Enablon, a subsidiary of Wolters Kluwer

Enablon Hosted Solution System

System and Organization Controls Report

Report on Controls Placed in Operation and Tests of Operating Effectiveness Relevant to Security

For the Period
May 1, 2022, to April 30, 2023

I. Independent Service Auditor's Report

To Management of Enablon:

Scope

We have examined Enablon, a wholly owned subsidiary of Wolters Kluwer, accompanying description of its hosted solution system in Section III, titled "Enablon's Description of its Hosted Solution System," throughout the period May 1, 2022, to April 30, 2023 (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) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period May 1, 2022, to April 30, 2023, to provide reasonable assurance that Enablon's 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*).

Enablon uses subservice organizations, Deft and Equinix, to provide data center hosting, maintenance and support of the infrastructure, and physical security and environmental protection controls of the data center facilities. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Enablon, to achieve Enablon's service commitments and system requirements based on the applicable trust services criteria. The description presents Enablon's controls, the applicable trust services criteria and the types of complementary subservice controls assumed in the design of Enablon's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section V, titled "Other Information Provided by Enablon," is presented by Enablon management to provide additional information and is not part of the description of the service organization's description of its hosted solution system. Information about Enablon's management responses to testing exceptions has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

Service Organization's Responsibilities

Enablon 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 Enablon's service commitments and system requirements were achieved. In Section II, Enablon has provided an assertion about the description and suitability of design and operating effectiveness of the controls stated therein. Enablon is also responsible for preparing the description and assertion, including the completeness, accuracy and method of presentation of the description and assertion, providing the services covered by the description, selecting the applicable trust services criteria and stating the related controls in the description, and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their information needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of the controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested, and the nature, timing and results of our tests are presented in Section IV.

Opinion

In our opinion, in all material respects:

- The description presents Enablon's hosted solution system that was designed and implemented throughout the period May 1, 2022, to April 30, 2023, in accordance with the description criteria.

- The controls stated in the description were suitably designed throughout the period May 1, 2022, to April 30, 2023, to provide reasonable assurance that Enablon's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organizations applied the complementary controls assumed in the design of Enablon's controls throughout that period.

- The controls stated in the description operated effectively throughout the period May 1, 2022, to April 30, 2023, to provide reasonable assurance that Enablon's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Enablon's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Enablon; user entities of Enablon's hosted solution system during some or all of the period May 1, 2022, to April 30, 2023; business partners of Enablon subject to risks arising from interactions with the hosted solution system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization

- How the service organization's system interacts with user entities, business partners, subservice organizations and other parties

- Internal control and its limitations

- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements

- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

RSM US LLP

Los Angeles, California
August 7, 2023

II. Enablon's Assertion

We have prepared the accompanying description of Enablon's hosted solution system in Section III, titled "Enablon's Description of its Hosted Solution System," throughout the period May 1, 2022, to April 30, 2023 (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 hosted solution system that may be useful when assessing the risks arising from interactions with Enablon's system, particularly information about system controls that Enablon 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 (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*).

Enablon uses subservice organizations, Deft and Equinix, to provide data center hosting, maintenance and support of the infrastructure, and physical security and environmental protection controls of the data center facilities. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Enablon, to achieve Enablon's service commitments and system requirements based on the applicable trust services criteria. The description presents Enablon's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Enablon's controls. The description does not disclose the actual controls at the subservice organizations.

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

- The description presents Enablon's hosted solution system that was designed and implemented throughout the period May 1, 2022, to April 30, 2023, in accordance with the description criteria.

- The controls stated in the description were suitably designed throughout the period May 1, 2022, to April 30, 2023, to provide reasonable assurance that Enablon's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of Enablon's controls throughout that period.

- The controls stated in the description operated effectively throughout the period May 1, 2022, to April 30, 2023, to provide reasonable assurance that Enablon's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Enablon's controls operated effectively throughout that period.

III. Enablon's Description of its Hosted Solution System

Overview of Operations

Background

Enablon, a wholly owned subsidiary of Wolters Kluwer, is a provider of integrated software solutions for Environmental, Social and Governance (ESG), Governance, Risk and Compliance (GRC), Engineering and Operations, and Environmental, Health, Safety and Quality (EHSQ). Enablon has a global headquarters in the Paris area (Bois-Colombes) of France, and a North American headquarters in Chicago, Illinois, and office facilities in The Hague, the Netherlands. Enablon has more than 700 personnel globally.

In July 2016, Wolters Kluwer completed an acquisition of Enablon, which, at the time, was delivering sustainability, environmental health and safety (EH&S), and risk and compliance products and services. Enablon is supported by the Wolters Kluwer Corporate Performance and Environmental, Social & Governance (CPESG) division. The parent company, Wolters Kluwer, provides certain shared administrative services to Enablon, such as accounting, information security and HR functions, but Enablon personnel remain responsible for the operations, management and oversight of the Enablon solution.

In October 2018, Wolters Kluwer acquired eVision, with its main office located in The Hague, the Netherlands, which focused on operational risk management (ORM) software and services. The ORM software and services has been adopted into the Enablon Global Cloud Services family and the service has been renamed to the Enablon Global Cloud Services: Public Cloud.

In February 2020, Wolters Kluwer completed an acquisition of CGE Risk, which, at that time, was delivering products and services in the area of barrier-based risk management, including the Bowtie suite, with its office located in The Hague, the Netherlands.

