



SOC 1-2-3 Reports for Vendor Risk Management

Understanding SOC Report Content

Introduction



Gary Nelson

Principal

Schellman



Profile & Career History

- Husband of wife age 39+?; father of 3 ages 20, 18, and 15
- Principal at Schellman for the Atlanta / Southeast markets
- Practice Leader in AICPA attestation services in information security and privacy
- Leader in Schellman's CMMC and cybersecurity assessment practices
- CPA licensure in multiple states
- Certifications as CISA, CISSP, CIA, CCA, PCI QSA, CIPP/US, CIPT, and an FIP designation
- Information security and privacy career spans over 25 years
- Prior to joining Schellman in 2006, held information security consulting and audit positions at Arthur Andersen, Protiviti, and Carnival Corporation
- Actively participate in multiple industry organizations, such as AICPA, ISACA, and CSA

Agenda

1 SOC Reporting Fundamental Concepts

2 Report Content Comparisons

3 Your Action Items



1

SOC Reporting Fundamental Concepts

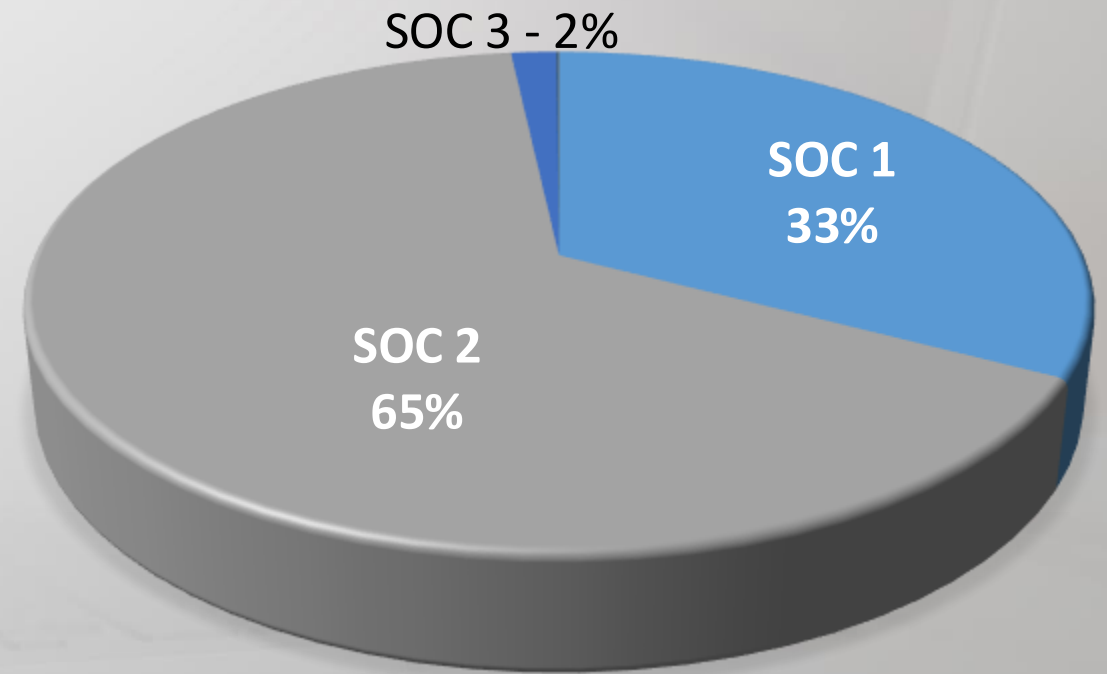
SOC Examinations

- Historically branded as Service Organization Controls Reports
- Rebranded as System and Organization Controls Reports
 - Allow for certain SOC reports to be adopted by non-service providers
 - Allows for expansion of the SOC suite (Cybersecurity, Vendor Supply Chains, etc.)



