements, and break/fix changes. For each change, a formal request is created which is routed through to the appropriate stakeholders. All changes are documented, subjected to multiple levels of quality assurance testing, and can only be approved for production release via explicit sign-off from the business owner of the application. All application changes are moved into production by approved and authorized personnel in Information Technology, and only after all required approvals are obtained. Application developers do not have access to production libraries. Production libraries are maintained separately from development and test libraries. Change Advisory Board (CAB) reviews are required for all production change approvals.

System software patches are managed using a standard Microsoft Service. Patches are downloaded automatically and are deployed within the infrastructure after isolated testing is completed successfully. Patches are deployed during specified maintenance windows.

Physical Datacenter Access Controls

During the period under review, only the primary data center located in Columbia, South Carolina, was included in the testing. The tier 4 secondary data center located in Spartanburg, SC was considered out of scope.

Data pertaining to the Company's insurance transactions and those of its customers are housed at Segra in Columbia, South Carolina. Access to the server room is physically secured and entry is permitted by authorized personnel only. Company personnel are required to display their identity badges always when onsite at the facility. Access to the datacenter is via escort by a Segra employee, and access to Seibels' data is restricted to essential Seibels staff. Electromechanical locks are present at the one datacenter entrance and interior doors are unmarked. The datacenter door utilizes non-removable hinges and pick plates. Visitors to the datacenter must always sign a log and be escorted. Closed circuit video surveillance has been installed at all entrance points on the interior of the datacenter.

Logical Access

There are multiple controls used to secure the Company's IT environment. User IDs and passwords control access to systems. On web-based applications, the Company has implemented security requiring agency id, user name, and password to access the Point-of-Sale application, and, once logged-in, the Company has implemented role-based security. Each user is provided a unique user ID and password to gain system access and this password expires every 90 days.

Employee and contractor access to the network is managed via Active Directory. Active Directory security is configured to require strong passwords that must be changed periodically and are locked after multiple failed logon attempts. Access is granted for new user IDs via a documented access request process that requires proper

approval from the hiring manager. Policies and procedures ensure that Seibels employees and contractors have their access removed immediately upon termination.

Individual access to iSeries system applications and utilities is managed via iSeries security. On the iSeries, authorization lists are used to grant authority to individual menu options and functionalities per department. Change of library lists are used depending upon which item the user has chosen. This manipulation of library lists helps insure the user is only accessing data for which they have authority. The iSeries security is configured to require strong passwords that must be changed every 90 days and that are locked after multiple failed logon attempts. Periodic review of iSeries access is conducted to ensure all active accounts are valid and configured appropriately based on the individual's job function. Access is granted via a documented access request process that requires proper approval from the hiring manager. Policies and procedures ensure that Seibels employees and contractors have their access removed immediately upon termination.

Technology Services utilizes Sophos Enterprise Security and Control (Sophos), which provides a single, comprehensive virus management solution that works to prevent virus infections and automates the virus definition updating process. Sophos is used to scan desktops and servers within the infrastructure for viruses and infected files. Current virus signature updates are obtained through automated distributed update functionality which in turn is pushed out real-time to attached network servers and end-points.

Data Transmissions / Processing Integrity

Data transmissions are monitored using automated tools. Any interruptions in processing generate system alerts that are tracked and attended to immediately. Technology Services and IT On Call staff review cycle processing results, assuring all processing is completed accurately. Business analysts and Accounting staff review all report results and monitor SFTP transmissions for completeness and accuracy. Technology Services verifies all print jobs daily for completeness and accuracy, to ensure that what is produced by the systems are sent to the correct customers.

Dedicated firewalls are in place and rules restrict access to customer data to limit the possibility of disruptions to customer operations from unauthorized users. The firewalls are configured to restrict access to authorized users and connections only. Firewall activity is logged and monitored by Technology Services.

Data Backup and Retention

Production systems are backed up in accordance with documented procedures that include both networked servers and the iSeries system. Differential backups are taken on the iSeries daily (Monday through Saturday) with a full backup occurring on Sundays. Backup media is stored offsite at Vital Records. Daily backups are stored onsite and are rotated on a two-week schedule. Weekly backups are stored offsite and are rotated on a five-week schedule. Monthly backups are stored offsite and are retained indefinitely. Additionally, the iSeries and the critical Network servers are replicated to our cloud data center solution in Spartanburg, SC. Differential backups are taken on networked servers daily (schedules vary due to a workload distribution methodology and can occur Sunday through Friday, Monday through Saturday or, Tuesday through Sunday) with a full backup occurring on the seventh day of the schedule.

Seibels has documented data retention policies that are currently being reviewed by the executive committee and await approval. These policies include a Retention Schedule and Records Management procedures for all customer and company-maintained data. Seibels employs third party vendors for data and electronic equipment destruction.

Complementary Subservice Organization Controls and Monitoring

Seibels' controls related to its system covers only a portion of overall internal control for each user entity of Seibels It is not feasible for the applicable trust services criteria related to Seibels' system to be achieved solely by Seibels Therefore, each user entity's internal controls must be evaluated in conjunction with Seibels' controls and the related tests and results described in Section Four of this report, considering the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Subservice Organization	Service(s) Provided	Relevant Criteria Addressed
Vital Records	A service provider used for storage of backup tapes. The following control groupings are critical to achieving the applicable control objectives: • The subservice organization is responsible for the design and operation of backup tape off-site rotation and storage which relates to management's description. In addition, Seibels has identified the following controls to help monitor the subservice organization: • Reviewing documentation from the subservice organization and applicable SOC reports.	A 1.2
Immedion	A service provider used for datacenter services. The following control groupings are critical to achieving the applicable control objectives: • The subservice organization is responsible for datacenter services and offsite recovery which relates to management's description. In addition, Seibels has identified the following controls to help monitor the subservice organization: • Reviewing documentation from the subservice organization and applicable SOC reports.	CC 6.4, CC 7.4 & A 1.2

Subservice Organization	Service(s) Provided	Relevant Criteria Addressed
Net3	A service provider used for cloud infrastructure support. The following control groupings are critical to achieving the applicable control objectives: • The subservice organization is responsible for cloud disaster recovery services. In addition, Seibels has identified the following controls to help monitor the subservice organization: • Reviewing documentation from the subservice organization and applicable SOC reports.	A 1.2
Dell SecureWorks	A service provider used for security incident and event monitoring. The following control groupings are critical to achieving the applicable control objectives: • The subservice organization is responsible for the design and operation of system security monitoring which relates to management's description. In addition, Seibels has identified the following controls to help monitor the subservice organization: • Reviewing documentation from the subservice organization and applicable SOC reports.	CC 7.2
Segra	A service provider used for datacenter services. The following control groupings are critical to achieving the applicable control objectives: • The subservice organization is responsible for various datacenter services which relates to management's description. In addition, Seibels has identified the following controls to help monitor the subservice organization: • Reviewing documentation from the subservice organization and applicable SOC reports.	CC 6.4

Complementary User Entity Controls

Seibels' services were designed with the assumption that certain controls would be implemented by user entities. These controls should be in operation at user entities to complement Seibels' controls. The user entity controls subsequently presented should not be regarded as a comprehensive list of all controls that should be employed by user entities.

Complimentary User Entity Controls (CUECs)	Related Criteria
General Information Security Controls	
User organizations are responsible for ensuring confidentiality of any user IDs, passwords, and encryption keys assigned to them for accessing client data.	CC 6.1 & CC 6.6
User organizations using IPX are responsible for configuring password parameters to be in line with user entity policies.	CC 6.1