

BlueJeans

Blue Jeans Network, Inc.
System and Organization Controls (“SOC”) for Service
Organizations: Trust Services Principles Report
Relevant to Security, Availability, and Confidentiality
Related to the BlueJeans Cloud-Based Video Conferencing
Services Platform

For the period October 1, 2017 to August 31, 2018

Standards for Attestation Engagements,
SOC 3[®] Engagement



Table of Contents

Section I – Independent Service Auditors’ Report	1
Section II – Assertion of the Management of Blue Jeans Network, Inc.	3
Section III – BlueJeans’ Description of the Boundaries of the System	4
A. Introduction	4
B. System Overview	4
C. Description of the Control Environment	6
D. Complementary Subservice Organization Controls (“CSOCs”)	8
E. Complementary User Entity Controls (“CUECs”)	9
F. Principal Service Commitments and System Requirements	10



Section I – Independent Service Auditors’ Report

To the Management
Blue Jeans Network, Inc.
Mountain View, California

Scope

We have examined Blue Jeans Network, Inc.’s (“BlueJeans” or the “service organization”) accompanying assertion titled “Assertion of the Management of Blue Jeans Network, Inc.” (“assertion”) that the controls within BlueJeans’ Cloud-Based Video Conferencing Services Platform (the “System”) were effective throughout the period October 1, 2017 to August 31, 2018, to provide reasonable assurance that BlueJeans’ service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (“applicable trust services criteria”) set forth in TSP 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Trust Services Criteria*).

Service Organization’s Responsibilities

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

Service Auditors’ Responsibilities

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

Our examination included:

- Obtaining an understanding of the System and BlueJeans’s service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve BlueJeans’ 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 BlueJeans’ service commitments and system requirements based the applicable trust services criteria.

To the Management
Blue Jeans Network, Inc.

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

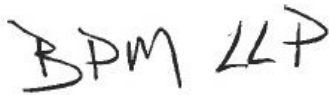
Our examination was not conducted for the purpose of evaluating or testing BlueJeans' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

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 BlueJeans'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 the System were effective throughout the period October 1, 2017 to August 31, 2018, to provide reasonable assurance that BlueJeans's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Handwritten signature in black ink that reads "BPM LLP". The letters are stylized and slanted.

San Jose, California
November 19, 2018



Section II – Assertion of the Management of Blue Jeans Network, Inc.

We are responsible for designing, implementing, operating, and maintaining effective controls within Blue Jean Network, Inc.'s ("BlueJeans") Cloud-Based Video Conferencing Services Platform (the "System") throughout the period October 1, 2017 to August 31, 2018, to provide reasonable assurance that BlueJeans' service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the System (the "description") is presented in "Section III – BlueJeans' Description of the Boundaries of the System" and identifies the aspects of the System covered by our assertion.

BlueJeans uses subservice organizations as follows:

- ◆ Amazon Web Services ("AWS") for data storage services.
- ◆ Equinix, Inc. ("Equinix") for data center hosting services.
- ◆ Telstra Corporation Limited ("Telstra") for data center hosting services.
- ◆ Arcserve, Inc. ("Arcserve") (previously Zetta) for data backup and storage services.

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at BlueJeans, to achieve BlueJeans' service commitments and system requirements based on the applicable trust services criteria. The description does not disclose the actual controls at the subservice organizations.

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

We have performed an evaluation of the effectiveness of the controls within the System throughout the period October 1, 2017 to August 31, 2018, to provide reasonable assurance that BlueJeans' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Trust Services Criteria*). BlueJeans' 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 III F., *Principal Service Commitments and System Requirements*.

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 October 1, 2017 to August 31, 2018, to provide reasonable assurance that BlueJeans' service commitments and system requirements were achieved based on the applicable trust services criteria.

The Management of Blue Jeans Network, Inc.

Section III – BlueJeans’ Description of the Boundaries of the System

A. Introduction

Company Background and Scope

Blue Jeans Network, Inc. (“BlueJeans” or the “Company”) provides a cloud-based video conferencing services platform (the “System”) that allows individual users, teams and groups to connect across many devices and platforms. With a platform comprising an integrated suite of video conferencing and collaboration services, BlueJeans offers users the power to expand phone calls into video meetings. BlueJeans supports multi-party bridging, multi-vendor and multi-device video calling and collaboration. The BlueJeans feature set enables users to connect across several platforms and endpoints (browsers and smart devices, Android and iOS). In addition, each meeting can be secured and encrypted.

