System and Organization Controls (SOC) 3 Report

Management's Report of Its Assertions on Bentley Systems, Inc.'s Connect Cloud Services System Based on the Trust Services Criteria for Security

For the Period July 1, 2019 to June 30, 2020

TABLE OF CONTENTS

SECTION ONE: REPORT OF INDEPENDENT ACCOUNTANTS

To: Bentley Systems, Inc.

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of Its Assertions on the Effectiveness of Its Controls over Bentley Systems, Inc.'s Connect Cloud Services System Based on the Trust Services Criteria for Security" (Assertion) that Bentley Systems' controls over the connect cloud services system (System) were effective throughout the period July 1, 2019 to June 30, 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the trust services criteria relevant to security (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*).

Service Organization's Responsibilities

Bentley Systems management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the connect cloud services system and describing the boundaries of the System;
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of the System; and
- Identifying, designing, implementing, operating, and monitoring effective controls over the connect cloud services system (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. 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. An examination involves performing procedures to obtain evidence about management's assertion, which includes:

- Obtaining an understanding of Bentley Systems' connect cloud services system relevant security policies, procedures, and controls;
- Testing and evaluating the operating effectiveness of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Bentley Systems' 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

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design and operating effectiveness of the controls to achieve Bentley Systems' connect cloud services system's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system of controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; b) breakdown of internal control at a vendor or business partner; and c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, management's assertion that the controls within Bentley Systems' connect cloud services system were effective throughout the period July 1, 2019 to June 30, 2020 to provide reasonable assurance that Bentley's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

CyberGuard Compliance, LLP

August 10, 2020
Orange, California

SECTION TWO: MANAGEMENT'S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER BENTLEY SYSTEMS, INC.'S CONNECT CLOUD SERVICES SYSTEM BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY

August 10, 2020

Scope

We, as management of Bentley Systems, are responsible for:

- Identifying the Bentley Systems connect cloud services system (System) and describing the boundaries of the System, which are presented in the section below (Attachment A) titled Description of Bentley Systems, Inc.'s connect cloud services system (Description);
- Identifying our principal service commitments and system requirements (Attachment B);
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in the section below (Attachment A) Description of Bentley Systems, Inc.'s connect cloud services system;
- Identifying, designing, implementing, operating, and monitoring effective controls over Bentley Systems' connect cloud services system (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements; and
- Selecting the trust services categories that are the basis of our assertion.

Bentley utilizes Microsoft Azure (Azure) as the hosting platform provider used for Bentley CONNECT Cloud Service. The Description (Attachment A) includes only the controls of Bentley Systems. The Description also indicates that certain trust services criteria specified therein can be met only if sub-service organizations' controls assumed in the design of Bentley Systems' controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of the sub-service organizations. However, we perform annual due diligence procedures for third-party sub-service organizations and, based on the procedures performed, nothing has been identified that prevents the sub-service organizations from achieving their specified service commitments.

The Description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Bentley Systems' service commitments and system requirements based on the applicable trust services criteria. The Description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Bentley Systems' controls.

We assert that the controls within the system were effective throughout the period July 1, 2019 to June 30, 2020, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to Security set forth in the AICPA's TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy, if subservice organizations and user entities applied the complementary controls assumed in the design of Bentley Systems' connect cloud services system controls throughout the period July 1, 2019 to June 30, 2020.

Bentley Systems, Inc.

SECTION THREE:

ATTACHMENT A: DESCRIPTION OF BENTLEY SYSTEMS, INC.'S CONNECT CLOUD SERVICES SYSTEM

Overview of Bentley Systems, Inc.'s Operations

Founded in 1984, Bentley Systems, Inc. is a global leader in providing infrastructure engineering software solutions for professionals and organizations involved in project delivery and operational performance of infrastructure assets. Bentley is dedicated to advancing infrastructure through comprehensive software solutions that span engineering disciplines, assets and lifecycle processes. Bentley's integrated software platform encompasses both the design and construction of infrastructure, which is referred to as project delivery, and the operation of infrastructure assets, which is referred to as asset performance.