SOC Examinations

- Nearly all SOC reports are SOC 1 – 3
- SOC 1 recently removed from “king of the hill” by SOC 2
- Growing interest in SOC 3 for marketing and “check-the-box” requests



SOC 1-2-3 Examinations



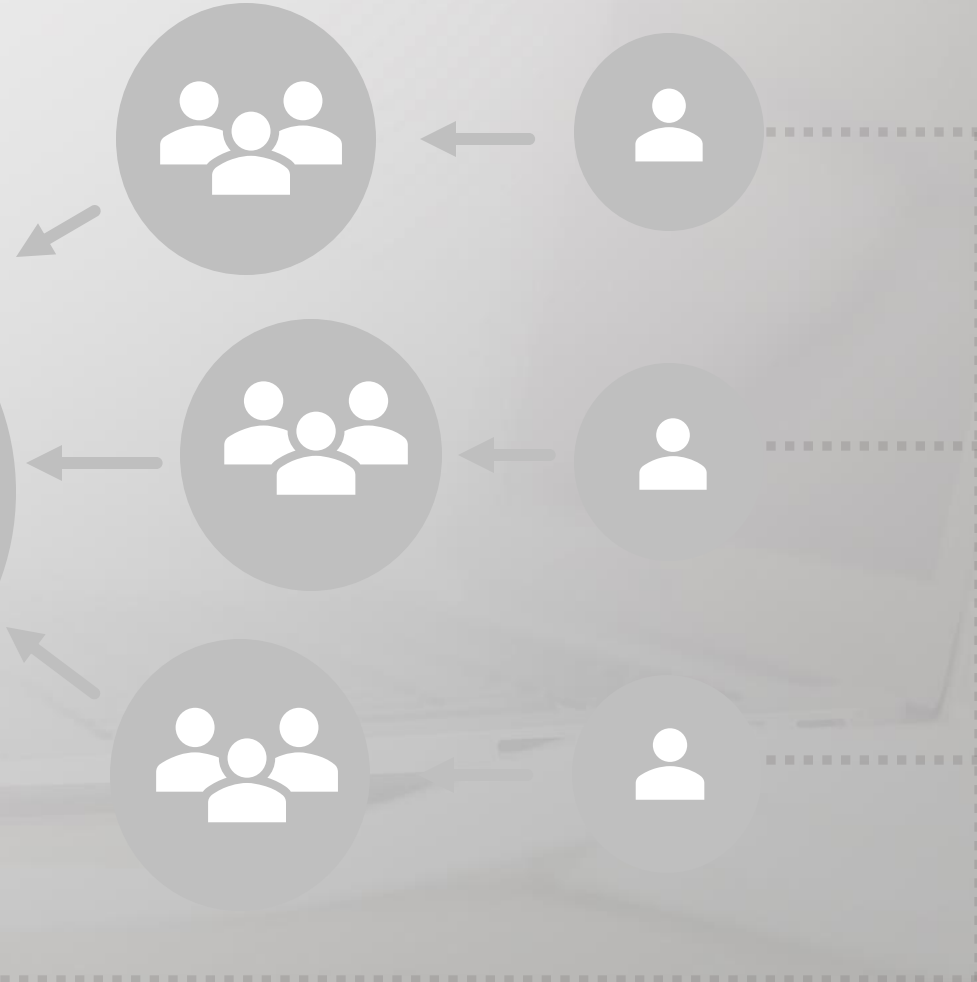
The Service
Organization



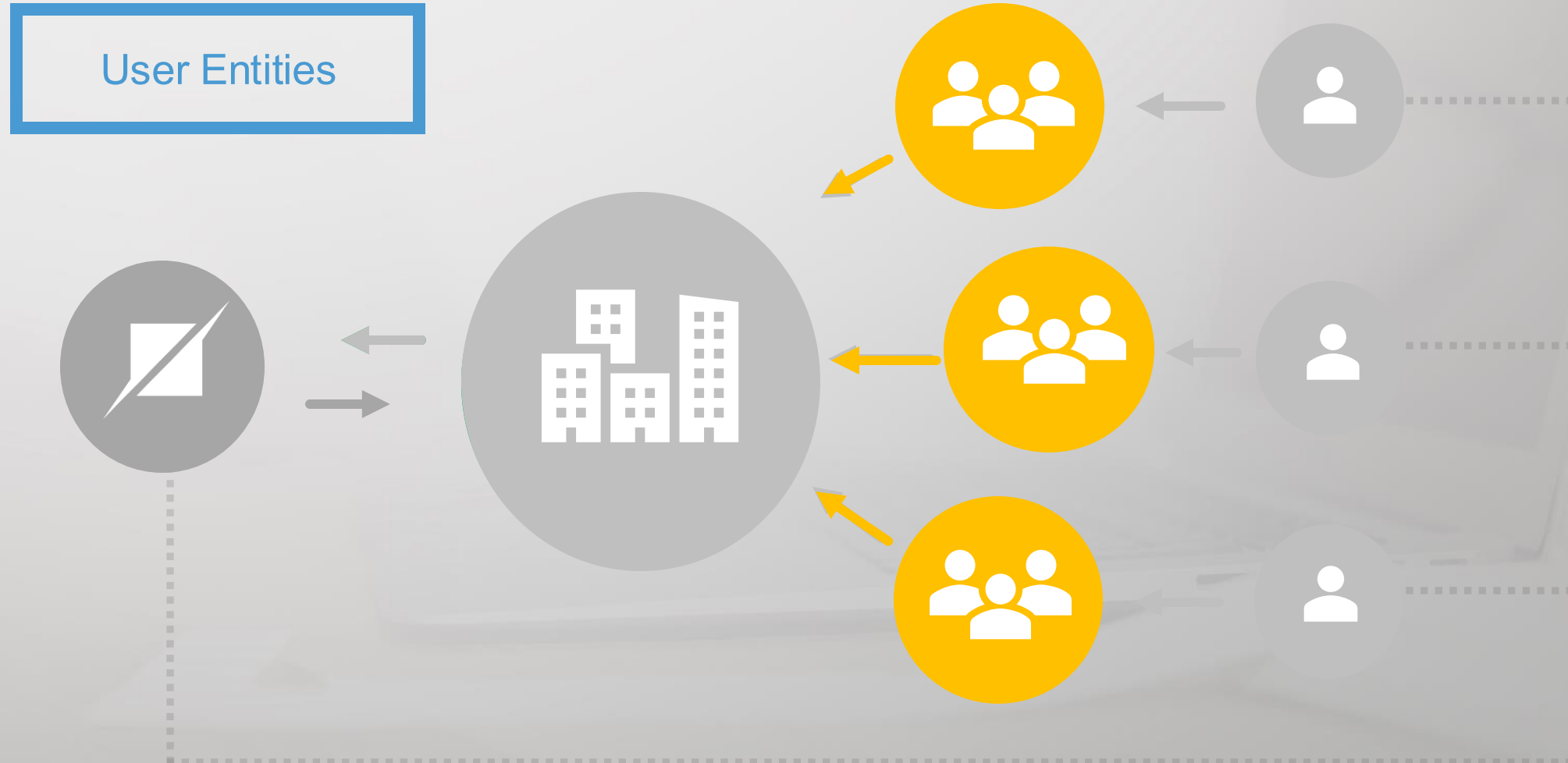
SOC 1-2-3 Examinations



The Service Auditor



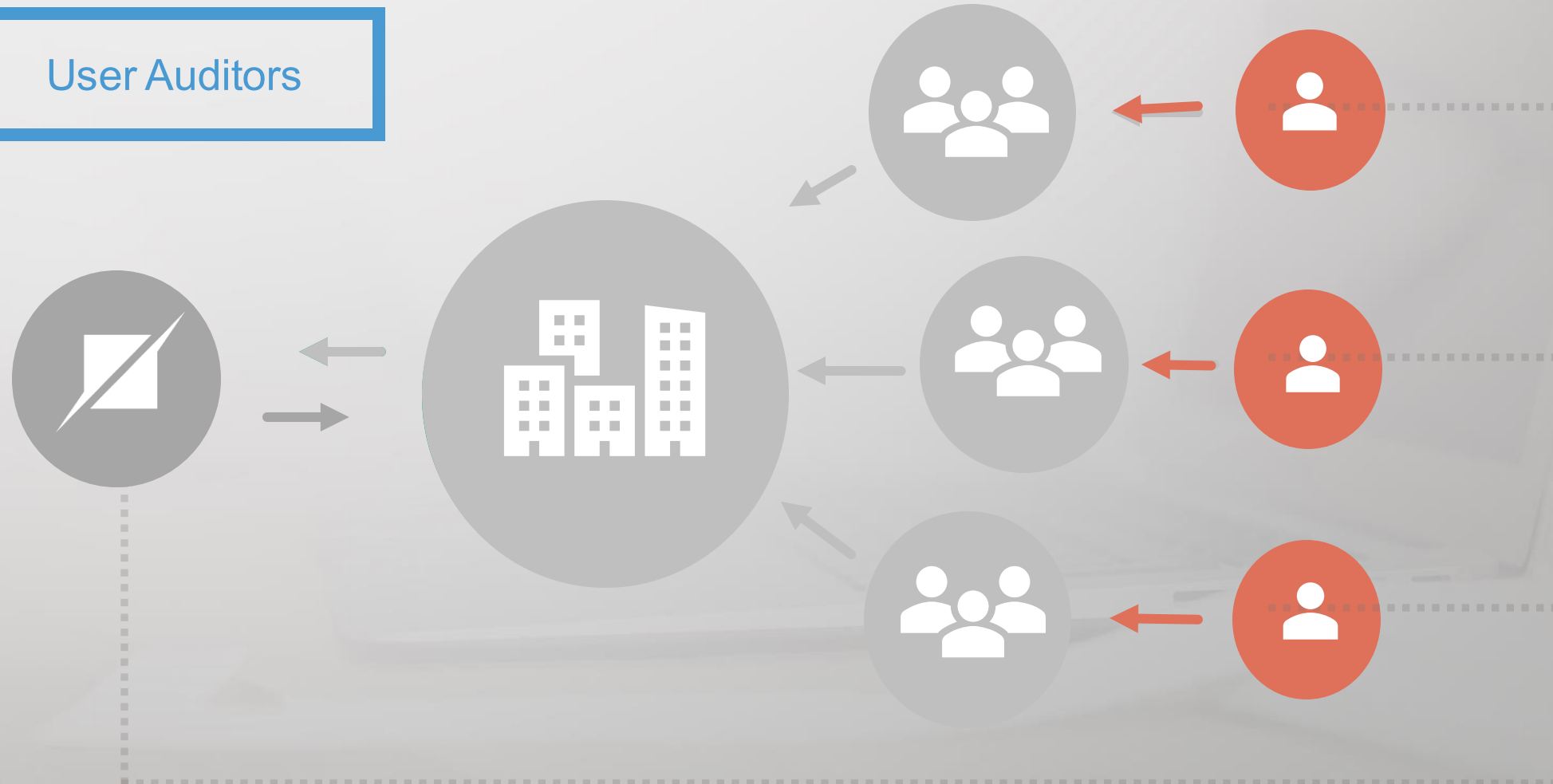
SOC 1-2-3 Examinations



SOC 1-2-3 Examinations



User Auditors



SOC 1-2-3 Examinations



The Primary Parties



SOC 1-2-3 Examinations



Report Sections That Are the Same For All Three

- Opinion Letter
 - Provided by the Service Auditor
- Assertion Letter
 - Provided by Management
- System Description
 - Provided by Management and Validated by Service Auditor



SOC 1 and SOC 2 Examinations



More Meat on the Bone

- Opinion Letter
 - Provided by the Service Auditor
- Assertion Letter
 - Provided by Management
- System Description
 - Provided by Management and Validated by Service Auditor
- Control Activities (Type 1) or Testing Matrices (Type 2)
 - Controls Provided by Management and Validation/Testing Provided by Service Auditor
- Other Information Provided by Management
 - Unaudited Content



SOC 1-2-3 Examinations



Overview Comparison

Attribute	SOC 1	SOC 2 / SOC 3
Standard	AT-C Sec. 105, 205, 320	AT-C Sec. 105, 205
Subject Matter	Internal Controls over Financial Reporting	Service Commitments and System Requirements
Criteria	Defined by the Service Organization	Trust Services Criteria
Reporting Types	Type 1 & 2	Type 1 & 2 (SOC 2) Type 2 (SOC 3)
Primary Users	Existing Customer Organizations/ Financial Auditors	Interested Parties