BlueJeans has several different offices, including Mountain View, California (headquarters); San Francisco, California; Orange County, California; Bangalore, India; London, United Kingdom (UK); and Sydney, Australia. BlueJeans utilizes service providers (subservice organizations) for data center hosting services with locations in the United States and abroad. More details regarding BlueJeans’ subservice organizations can be found in Section D *Complementary Subservice Organization Controls*.

BlueJeans is privately held and the BlueJeans’ website address is www.bluejeans.com.

B. System Overview

The System is designed to enable any customer to engage their audience through video to share content and ideas in an interactive experience. The System offers:

- ◆ **Room to Remote Video Conferencing** that allows any customer to use their installed video system and meet with any parties through their own systems and devices.
- ◆ **Cloud-based Video Bridging** as a way to reduce costs and infrastructure overhead when connecting through multi-point devices.
- ◆ **Mobile Video Collaboration** to provide high quality video collaboration using smart phones and the latest tablet devices.

This System provides customers and users with the ability to:

- ◆ Schedule people in various departments across many time zones.
- ◆ Have guests join meetings, easily.
- ◆ Share and collaborate on content.
- ◆ Integrate with well-known and widely used enterprise applications such as Microsoft Outlook and Google Calendar.

Overall, the System is enterprise-grade and simple to setup.

Elements of the System

The System is a single conferencing and collaboration service for a customer’s combined video, audio, and web conferencing and collaboration needs. With inputs and insights derived from our internal analytics; BlueJeans provides a more personalized experience and customers are able to leverage the power of video conferencing for faster communication with enhanced collaboration.

Section III – BlueJeans’ Description of the Boundaries of the System

The System is composed of several core elements and their respective features include: BlueJeans Meetings (core software), BlueJeans Events (broadcast), BlueJeans Rooms, Command Center (analytics), Relay (integration software for room systems and BlueJeans), and the Administration portal.

BlueJeans Meetings seamlessly delivers interactive, multi-party face-to-face video meetings that are securable and offer the ability to add participants to in-progress meetings, from a laptop, mobile device or room system. BlueJeans Meetings is comprised of integrated components that support a wide variety of room, browser and mobile endpoints. It supports a range of telecommunication standards for audio-visual sessions on any packet network. The call signaling helps transmit calls across the following networks: Internet Protocol (“IP”) and Public Switched Telephone Network. In addition, BlueJeans Meetings supports H.323 and Session Initiation Protocol (“SIP”) for controlling audio-visual sessions over IP networks.

BlueJeans Events has reinvented the online event by blending the interactivity and engagement of a video meeting with the scalability of a broadcast event. By creating an easy, open and collaborative experience for both organizers and attendees, BlueJeans Events enables a whole new class of interactive events in business, media, entertainment, gaming, and education.

BlueJeans Rooms provides the capability to make any conference room an easy to use video room that interoperates with existing systems or new hardware.

Relay is a software platform that integrates customer-premise components and applications with the BlueJeans cloud for a superior collaboration experience. Relay integrates calendar applications, conference room systems, and tablet devices to make joining a BlueJeans meeting easy and automatic.

Command Center is an analytics dashboard for the customers, provides insight into historical meetings, events, and related information.

The Enterprise Administration portal is used by Enterprise Administrators for creating, updating and deactivating user accounts in the System.

Encryption can be leveraged by administrators for video meetings between secure video endpoints. The core platform supports industry standards based authentication.

Access to the System

BlueJeans Only

BlueJeans has implemented role based access controls to help prevent unauthorized access to the System. As a standard, BlueJeans restricts access to the production environment to only those employees with a job function(s) that requires access using two factor authentication (“2FA”) over site to site virtual private network (“VPN”). Access policies are reviewed and modified periodically. Customers do not have access to back-end production environment.

Customer Users

Customers access BlueJeans administrative applications through web interfaces, and can use an Enterprise Administrator role to both manage the roles of customer’s users who have a license to start meetings as well as to schedule and manage meetings. BlueJeans accounts are secured with username and password authentication or Single-Sign-On (“SSO”). Password policies and failed login notifications are configurable by a customer’s Enterprise Administrator. Passwords are stored as salted and hashed strings using one-way SHA-256 algorithm in the database and can never be viewed in plain text.