The operations and corporate facilities are in Exton, Pennsylvania, USA. Bentley utilizes a combination local area network [LAN] / wide area network [WAN] to share data among its colleagues. The Information Technology [IT] operations are in the cloud and provided by Microsoft Azure. Bentley's colleagues have access to the cloud infrastructure 24 hours a day, 7 days a week, and 365 days a year. Bentley uses internal IT expertise and follows internal business and IT policies and procedures to support its daily IT administration and service operations.

In 2015, Bentley launched the Bentley CONNECT Cloud Service [BCCS] platform that allows users to leverage cloud technology to advance the digital maturity of the infrastructure industry throughout the infrastructure lifecycle. Bentley constantly strives to advance the BCCS platform by releasing new Cloud Services. In 2019 Bentley expanded BCCS to include Digital Twin cloud Services. BCCS is designed to keep users' data secure with enterprise grade security.

The environment is stable and there have been no significant changes to the system. Bentley prepared this description to meet the common needs of a broad range of users. Understandably, as written, this may not include every aspect that each user may consider important to address their unique needs.

System Overview

The System is comprised of the following components:

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

Infrastructure

BCCS is developed by Bentley software groups, operated and managed by Bentley Information Technology Operations [IT Operations] and Bentley CONNECT Service Management Team [BCSM]. The BCCS infrastructure is designed with multiple layers of security, including encrypted secure file transfer, isolated networking, and application level user configured controls. Below, in Diagram 1, is a graphical overview of the BCCS infrastructure showing the security layers and the interrelationships between the applications and supported user interfaces.

Azure PaaS

BCCS is implemented on the Microsoft Azure Platform-as-a-Service [PaaS]. Bentley performs specific activities to monitor the environment provided by the Microsoft Azure PaaS. Bentley is directly responsible for application security of BCCS software deployed within the PaaS.

Microsoft provides the physical infrastructure of the PaaS and is responsible for the security and availability of the platform in general. Bentley reviews the Microsoft Azure SOC1, SOC2, and ISO 27001 assessments and reports regularly to verify the applicable physical, environmental, and operational security controls are in place per contractual agreements.

The below high-level architecture describes the core components of the system in respect to each other. Detailed descriptions of each component follow.