SOC 1-2-3 Examinations



Overview Comparison

Attribute	SOC 1	SOC 2 / SOC 3
What Controls Address	Control Objectives	Trust Services Criteria
Professional Opinion Purpose	Achieve the Control Objectives	Meet Service Commitments and System Requirements
Typical System in Scope	Outsourced Business Processes Impacting Financial Reporting	Outsourced Hosting, Security, or SaaS Services
Mappings to Other Frameworks	Possible but Manual Effort	Existing Mappings Developed by AICPA and others
Demand Trends	Stable	Continued Growth





2

Report Content Comparisons



INDEPENDENT SERVICE AUDITOR'S REPORT

uStar, Inc. ("BluStar"):

We have examined BluStar Inc.'s ("BluStar" or the "service organization") accompanying description of its Imaginary Services system, in Section 3, throughout the period May 1, 201X, to October 31, 201X, (the "description"), and on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period May 1, 201X, to October 31, 201X, to provide reasonable assurance that BluStar's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for security, availability, processing integrity, and confidentiality* (AICPA, *Trust Services Criteria*).

BluStar uses various subservice organizations for cloud hosting services, data center hosting services, physical data media vaulting services, and physical media and data destruction services. The description includes complementary subservice organization controls that are suitably designed and operating effectively, along with controls at BluStar, to achieve BluStar's service commitments and system requirements based on the applicable trust services criteria. The description presents BluStar's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the system. The description does not disclose the actual controls at the subservice organizations. The description did not include the services provided by the subservice organizations, and we have no assurance regarding the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Information included in Section 5, "Other Information Provided by BluStar is presented by BluStar. This information provides additional information and is not a part of the description. Information about BluStar's responses to exceptions noted has not been subjected to the procedures applied in the examination, the suitability of the design of controls, and the operating effectiveness of controls. Therefore, we do not express an opinion on the achievement of the service organization's service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

BluStar is responsible for its service commitments and system requirements and for implementing effective controls within the system to provide reasonable assurance that its service commitments and system requirements were achieved. BluStar has provided the description ("description") about the description and the suitability of design and operating effectiveness of controls. BluStar is also responsible for preparing the description and assertion, and for the presentation of the description and assertion; providing the applicable trust services criteria and stating the relationship between the achievement of the service organization's service commitments and system requirements and the applicable trust services criteria.

This Section provides:

- Scoping information regarding the in-scope services
- The as of date (Type 1) or examination period (Type 2)
- Content that was not tested
- Significant control issues, if any (explanatory paragraph)
- The auditor's bottom line (opinion)



MANAGEMENT'S ASSERTION

Anatomy of your SOC Report - Section 2



have prepared the accompanying description of BluStar's Imaginary Cloud Services system, in Section 3, throughout the period May 1, 201X, to October 31, 201X, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Imaginary Cloud Services system that may be useful in assessing the risks arising from interactions with BluStar's system, particularly information about system controls that BluStar has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, processing integrity, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for security, availability, processing integrity, and confidentiality* (AICPA, *Trust Services Criteria*).

BluStar uses various subservice organizations for cloud hosting services, data center hosting services, critical data media vaulting services, and physical media and data destruction services. The description includes complementary subservice organization controls that are suitably designed and operating effectively throughout that period, along with controls at BluStar, to achieve BluStar's service commitments and system requirements based on the applicable trust services criteria. The description presents BluStar's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of BluStar's controls. The description does not disclose the actual controls at the subservice organization.

We confirm, to the best of our knowledge and belief, that

- the description presents BluStar's Imaginary Cloud Services system that was designed and operated throughout the period May 1, 201X, to October 31, 201X, in accordance with the description criteria;
- the controls stated in the description were suitably designed throughout the period May 1, 201X, to October 31, 201X, to provide reasonable assurance that BluStar's service commitments and system requirements would be achieved based on the applicable trust services criteria if the subservice organizations applied their controls effectively throughout that period; and
- the controls stated in the description operated effectively throughout the period May 1, 201X, to October 31, 201X, to provide reasonable assurance that BluStar's service commitments and system requirements were achieved based on the applicable trust services criteria if the subservice organization controls assumed in the design of BluStar's controls operated effectively throughout that period.