Meeting Security

BlueJeans provides customers the ability to set certain security standards with respect to the System within their respective organizations. General settings, which are available for Customer selection, include requiring end users to have stronger personal meeting identification (“ID”) sequences and passcodes, requiring minimum length of meeting IDs (up to 18 digits), enforcing moderated meetings with passcodes, forcing moderators to login, allowing moderator access only from specific IP address ranges and disallowing meetings from banned countries. ‘In Meeting’ security options include locking meetings to include only those participants logged in and the ability to expel participants when required.

Administration of the System

BlueJeans’ Operations team is responsible for performing all operational tasks per approved policies and procedures, including tracked change/patch management for updating application binaries, data, software stack, hardware and emergency fixes, monitoring the System for performance, capacity and availability, and maintaining backups of production data.

C. Description of the Control Environment

The following section is a description of control environment as it relates to the System.

Core Security, Protection, and Confidentiality

BlueJeans documents its overall security approach in its Information Security and Confidentiality Policy document. Within this document are key areas describing how BlueJeans addresses the classification, protection, handling, responsibility, transmission, storage and access of data.

To protect confidential data, the control framework that underpins the BlueJeans organizational environment starts with the management team and is executed by their respective managers and teams. BlueJeans communicates its confidentiality commitment to every customer within the contract prior to delivery of service. Appropriate logical security controls are implemented by IT to ensure that System access is restricted to employees with a business need-to-know and System access is monitored.

The System is designed to enable authenticated customers to access and manage their recorded and/or uploaded video content and manage access to the System. BlueJeans has also implemented technical and physical controls designed to prevent unauthorized access to or disclosure of content. Internally, confidentiality requirements are communicated to employees through training and policies. Employees are required to attend security awareness training, which includes information, policies, and procedures related to protecting customers’ content. BlueJeans monitors the performance of third parties through periodic reviews, which evaluate performance against contractual obligations, including confidentiality commitments.

Overall, management’s philosophy, its skilled managers and underlying culture contribute to the strength of the control environment. This philosophy influences how customers are supported, how internal decisions are made, and how risks are addressed.

Section III – BlueJeans’ Description of the Boundaries of the System

BlueJeans Personnel and Management Responsibility

BlueJeans’ leadership and organizational structure provide a framework for planning, executing and controlling business operations. Starting with the Chief Executive Officer (“CEO”) and the Executive team, this structure provides the leadership and vision to ensure success of the System solution, adequate staffing, security, efficiency of operations, and segregation of duties while setting the tone and establishing the core values of BlueJeans.

BlueJeans follows a structured on-boarding process to familiarize new employees and contractors with BlueJeans applications, processes, systems, security policies and practices. New hires are provided with the BlueJeans’ Code of Conduct and are required to complete an initial and an annual Security and Awareness training. BlueJeans maintains high standards for hiring and places emphasis on education, integrity, and functional roles performed previously to assess if a candidate is a “good fit” for the team. BlueJeans has also implemented controls over the key aspects off-boarding process. When the need arises for termination or separation, HR maintains an exit checklist and initiates/approves their termination.

The Management team has regularly scheduled meetings to discuss business strategy (including customer challenges and legal updates), development, releases and enhancements to the product line, core financials, product sales, and other matters important to the current and future success of the BlueJeans. In addition, the Management team develops a Board deck or summary of recent business activity to be presented at regularly scheduled (usually quarterly) and special meetings of BlueJeans’ Board of Directors.

The Operations Team along with the Information Security Team designs key controls and monitors the operation of those controls to meet compliance efforts for BlueJeans. The Chief Technology Officer (“CTO”) and the Director of Information Security delegate responsibility for internal information technology (“IT”) related controls to other members of the organization where needed. To maintain these standards, compliance audits are performed to meet the needs of BlueJeans’ clients and ensure that employees understand and follow internal policies.

To secure the System and the business operational environment, management has documented and implemented policies. These policy and standards documents are reviewed, managed and updated (annually) by the CTO or the Director of Information Security to ensure security measures, confidentiality practices and availability concerns, when applicable, meet good practices.