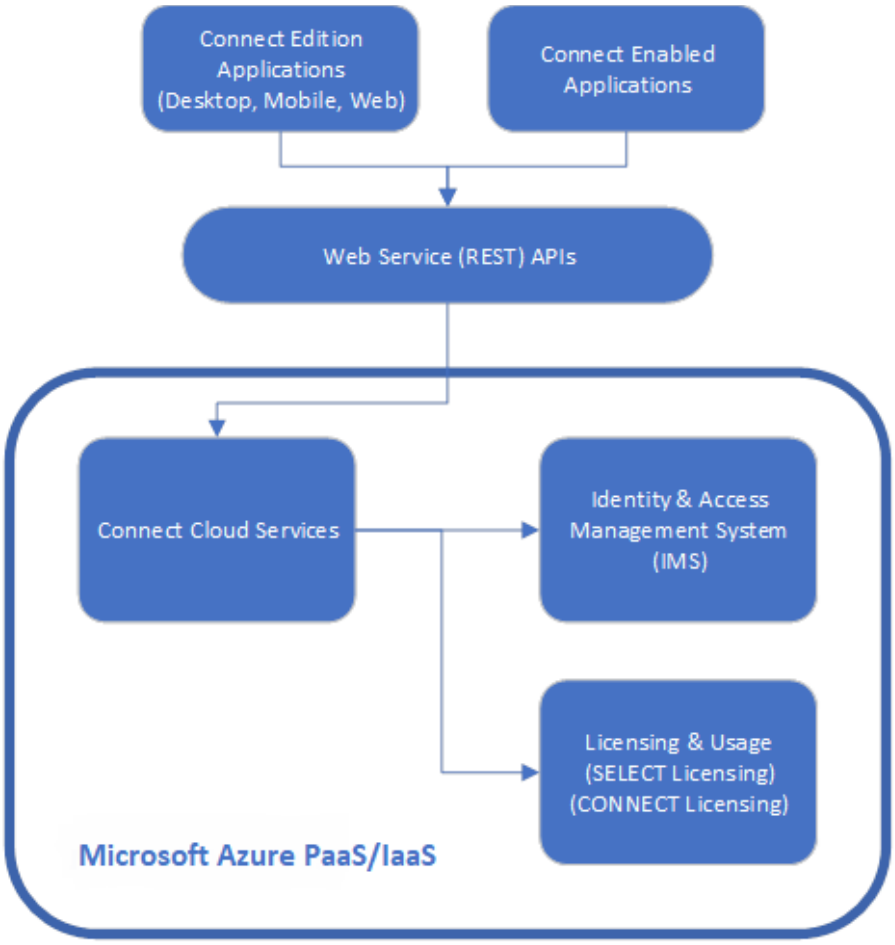

Diagram 1 BCCS architecture

Software

CONNECT Edition Applications

This is defined as any Bentley applications with CONNECT functionality integrated and directly enabled as part of the product installation via CONNECTION Client. This includes access to BCCS.

CONNECT Enabled Applications

This is defined as any Bentley applications that have the ability to communicate and leverage with a locally installed CONNECTION Client application on the desktop. CONNECT Enabled applications are previous editions of current Bentley applications with limited CONNECT functionality enabled by CONNECTION Client. As Bentley continues to innovate and release new versions of its software platforms, CONNECT Enabled applications will eventually be deprecated.

Bentley CONNECT Cloud Services [BCCS]

BCCS is comprised of multiple services that include several core services available to subscribed users. At the center of the system are two main services; Business and Content services. Business services are what provides the input/output routines that support BCCS to the user. Content services are the sub-systems that store, access, change and process user created data supporting all business services. BCCS provides a central functionality of the Bentley Software family of applications. BCCS forms the foundation for various Bentley brands including iTwin Services, ProjectWise 365 Services, etc.

Identity and Access Management

BCCS has been developed with leading industry identity and access management that secures application access. Implementing industry-standard protocols, the system is secure through all access points including web users, desktop clients and mobile clients. All communications are encrypted while in transit and protected against unauthorized access.

BCCS user authentication is provided by the Bentley Identity Management System [IMS]. Bentley IMS functions as both an Identity Provider (IdP) and a Service Provider. This allows for a single user logon that is shared with multiple applications, platforms and services. Bentley IMS has the capability to allow an organization to federate with their own identity provider to provide federated identity functionality to their users. This allows organizations to apply their own IT policies on the user authentication. Bentley IMS supports just-in-time provisioning of federated users in order to simplify the administration of these users. Bentley IMS provides company administrators with a User Management interface which allows the designated administrators to perform delegated management of their users. This includes the ability to add/remove user associations with their account, assign users to groups, and assign roles.

Licensing and Usage

Licensing is provided by SELECTserver and Subscription Entitlement Service [SES]. Licensing servers and services provide runtime components required for applications to access Bentley Cloud Services and Bentley applications. The components provided are common across all applications and are required to participate in capabilities provided through the CONNECT Edition and CONNECT Enabled applications.

Licensing Technology

SELECT Licensing enables all Bentley SELECT licensed products to be activated via the Bentley SELECTserver. BCCS utilizes the same centralized application license verification mechanism called Bentley SELECTServer. The purpose of SELECTServer is to verify licensing for the CONNECT-enabled Bentley applications the user is utilizing to access BCCS.

Diagram 2 BCCS Software

The SES delivers a licensing process that has been built from the ground up to improve the Bentley customer's software delivery and usage experience. It is a cloud service built on and based on the latest Microsoft Azure PaaS services. It provides many additional capabilities. The SES will eventually replace SELECT Licensing (targeted roadmap by end of 2020, although subject to change) to enhance Bentley customers' licensing experience and allow company administrators to better manage their license usage.

Data

For specific information regarding data and Bentley's usage of customer information, refer to Bentley's Privacy statement, as published on the external website. This statement provides information about how Bentley collects, uses, discloses, transfers, and stores customer information, who Bentley shares it with, as well as the choices customers have regarding their information.

