



BUSINESS SOFTWARE, INC.

SaaS Solutions

SOC 3 – Security, Availability, and Confidentiality

For the Period December 1, 2020 to November 30, 2021



TABLE OF CONTENTS

SECTION I – Independent Service Auditor’s Report	3
SECTION II – Assertion of the Management of Business Software, Inc.	6
SECTION III – Description of Business Software, Inc.’s <i>SaaS Solutions</i>	8

SECTION I
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: The Management of Business Software, Inc.

Scope

We have examined Business Software, Inc.'s (BSI's) accompanying assertion titled "Assertion of the Management of Business Software, Inc." (assertion) that the controls within BSI's *SaaS Solutions* System (TaxFactory™, ComplianceFactory™, and TaxProfileFactory™, collectively, the "*SaaS Solutions*") were effective throughout the period December 1, 2020 to November 30, 2021, to provide reasonable assurance that the *SaaS Solutions* System were protected against unauthorized access, use, or modification to achieve BSI's commitments and system requirements based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants' *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

Our examination included:

- (1) Obtaining an understanding of the *SaaS Solutions* System and BSI's service commitments and system requirements.
- (2) Assessing the risks that controls were not effective to achieve BSI's service commitments and system requirements based on the applicable trust services criteria.
- (3) Performing procedures to obtain evidence about whether controls within the *SaaS Solutions* System were effective to achieve BSI's service commitments and system requirements based on the applicable trust services criteria.
- (4) Evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the *SaaS Solutions* System that individual report users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements 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, BSI's management's assertion that the controls within BSI's *SaaS Solutions* System were effective throughout the period December 1, 2020 to November 30, 2021 to provide reasonable assurance that BSI's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Windham Brannon, LLC

Certified Public Accountants

May 10, 2022

SECTION II

ASSERTION OF THE MANAGEMENT OF BUSINESS SOFTWARE, INC.



ASSERTION OF THE MANAGEMENT OF BUSINESS SOFTWARE, INC.

We are responsible for designing, implementing, operating, and maintaining effective controls over security, availability, and confidentiality within Business Software, Inc.'s (BSI's) System (TaxFactory™, ComplianceFactory™, and TaxProfileFactory™, collectively, the “*SaaS Solutions*”) throughout the period December 1, 2020 to November 30, 2021, to provide reasonable assurance that BSI's commitments and system requirements relevant to security, availability, and confidentiality were achieved.

Our description of BSI's *SaaS Solutions* System in Section III identifies the aspects of the *SaaS Solutions* system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2020 to November 30, 2021 to provide reasonable assurance that BSI's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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.

Based on this evaluation, we assert that the controls within the *SaaS Solutions* System were effective throughout the period December 1, 2020 to November 30, 2021 to provide reasonable assurance that the System was protected against unauthorized access, use, or modification to achieve BSI's commitments and system requirements based on the applicable trust services criteria.

SECTION III

**DESCRIPTION OF BUSINESS SOFTWARE, INC.'S
*SAAS SOLUTIONS***

History

Since its founding in 1979, Business Software Inc.'s (BSI's or the Company's) full-time business has been regulatory and compliance software for payroll systems. BSI pioneered the modern tax system with the introduction of BSI-TAX™, its flagship product. Since then, BSI has revolutionized payroll tax procedures and been a full-time payroll tax specialist devoted exclusively to regulatory and compliance software. BSI's many years of specialization has resulted in industry-leading expertise and payroll compliance solutions. These solutions improve the efficiency of processes related to payroll tax and regulatory compliance and automate tedious manual processes for improved compliance and greater internal efficiency. Simplifying payroll tax and compliance is BSI's core business. Over 42 years of industry experience, development ingenuity, and advanced technology has distinguished BSI as the leading provider of payroll regulatory and compliance solutions. BSI presently has more than 3,000 customers in the United States, Canada, and around the world using one or more of its payroll compliance products. These customers represent almost 27 million employees whose payroll liabilities are calculated by BSI's products. In fact, many of the largest companies in the world are BSI customers. This diverse group of major organizations, service bureaus, and payroll system providers has leveraged the innovatively-engineered solutions from BSI to increase efficiency and solve their payroll tax challenges.

At BSI, dedicated researchers stay abreast of legislative activity and analyze newly enacted regulations to consistently provide products that anticipate customer needs. Compliance with regulatory and legal requirements is monitored via alerts and feeds, direct contact with government entities on a prescribed, regular basis, membership in industry groups such as the APA and NACTP, and subscriptions to information services such as Wolters Kluwer and Bloomberg BNA. This focus and expertise provide extra value for BSI's products, supplemented by timely BSI support.

BSI is headquartered in Peachtree Corners, Georgia, a suburb of the metropolitan Atlanta, Georgia area. BSI has experienced substantial growth and continues to capitalize on its experience. With a unique blend of technological innovation and fast-paced delivery of advanced feature content, BSI sets the industry standards.

Solutions

BSI specializes in providing solutions that improve the efficiency of processes related to payroll tax and regulatory compliance. By leveraging its development and regulatory expertise, BSI is able to offer solutions in both on-premise and on-demand environments that automate tedious manual processes for increased compliance and greater internal efficiency. The following is an overview of BSI's on-demand solutions – TaxFactory™, ComplianceFactory™, and TaxProfileFactory™ (collectively the *SaaS Solutions*):

TaxFactory

TaxFactory performs calculations of federal, state and local and U.S. territory payroll taxes for the employee and employer. The burden of tracking regulatory rules is eliminated for tax calculations, wage and benefit plan taxability, wage attachments and deferred income. TaxFactory integrates with internal systems, including HR/Payroll and Deferred Income and increases productivity and facilitates payroll withholding compliance. Its extensive capabilities allow BSI's customers to improve their own effectiveness while reducing overall costs.