Risk Management

BlueJeans takes a pro-active approach to identify, understand, and mitigate risks to BlueJeans, its business and technical operations, and to its customers and the System. BlueJeans’ more formal risk assessment and overall risk effort generally includes a multi-step process beginning with the (1) review of critical risks (internal and external) by the Director of Information Security, (2) a subsequent review with the CTO, (3) follow-up with ongoing and independent third-party provider performing independent and dynamic security tests, (4) a risk assessment meeting with key executives and teams and (5) final compilation, creation and updating of significant operational and technical risks. This compilation includes an assessment of the likelihood of these risks and subsequent actions to remediate high or critical risks.

Section III – BlueJeans’ Description of the Boundaries of the System

BlueJeans Risk Analysis

The Director of Information Security documents noted risks in a “Risk Register,” measured based on the probability, potential impact and overall risk significance that an occurrence would have to the System. Mitigation activities are tracked in a ticketing system and follow the change management process in place at BlueJeans.

In summary, the internal risk assessment and management program is two-fold. First, the program requires BlueJeans management and core staff to be aware of potential risks and identify new, significant risks within the System. Second, the risk assessment program enables BlueJeans staff to understand how the ongoing operations that underpin the System impacts user organizations relying on BlueJeans.

Incident Management and Communication

BlueJeans strives to provide a robust communication process to its customers, vendors, and employees. The Executive team is committed to maintaining an effective communications system to ensure System related issues, outages, and critical fixes are addressed and resolved in a timely manner.

Incident Management procedure is triggered in the event there is severe degradation, an outage of the System, a suspected breach, or a known intrusion. All incidents are logged into the issue tracking software and tracked through to completion by the Engineering/Security/Support/IT/Operations teams. The Executive team is informed of the incident management progress. If the production environments are inaccessible for any significant period of time, Customer Support will notify affected customers and provide updates when the System is restored.

BlueJeans has a designated senior contact within Customer Support to establish and maintain communication mechanisms that ensure all customers are provided new release information and any customer issues are addressed timely and resolved to customers’ satisfaction. A list of the new features, upgrades, and fixes in each release of the application is provided to all customers and BlueJeans partners.

Product Planning, Release Cycle and Testing

At BlueJeans, long range planning goes into developing and ultimately delivering the Video Conferencing service to the marketplace. To meet the needs of these customers quickly and effectively, BlueJeans attempts to have manageable release cycles that are short in duration, predictable in delivery and flexible to meet a variety of needs. BlueJeans follows a documented “Software Release Process” that includes steps for the product releases, emergency fixes and configuration and infrastructure changes. The release methodology has segmented environments for development, QA, staging, and production. This segmentation allows BlueJeans to perform updates quickly, but not expose production to changes without proper testing and approval. All product releases and changes are tracked through the project tracking system. BlueJeans requires that only tested and approved changes shall be made to the System and all changes made are documented, tested and approved by stake holders prior to production rollout, except in emergencies when the changes are approved post-production rollout.

D. Complementary Subservice Organization Controls (“CSOCs”)

The System’s primary production solution is located at Equinix, Inc. (“Equinix”) data center in San Jose, California, and has redundant Points of Presence (“PoPs”) located in the Equinix data centers in Ashburn, Virginia, Singapore and Amsterdam, as well as a Telstra Corporation Limited (“Telstra”) data center in Sydney, Australia. The System is delivered from these secure facilities in geographically separate locations.

Section III – BlueJeans’ Description of the Boundaries of the System

The System was designed with the assumption that certain complementary subservice organization controls are suitably designed and operating effectively, along with controls at BlueJeans, to achieve BlueJeans’ service commitments and system requirements based on the services criteria relevant to security, availability, and confidentiality.

Data backup is encrypted and sent to Arcserve, Inc. (“Arcserve”) over Hypertext Transfer Protocol Secure (“HTTPS”) to be stored in their infrastructure.

Aside from the main data centers helping to distribute the System, Amazon Web Services (“AWS”) services are used to augment the Company’s data center capabilities. BlueJeans employees do not have physical access to AWS data centers.

In addition, BlueJeans deploys firewalls, system-hardening procedures, standard application and secure protocols for access, and third-party monitoring to protect against unauthorized access to systems.