To utilize BCCS, customers upload their data for storage and processing. Bentley utilizes customer usage data to support the services and products subscribed to by the customer in accordance with the Service Level Agreements as defined in the executed contract.

Customer Usage Data

As defined above, please reference Bentley's Privacy statement. Information specific to the products and applications used by the customer can be found in their executed software license agreement or terms of service.

Data Ownership

As defined above, please reference Bentley's Privacy statement. Customers own the data they upload and have the ability to share this data for collaboration or other purposes. Bentley reserves the right to take appropriate actions on data stored that is reported or indirectly discovered to be illegal in nature or has a nefarious purpose.

People

Bentley Cloud Services Management team is supported by the following functional departments, containing Subject Matter Experts in each of their relevant areas, as described below. Within these departments are colleagues who are accountable and responsible for successfully operating the controls , and/or provide support the SOC2 control framework.

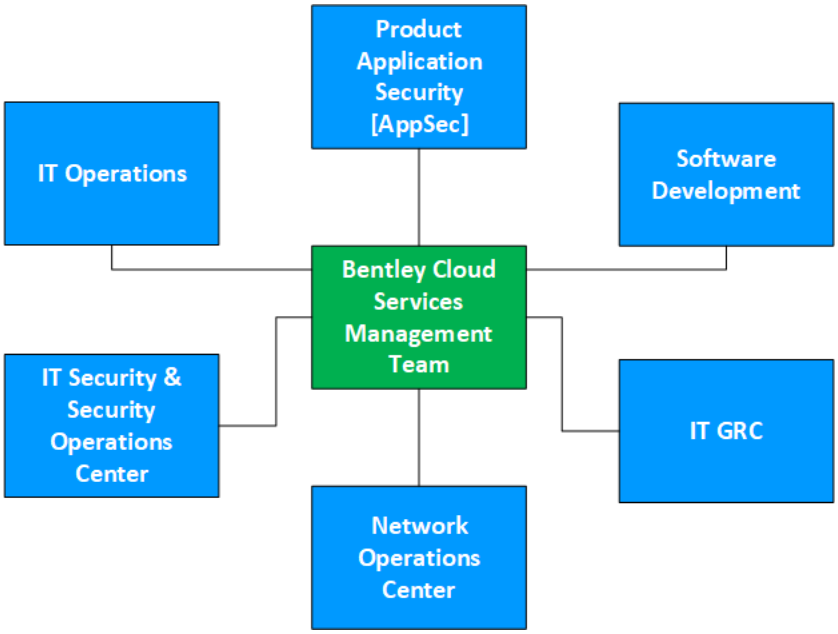

Diagram 3 Interdepartmental support model - Bentley CONNECT Cloud Services. This depicts colleagues accountable for control operation.

Bentley Cloud Services Management

The Bentley Cloud Services Management team is responsible for infrastructure support and deployment of all services to production. This includes providing proactive/reactive cloud production system monitoring for the application layer. The team also provides other services, such as production issue troubleshooting, defect detection and logging, security analysis/guidance, operational test verification/scheduling, operational test framework development/ownership, and analytics logging. The BCSM team is also involved throughout the Release Process.

Product Application Security [AppSec]

Bentley's AppSec team is responsible for the secure development of each Cloud Service. This team consists of colleagues responding to potential incidents and addressing pre-release issues to ensure risks are detected, assessed and mitigated at all levels. They also define standards, processes and procedures for securing code including prevention, detection and response.

IT Operations

Bentley's IT Operations team is responsible for managing and maintaining Bentley's network infrastructure.

IT Security

Bentley's IT Security is responsible for defining and executing the corporate cybersecurity strategy. This in part includes defining the appropriate risk-based detection and monitoring, policy mandates and required security awareness training. Bentley's security strategy conforms with industry standards and control framework best practices.

Bentley's IT Security department includes a designated Security Operations Center [SOC]. The SOC team coordinates the activities related to Information security and the safeguarding of user data. They are responsible for identifying, responding to and recovering from all security-related incidents reported both internally and externally.