This Assertion Letter provides:

- Scoping information regarding the in-scope services
- Management's claim (assertion) regarding how they describe their system, if other third-parties are involved, and confirms the period of coverage or date of the examination
- Significant matters for regarding the description and controls testing, if applicable



OVERVIEW OF OPERATIONS

Company Background

Based in Anytown, Anystate, BluStar, Inc. ("BluStar" or the "service organization") was founded in 1870. With over 75,000 employees, BluStar is a cloud company committed to enhancing the performance of their client application hosting experiences. These cloud services include identifying several imaginary and made up opportunities and vectors for success in technology. BluStar's services are designed to enable clients to amazing fictitious services and tools.

Description of Services Provided

BluStar provides and supports an unreal website for Imaginary Cloud Services users that is used to manage customer accounts and widgets related to their bright ideas, in addition to companion only offers for the Foundation accounts and transaction activity for Supreme companion accounts. Imaginary Cloud Services provides companion data to BluStar which is used to credit/debit against the customer account and a current volumes available for takeback options.

The hosted website is for customer access which allows companions to check transaction volumes, perform gift, power card, and turbo card takebacks against a customer's account. These Subscriptions are provided by the third-party vendor SubscriptionWiz.

BluStar also supports a customer tech application where customer tech representatives (CTR) assist customers and Client Liaisons with their questions and support their friendship accounts. CTRs can see on the website in addition to other supporting data such as transaction history. CTRs with appropriate access can award "goodwill" transactions to the companion application. These transactions are posted as CTR modifications.

BluStar generates application reports which are e-mailed to Imaginary Cloud Service users on a basis.

An overview of the data process flows is as follows:
[example data / process flow diagram]

PRINCIPAL SERVICE COMMITMENTS AND STANDARDS

BluStar designs its processes and procedures related to the following objectives for its Imaginary Cloud Services. Those objectives include: making to user entities, the ABCD and regulations that govern the services, and the financial, operational, and compliance services. The Imaginary Cloud Services of BluStar are designed to meet and data security requirements in which P

Anatomy of your SOC Report - Section 3

- This Description Section provides:
- Key scoping information
 - The description of the services under examination
 - The control objectives / service commitments
 - The Five Components of the System
 - The relevance and involvement of other third-parties used by the vendor
 - Description of the vendor's risk management program

OVERVIEW OF OPERATIONS

Company Background

Based in Anytown, Anystate, BluStar, Inc. ("BluStar" or the "service organization") was founded in 1870. With over 75,000 employees, BluStar is a cloud company committed to enhancing the performance of their client application hosting experiences. These cloud services include identifying several imaginary and made up opportunities and vectors for success in technology. BluStar's services are designed to enable clients to access amazing fictitious services and tools.

Description of Services Provided

BluStar provides and supports an unreal website for Imaginary Cloud Services users that is used to manage customer accounts and widgets related to their bright ideas, in addition to companion only offers for the Foundation accounts and transaction activity for Supreme companion accounts. Imaginary Cloud Services provides companion data to BluStar which is used to credit/debit against the customer account and a current volumes available for takeback options.

The hosted website is for customer access which allows companions to check transaction volumes, perform gift, power card, and turbo card takebacks against a customer's account. These Subscription services are provided by the third-party vendor SubscriptionWiz.

BluStar also supports a customer tech application where customer tech representatives (CTRs) assist customers and Client Liaisons with their questions and support their friendship accounts. CTRs can see on the website in addition to other supporting data such as transaction history. CTRs with appropriate access can award "goodwill" transactions to the companion application. These transactions are posted as CTR modifications.

BluStar generates application reports which are e-mailed to Imaginary Cloud Service users on a daily basis.