The above mentioned subservice organizations have completed independent third-party examinations. BlueJeans requests these annual independent third-party SOC reports and/or ISO 27001 certifications from the subservice organizations and reviews the reports for exceptions and complementary user entity controls that must be implemented within the BlueJeans control environment.

As noted in the above reports, these subservice organizations have the responsibility to implement the types of controls expected by BlueJeans to both ensure availability of the System and ensure that security of the System is not impacted. Access is restricted to only authorized employees or third-party managed providers contracted to BlueJeans. BlueJeans reviews third-party access into the data centers on a quarterly basis.

E. Complementary User Entity Controls (“CUECs”)

The System was designed with the assumption that certain user entity controls are suitably designed and operating effectively, along with controls at BlueJeans, to achieve BlueJeans’ service commitments and system requirements based on the trust services criteria relevant to security, availability, and confidentiality.

This section describes certain CUECs that should be operating effectively at user entities. However, there may be related controls not identified in this report, which may be appropriate for a specific user entity’s operations.

User Entity Commitments

1. User entities, in accordance with contractual agreements, are responsible for accepting and complying with the Terms of Service with BlueJeans.
2. User entities must follow the guidelines of the contract with respect to the System services.
3. User entities are responsible to meet the applicable privacy and regulatory laws for their industry.
4. User entities agree that it will use the Service only in compliance with the Suppliers Acceptable Use Policy.
5. User entities are responsible for understanding the operating systems, web browsers and mobile devices that can be used with the System and ensuring their security configurations are up-to-date.
6. User entities are responsible for reviewing the completeness and accuracy of the reports that are produced by the System.

Section III – BlueJeans’ Description of the Boundaries of the System

7. User entities are responsible for setting the proper configurations for each scheduled meeting based on the options provided by the System.

Security Access

8. User entities must identify an administrative user name and password for its account.
9. User entities are responsible for all activity under its user accounts, including notifying BlueJeans of failed login attempts from an unknown source.
10. User entities are responsible for ensuring the security and confidentiality of all user IDs and passwords, preventing unauthorized access to, or use of the System, and notify BlueJeans Customer Support promptly of any actual or suspected unauthorized use of the System.
11. User entities and their account administrator are responsible for managing their passwords within the System and meeting their internal password configuration standard.
12. User entities are responsible for disabling access of employees to the System immediately upon termination.
13. User entities ascertain that expressed consent has been obtained from their users to transfer user data to the United States, if applicable.
14. User entities are responsible to enable encryption within the System for secure meetings with the understanding that only encrypted endpoints will be able to access the meeting.

Organization

15. User entities are responsible for communicating and providing up-to-date organizational contact information to BlueJeans.
16. User entities are responsible for obtaining and maintaining any equipment or ancillary services needed to connect to, access or use the System

Data Management

17. User entities are responsible for the accuracy, quality, integrity, legality and appropriateness of the content.
18. User entities are responsible for maintaining adequate backups of their content.
19. User entities are responsible for determining the applicability of recording any parts of meetings.
20. User entities are responsible for determining the necessity of a scheduled meetings encryption and enabling this feature.
21. User entities are responsible for setting data retention of scheduled videoconference meetings.

Incident Management

22. User entities are responsible for notifying BlueJeans if they detect or suspect a security incident related to the System.

F. Principal Service Commitments and System Requirements

BlueJeans designs its processes and procedures related to the System to meet its objectives for its Cloud-based Video Conferencing services. Those objectives are based on the service commitments that BlueJeans makes to user entities, relevant laws and regulations, and the financial, operational and compliance requirements that BlueJeans has established for the services.

Section III – BlueJeans’ Description of the Boundaries of the System

Security, availability, and confidentiality commitments to user entities are documented and communicated in Service Level Agreements (“SLAs”) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- ◆ Security principles within the fundamental designs of the Video Conferencing services that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- ◆ Use of encryption technologies to protect customer data both at rest and in transit.
- ◆ Relevant physical and logical security controls designed to prevent unauthorized access to the infrastructure and service that support the System.
- ◆ Role-based security model to secure access to data hosted within the System.
- ◆ Backup of customer data upon request.

BlueJeans establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other System requirements. Such requirements are communicated in BlueJeans’ System policies and procedures, System design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the System is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.