Software Development

Bentley's Software Development group is comprised of cross-functional units each focusing on brands within their realm of expertise. Their objective is to continually improve products and services to serve the customers' needs. Through a variety of established communication channels, information regarding feature requests and other related enhancements is collected and disseminated to the developers. These are evaluated and prioritized to be incorporated in future iterations.

IT Governance, Risk and Compliance [IT GRC]

Bentley's IT GRC team is responsible for oversight of governance, risk and compliance of the SOC2 Type II Certified Bentley CONNECT Services environment. This team works with the control owners (in Diagram 3 above) to define controls and ensure they are successfully operating. This includes a continuous monitoring of control health, along with conducting internal risk assessments, internal audits and facilitating the annual independent audit.

Network Operations Center

Bentley's Network Operations Center [NOC] is responsible for monitoring all systems and escalation of events to the appropriate groups. This team is the first point of contact for issues reported from any of the groups in Diagram 3, along with any internal colleagues. The NOC is a 24/7/365 team on monitoring and escalation of events and incidents.

Data Office

Bentley introduced a new Data Office in June 2019 to help optimize data as a critical asset and competitive advantage, aligning data to our key objectives, and building a useful, scalable, and robust data platform, enabling quick and accurate data access for colleagues and users.

Policies and Procedures

BCCS has implemented policies and procedures necessary to operate in-scope controls and functional areas. The following documentation was created utilizing the Information Technology Infrastructure Library [ITIL] framework and other security frameworks for best practices for delivering IT services:

- Information Security
- Physical and Environmental
- Risk Assessment
- Supplier Relationship
- Incident Management
- Business Continuity
- Human Resources
- Operations Security
- Communications
- Compliance and in-scope controls

In addition, specific operational protocols are implemented in the following areas:

- Policy Management
- Access Management
- Access Control
- Cryptography
- Continuous Compliance Control Monitoring
- Internal Audits

Scope

The scope is comprised of the Bentley CONNECT Cloud System [BCCS], including the specific aspects as necessary to provide its services, as follows: infrastructure, software, data, people, and procedures. The BCCS boundaries include applications and infrastructure that support services provided to its users.

The scope includes Bentley's service commitments and system requirements based on the Trust Services Criteria relevant to security as outlined in the *TSP Section 100: 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Control Environment

Key facets of Bentley's control environment for all processes performed by the Company are summarized below. These areas include the following:

- Integrity and Ethical Values
- Commitment to Competence
- Board of Directors Participation
- Management's Philosophy and Operating Style
- Human Resources Policies and Practices
- Organizational Structure and Assignment of Authority and Responsibility

Integrity and Ethical Values

Integrity and ethical values are essential elements of Bentley's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of Bentley's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. Specific control activities that the service organization has implemented in this area are described below:

- The Code of Conduct contains organizational policy statements and codes of conduct to which colleagues are required to adhere.
- Colleagues electronically acknowledge that they have reviewed the Code of Conduct and understand their obligation to adhere to the policy statements.
- Colleagues sign an agreement that documents their understanding of Bentley's policy and procedure for handling sensitive or confidential information.

Commitment to Competence

Bentley's management defines competence as the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into requisite skills and knowledge. Bentley is focused on hiring experienced colleagues to meet required business needs. Specific control activities that the service organization has implemented in this area are described below:

- Bentley is part of the technology industry, which is a rapidly evolving field. Therefore, job descriptions are modified as necessary to meet business needs and to ensure we are sourcing the most highly qualified candidates.
- Colleagues are provided with orientation, initial on-boarding training, continuous learning opportunities and supervision requisite for each position.

Board of Directors Participation

Bentley's Board of Directors is committed to control compliance, including the oversight of management activities.

Management's Philosophy and Operating Style

Bentley's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward information processing, accounting functions, and personnel. Management holds periodic meetings to discuss operational issues.