An overview of the data process flows is as follows:
[example data / process flow diagram]

PRINCIPAL SERVICE COMMITMENTS AND SCOPE

BluStar designs its processes and procedures related to the management of its services. Those objectives for its Imaginary Cloud Services. Those objectives include the ABCD and regulations that apply to the services, and the financial, operational, and compliance requirements for the services. The Imaginary Cloud Services of BluStar are designed to meet the data security requirements in which P

Anatomy of your SOC Report - Section 3

This Description Section provides:

- Your control responsibilities (CUECs)
- Your service responsibilities (CUERs)
- Dependencies on controls at other third-parties (CSOCs)
- The description of the services under examination
- The control objectives / service commitments
- Criteria excluded from scope (SOC 2)

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Imaginary Cloud Services users' system provided by BluStar. The scope of the testing was restricted to the Imaginary Cloud Services users' system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period May 1, 201X, to October 31, 201X.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls;
- Whether the control is manually performed or automated;

The types of tests performed with respect to the operational effectiveness of the control activities in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and the performance and application of the related control activity through interviews, telephone calls, e-mails, web-based conferences, or other means preceding.
Observation	Observed the relevant processes or procedures during which the control was not limited to, witnessing the performance of control activities or performance with relevant personnel, systems, or performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This includes system configurations and settings, or other data, signatures, approvals, or logged events, tracing events forward to control resolution, detailed documentation, and prerequisite events (e.g.,

Anatomy of your SOC Report - Section 4

Applies to SOC 1 and SOC 2 only

- Anyone remember why?

This Section provides:

- The specific control activities specified by the service organization
- The specific tests the auditor used to determine control effectiveness (Type 2 only)
- The results of the auditor's tests that were applied to controls (Type 2 only)



SECTION 5

OTHER INFORMATION PROVIDED BY BLUSTAR

Applies to SOC 1 and SOC 2 only

This Section provides:

- Management responses to testing exceptions (Type 2) are very common, as applicable
- Almost anything the vendor wants to include (e.g., control mappings, future controls and changes, privacy notices, etc.)
- The auditor provides no assurance on this section



The background image shows a row of three doors on a brick wall. From left to right, the doors are red, yellow, and blue. Each door has a semi-circular transom window above it with a decorative stone frame. The red door has the number '42' on it. The yellow door has a small plaque. The blue door has a small plaque. To the right of the blue door, there is a sign that says 'SMITHWICK SOLICITORS'. The entire image has a blue overlay.

3

Your Action Items

Your Primary Responsibility



- If you intend to use the SOC 1, SOC 2, or SOC 3 report, you must:
 - Understand the concept of a specified user and determine if you qualify (for SOC 1 or SOC 2)
 - Understand the concept of a 'broad-base' of users
 - Understand what each section of the report provides (*high-level*)
 - Understand what the vendor expects of your organization (*detail level*) complementary user entity responsibilities (CUERs) and complementary user entity controls (CUECs)



Checklist – Section 1



- Ensure the scope (name of system) is consistent with the service you are using or plan to use.
- Ensure the period of coverage is sufficient for your purposes.
- Determine if there are any paragraphs explaining control deficiencies and if they are material to your risk management for that vendor
- Determine if there are any disclaimers to processes or sections in the report
- *THEN*, read the auditors opinion paragraph and determine the affect of any modifications to your risk management for that vendor



Checklist – Section 2

- Ensure the scope, objectives / criteria, and period of coverage within the assertion are consistent with the auditor's report (Section 1)
- Read any paragraphs explaining control deficiencies or other matters and if they are material to your risk management for that vendor, if applicable

Checklist – Section 3



- Ensure the scope, objectives / criteria, service commitments, and period of coverage are consistent with the auditor's report (Section 1)
- Understand the description of the system boundaries and how the vendor's system interfaces with your environment
- Understand each control process and description of the vendor's risk management practices, and determine the effect on your risk management for that vendor
- Determine if there are any CUECs and how they are addressed in your organizations control environment



Checklist – Section 3



- Determine the nature and extent of other third parties used by the vendor, and if a controls report from those additional third parties are necessary.
- Determine the effect of any “Significant Changes” on your risk management for that vendor



Checklist – Section 4



- Ensure the controls that were tested (Type 2) are consistent with your expectations
- Determine if any control deviations / findings are material to your risk assessment for that vendor (not all 'findings' are bad)
- Communicate areas of concern or requested changes to be consideration with your vendor:
 - Examination period / date
 - Timing of report delivery
 - Modifications to scope
 - Modifications to testing (e.g., pen testing)
 - Different type of assurance report (e.g., ISO 27001 / 27701)





4


Questions ?



Thank you!

Follow us:

 Schellman & Company

 @schellmanco

 /schellmanco



Gary Nelson
Principal
Schellman