ComplianceFactory

ComplianceFactory offers a robust U.S. payroll tax management tool that simplifies the burden of maintaining compliance and offers management of high-volume filing and payment processing for companies of all sizes. A suite of applications improves the management of filing, processing payments and related payroll tax responsibilities through a simplified employer dashboard. ComplianceFactory integrates with internal systems including HR/Payroll, Accounts Payable, General Ledger and various back-office functions.

TaxProfileFactory

TaxProfileFactory sets up payroll tax configurations on demand for employees that are newly hired, have changes to their data or are subject to newly enacted taxes. It works both in interactive and batch mode. The solution automatically creates the employee tax profiles for federal, state, local and territory taxes and presents employees with the appropriate payroll tax forms based on their individual taxing situation. The system considers concepts such as reciprocity and nexus when determining the employee's individual workflow.

Using BSI's solutions in an on-demand environment gives customers greater flexibility and ease of use, while lowering total cost of ownership. BSI has partnered with an independent subservice organization to operate the data centers that house systems used in the provision of the *SaaS Solutions* (the "Remote Data Center"), to achieve heightened levels of data availability, integrity, security and fail-over capability in the event of a disaster.

People

BSI's organizational structure is currently segregated by function into four core areas:

- Administration & Finance
- Contracts, Legal & Compliance
- Operations
- Sales & Marketing

Segregation by function ensures that competency centers are similarly grouped to streamline intra-divisional processes and procedures. A three-tiered management structure is utilized to provide proper oversight and control at a team, department and division level.

All employees and contractors are required to participate in an orientation program conducted by BSI's Human Resources Department, upon being hired. This program is structured to cover BSI's general operating practices, policies and procedures and assists employees and contractors in becoming acclimated to BSI's business philosophy and environment. Through this program, new employees and contractors gain an understanding of BSI's overall mission and core values, departmental operation practices and individual job descriptions. Key aspects of the employee

handbook, including the security program, are reviewed during the orientation program, based on the nature of the hire. Employees receive training on security annually and those policies and procedures impacting BSI's security commitments.

Risk Assessment

The Security Committee has instituted a formal procedure to identify and address ongoing threats and disruptions to operation of the *SaaS Solutions* that would impair its security commitments. Identified threats and risks to the *SaaS Solutions* are regularly evaluated during a formal risk assessment conducted by the Security Committee.

Infrastructure

A local and remote data center (a subservice organization) are utilized to provide the *SaaS Solutions*. The data center located at BSI's corporate office houses internal company infrastructure and systems to support development and testing of the *SaaS Solutions*. Access to BSI's facility is controlled through utilization of an integrated security system to prevent and detect unauthorized physical access that incorporates, among other things, access cards to restrict facility access to employees only, door contacts and automatic door locks, continuous third-party monitoring, motion sensors, office closing procedures, and audible security alarms.

The remote data center is managed by a managed service provider (a subservice organization) that is responsible for implementing logical and physical security controls including the use of smart cards, biometric hand scanners, digital video surveillance and on-site security officers to prevent unauthorized access. Integrated systems to prevent and detect fires, electrical power fluctuations and temperature abnormalities are in place to maintain optimal environmental conditions for operating the *SaaS Solutions* and minimize threats to computer equipment. Uninterruptible power supplies are leveraged to protect systems and ensure failover performance in the event of an emergency.

Security

Security is proactively designed into all aspects of BSI's *SaaS Solutions* to ensure that data stored in, or transmitted to, the *SaaS Solutions* is protected and secured against intentional and unintentional attack, theft, destruction and misappropriation. Data and transport-level encryption and obfuscation is employed within the *SaaS Solutions* to maintain data integrity. The Company conducts periodic reviews of technology asset inventories to maintain the accuracy of inventory records for security purposes. Access to the *SaaS Solutions* and supporting systems requires a unique User ID and Password and additional security measures, such as password integrity parameters, are in place to ensure only authorized users are accessing the *SaaS Solutions*. Once authenticated, users are prevented from viewing or editing un-authorized information. Employee access to the *SaaS Solutions* is based on roles tied to job descriptions that are approved by the employee's manager.

Management is committed to developing and maintaining an environment that protects information resources from accidental or intentional unauthorized use, modification, disclosure, or destruction. In order to maintain a secure environment, BSI has developed a security program that includes various security standards such as password policies and restricting the transmission of data to encrypted connections. Management of firewalls, intrusion detection systems, authorization mechanisms, and security devices have been contracted to the managed service

provider to monitor and control network security. BSI has implemented procedures to monitor firewall and IDS event and resolution reports monthly. End user and server workload network traffic is segmented to support network isolation. Remote access to the *SaaS Solutions* is limited to virtual private network (VPN) software, secure sockets layer (SSL), Transport Layer Security (TLS) or other encrypted communication systems. Software for virus scanning has been implemented on workstations, laptops and servers to monitor for malicious attacks on the corporate network. Virus signatures are updated automatically as updates are available. Email communication is also scanned for viruses.

A formal product development team develops and modifies the *SaaS Solutions*. Development of the *SaaS Solutions* is rigorously controlled using a formal, documented, industry standard development methodology.

Availability

BSI has implemented procedures to maintain availability of the *SaaS Solutions*. Incident recovery plans are both tested and reviewed by senior leadership on an annual basis, to ensure business continuity. Uptime statistics and *SaaS Solution* performance is continually monitored by BSI across all production environments.

Confidentiality

The boundaries of the *SaaS Solutions* and BSI's security, availability, and confidentiality commitments are communicated to users. Access to the *SaaS Solutions* is predicated on execution of an agreement including security, confidentiality and data integrity provisions, as well as user responsibilities, the terms of which are developed and approved by BSI's Legal Department.