Human Resources Policies and Practices

Bentley's Human Resources policies and procedures relate to colleague hiring, orientation, training, evaluating, promoting, compensating, and remedial actions. Specific control activities that the service organization has implemented in this area are described below:

- Human Resources utilizes new hire document lists to ensure that specific elements of the hiring process are consistently executed, and a copy of the documents are maintained in the colleague file.
- Management designates performance and potential ratings evaluations for each colleague on an annual basis.
- Management has established colleague termination procedures that guide personnel in the termination process.

Organizational Structure and Assignment of Authority and Responsibility

Bentley's organizational structure provides the framework within which its activities for achieving entity wide objectives are planned, executed, controlled, and monitored. Bentley's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. Bentley has developed, and periodically reviews, an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities. Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are communicated to colleagues and updated as needed.

BCCS organization's control environment is primarily managed by the following management chain. This diagram depicts a consolidated organizational structure showing the relationship between Executive Management, Management and the Control Accountables. It is not all-inclusive of all roles within the organizational reporting line structure.

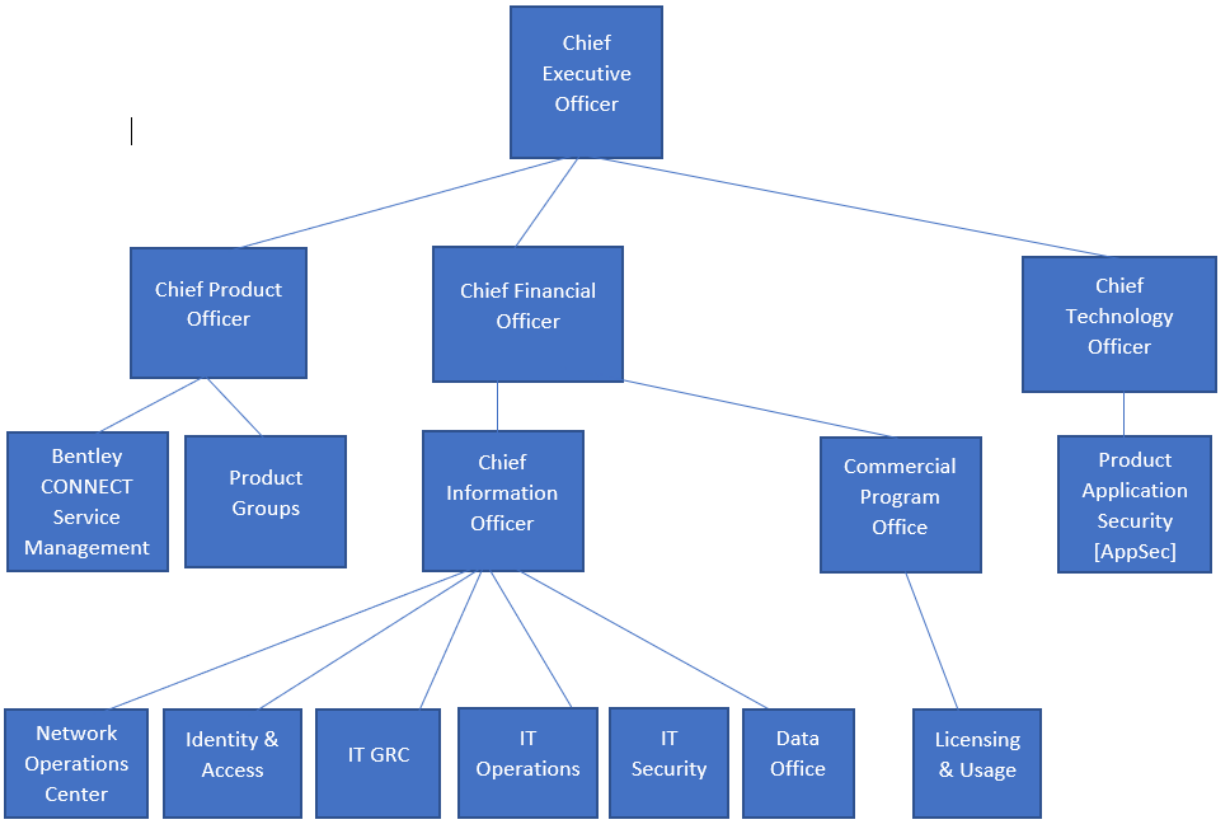

Diagram 4 BCCS Management Chain

Risk Assessment

Bentley has developed a robust and repeatable Risk Assessment methodology that has been tested in several internal cycles for various systems and applications. This methodology incorporates several ideologies from various frameworks such as ISO/IEC 27001:2013, ISO/IEC 27005:2011, NIST SP 800-53 and SOC2. The below summarizes the assessment lifecycle as it is applied to BCCS and supporting systems:

Diagram 5 Assessment Lifecycle

The key components of the Bentley Risk Assessment Process include these phases:

1. Kick-Off Meeting
2. Guided Assessment
3. Final Risk Report
4. Post Assessment Tasks
    a. Mitigation/Remediation Planning
    b. Mid-Cycle Assessment Review/Report

Kick-Off Meeting

The initial phase in the risk assessment process is to determine the key colleagues and groups that are required to participate. The scope of the risk assessment is defined to include all responsible individuals with a high level of efficiency.

Guided Assessment

The second phase in the risk assessment process is designed to provide the greatest efficiency and most complete assessment of risk for the system in scope. Each colleague that participates is considered to be in a management position or is considered a Subject Matter Expert with the system in scope. The assessment owner has the ability to review the raw risk identified and provide additional experience and knowledge to determine the final risk rating for each control question.

Final Risk Report

The third phase in the risk assessment process generates a Risk Assessment Report that is issued as part of official internal documentation. This document will include approvals from all applicable management.

Post Assessment Tasks

Mitigation/Remediation Planning

The fourth phase in the risk assessment process develops the mitigation and/or remediation plans required to reduce or eliminate risk details in the Risk Assessment Report.

Mid-Cycle Assessment Review/Report

The final phase in the risk assessment process is a high-level review of risks identified in phase three, current status on mitigation and remediation plans, and any documented risk acceptance from applicable management. The final step in the risk assessment process is to issue a follow-up report, added as an addendum to the official report that details updates from the mid-cycle review.

Monitoring

The Chief Information Officer [CIO] monitors the quality of internal control performance as a normal part of their activities. The CIO relies on their teams to be involved in day-to-day activities and regularly review various aspects of internal and customer-facing operations to (i) determine if objectives are achieved, (ii) identify any new risks that develop, and (iii) implement appropriate measures to address those risks. Bentley adopts a proactive approach to the monitoring of application security to ensure that issues or risks are addressed before becoming significant problems.

Monitoring of the Subservice Organization

Bentley utilizes Microsoft Azure (Azure) as the hosting platform provider used for Bentley CONNECT Cloud Service.

The following Complementary Subservice Organization Controls (CSOCs) are expected to be operating effectively at Azure, alone or in combination with controls at Bentley, to provide assurance that the required trust services criteria in this report are met.

Information and Communication

Description of Computerized Information Systems

The Bentley's internal network is Ethernet-based and is logically grouped into a single domain. The network consists of multiple business-class systems and Active Directory is utilized to manage access rights and permissions. Industry standard network operating and database systems from major vendors are used to support its network architecture, support database,

and application systems. Bentley has workstations throughout the Company that have connectivity to the network.

In addition, BCCS is a web-based system which resides in a secure cloud-based environment. Users access the system through the Internet and data communications with clients use TLS best practices.

Communication

Bentley management sends periodic communications as may be necessary regarding any impact to the in-scope systems. This includes organizational changes, along with policies and procedures. Established policies and procedures are formally documented and clearly communicated to all employees.

Description of Complementary User Entity Controls

BCCS was designed with the assumption that user entities will have internal controls to complement this system. The application of such internal controls by user entities is necessary to achieve certain criteria identified in this report. There may be additional criteria and related controls that would be appropriate for the processing of user entity transactions which are not identified in this report.

This section describes certain controls that Bentley assumes its user entities have implemented for achievement of criteria identified in this report. The complementary user entity controls presented below should not be regarded as a comprehensive list of all the controls that should be employed by user entities.

Provisioning Accounts

- Account administrators are responsible for restricting authority of provisioning new user accounts within any BCCS.

Termination Procedures

- Account administrators are responsible for restricting authority of terminating user accounts within any BCCS.

Network Security

- Users are responsible for ensuring user owned or managed applications, platforms, databases, and network devices that may process or store data derived from BCCS are logically secured.

General Controls

- Users are responsible for ensuring user access to reports and other information generated from BCCS is restricted based on business need.

- Users of BCCS are responsible for maintaining appropriate IT General Computer Controls and Application Controls.

Regulatory, Compliance, and Service Agreements

- Users are responsible for compliance with all applicable laws and regulations.
  Users are responsible for reviewing and approving the terms and conditions stated in service agreements with Bentley.

SECTION FOUR:

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

In 2015, Bentley Systems, Inc. (Bentley) launched the Bentley CONNECT Cloud Service (BCCS) platform that allows users to leverage cloud technology to advance the digital maturity of the infrastructure industry throughout the infrastructure lifecycle. BCCS is designed to keep users' data secure with enterprise grade security.

BCCS provides a central functionality of the Bentley Software family of applications including the foundation for various brands such as iTwin Services, ProjectWise 365 Services, etc. Other services include Licensing and Usage along with Identity and Access Management. Bentley constantly strives to advance the BCCS platform by releasing new Cloud Services.

BCCS is implemented on the Microsoft Azure Platform-as-a-Service [PaaS]. Bentley performs specific activities to monitor the environment provided by the Microsoft Azure PaaS. Bentley is directly responsible for application security of BCCS software deployed within the PaaS. Microsoft provides the physical infrastructure of the PaaS and is responsible for the security and availability of the platform in general. Bentley reviews the Microsoft Azure SOC2 and ISO 27001 reports regularly to verify the applicable physical, environmental, and operational security controls are in place.

BCCS has implemented policies and procedures necessary to operate in-scope controls and functionality. The following documentation was created utilizing the Information Technology Infrastructure Library [ITIL] framework and other security frameworks for best practices for delivering IT services:

- Information Security
- Physical and Environmental
- Risk Assessment
- Supplier Relationship
- Incident Management
- Business Continuity
- Human Resources
- Operations Security
- Communications
- Compliance and in-scope controls

In addition, specific operational protocols are implemented in the following areas:

- Policy Management
- Access Management

- Access Control
- Cryptography
- Continuous Compliance Control Monitoring
- Internal Audits

Key facets of Bentley's control environment for all processes performed by the Company are summarized below:

- Integrity and Ethical Values
- Commitment to Competence
- Board of Directors Participation
- Management's Philosophy and Operating Style
- Human Resources Policies and Practices
- Organizational Structure and Assignment of Authority and Responsibility

Services and responsibilities are documented and agreed to by both parties in executed Agreements. Requirements are also outlined in Bentley's online Cloud Services Terms of Services provided to its users through its public website. The BCCS platform, system description and control program are designed to support and meet its contractual commitments.

BCCS designs its processes and procedures related to the System to meet its objectives for its services. These objectives are based on the service commitments made to user entities. Security commitments are documented and managed through the control program. The security commitments include, but are not limited to, the following:

1. Bentley has formalized core values that demonstrate the importance of integrity and ethical values. The core values are available to employees via the intranet.
2. Roles and responsibilities are defined in written job descriptions specifying the responsibilities and professional requirements for key job positions.
3. All personnel are required to attend the Company's security awareness training at the time of hire and annually thereafter.
4. Bentley CONNECT maintains a listing of custom internal controls that identifies the business owners. The internal controls are communicated to the business owners, reviewed, and updated annually.
5. The Company has a comprehensive incident response process that is communicated to Network Operations Center staff and is regularly updated.
6. Bentley CONNECT provides a status page for external parties to track outages for Bentley CONNECT controlled systems.
7. A formal cyber risk assessment is performed annually to identify and evaluate internal and external security threats. The likelihood, impact, significance, and mitigation efforts are identified.

Bentley establishes operational requirements supporting the achievement of security commitments. These requirements are continuously monitored through oversight of the control program.