Enablon's North American (NAM) operations and European, Middle East and Africa (EMEA) operations are primarily supported from the North American headquarters in Chicago, Illinois, and the global headquarters in the Paris area (Bois-Colombes) of France. Internally, some shared services throughout the company, such as accounting, IT, information security and HR, are supported by personnel located in Enablon's global headquarters in the Paris area (Bois-Colombes) of France, Enablon's NAM headquarters in Chicago, Illinois, and the parent company, Wolters Kluwer.

Overview of Services Provided

Enablon supports highly complex project implementations. Enablon provides the ability to support a large variety of use cases that go beyond traditional solutions to address complex requirements in risk, EH&S and sustainability.

The Enablon solution is a platform of EH&S and operations risk management software that uses a variety of modules to provide specific services to customers based on their needs. Customers subscribe to the Enablon platform, and their users have access to the specific modules within the subscription. Enablon maintains specific databases that are designated for the customer's environment and store data that has been uploaded, entered or transmitted by the customer.

Subscription modules within the Enablon platform include, but are not limited, to the following categories:

- Business efficiency—Including a focus on key metrics, forecasting, objective management, profitability analyses and action plans

- Compliance—Including a focus on compliance management, audit management, policy management, mobile audits and document control features

- Green business—Including a focus on waste, water, air quality and environmental management systems

- Safe operations—Including a focus on Occupational Safety and Hazard Administration (OSHA) compliance, hazard analysis, permit management and safety training

Enablon uses two third-party data center providers to store and process customer data, typically based on geographic location of the customer. The chosen data center depends on customer requirements for the location of their data. Enablon solutions for EMEA customers are hosted at the Equinix data center facilities in France; the Enablon solutions for customers in North America are hosted by a Deft data center in the United States. For the U.S.-based data center, Enablon outsources hosting to Deft.

Scope of Report and Boundaries of the System

The scope of the report includes the security trust services category for Enablon's NAM and EMEA operations supporting the web-based Enablon solutions system. The scope is limited to Versions 8 and 9 of the Enablon hosted solution. The personnel and functions supporting the NAM and EMEA operations are primarily located in Chicago, Illinois, and the Paris area (Bois-Colombes) of France and are included in the scope of this report.

The scope of this report does not include Enablon's implementation services offering, public cloud services, or other versions of Enablon hosted solutions outside of application server Versions 8 and 9.

Enablon uses subservice organizations, Deft and Equinix, to provide data center hosting, maintenance and support of the infrastructure, and physical security and environmental protection controls of the data center facilities. The scope of this report includes only the applicable trust services criteria and related controls of Enablon and excludes the criteria and related controls of the subservice organizations.

The Enablon production network, where customer data travels, is completely separated and segregated from the corporate network. Customers gain access to the Enablon solution via the internet. Application users access the Enablon solution through a secured HTTPS connection that first authenticates users through a firewall and intrusion prevention system (IPS) layer, which is described later in this report. Enablon is responsible for the security of data upon receipt of customer data.

Clients using the Enablon hosted solution are each provided separate databases with separate user accounts and passwords to operate the hosted software. There is no commingled data used in the Enablon hosted solutions environment. Each customer's data is isolated to a specific data center.

The system boundaries start when data is input to the application, via the web interface. Customers input data into the system and are responsible for the accuracy of the information entered. System outputs consist of screen displays, customized reports available through the application, and data files and documents transmitted to third parties on behalf of the customers. Some customers may use Enablon to securely transmit reports, claims or forms to third parties (such as insurance carriers) on their behalf. Data transmissions to third parties are encrypted during transit using the Transport Layer Security (TLS) protocol. Once the user has extracted the necessary data from the system, the data exits the system boundaries. End user access is restricted to a public-facing Enablon website that is secured through HTTPS and requires user authentication. IT administrators must remotely connect to the Enablon application server via a VPN connection.

The mobile functionality of the Enablon platform is outside the boundaries of the system and is excluded from the scope of the report.

Principal Service Commitments and System Requirements

Enablon designs policies, procedures and controls to meet its objectives for the security of the Enablon hosted solution. Those objectives are based on meeting the service commitments that Enablon makes to user entities. Enablon has implemented an information security policy that encompasses a variety of processes, procedures and policies for managing information and technology assets intended to protect Enablon hosted solutions, as well as the underlying and supporting applications and data.

Security commitments are documented and communicated to user entities in the master services agreement (MSA). The agreements are used when creating new customer relationships and are provided to customers to document their agreement and communication of responsibilities, commitments and requirements (as applicable). The MSA communicates responsibilities of both parties, and the Hosted Software Information Security Framework documents Enablon's security commitments, as well as system requirements. The MSA is standard across both the NAM and EMEA regions and proposed by default. The final agreements with customers may include negotiated changes. However, these changes usually do not impact security commitments set forth in the agreements. The service commitments made to user entities are consistent between NAM and EMEA. The principal service commitments and system requirements listed below are a baseline set of requirements that apply to a broad range of customers. Individual customers may have specific requirements that are more stringent or more specific than those documented below:

Principal Service Commitments

Security

- Enablon maintains and enforces safety and physical security procedures with respect to the Cloud Subscription Services and protection of client data that is input into, accessed through or maintained or stored in a database within the hosted software in accordance with the Enablon Hosted Software Information Security Framework.

- Enablon, in conjunction with its applicable hosting service providers, maintains a security incident management process. This process defines steps for minimizing loss of data, vulnerability identification, vulnerability remediation and notification guidelines. Enablon shall promptly report to the user entity any compromise of security related to customer data within several working days of Enablon having ascertained that a client's data has been impacted.

- Data is backed up regularly and encrypted when replicated to tape medium.

System Requirements

Enablon has established system requirements for Enablon's hosted solution in the Enablon Hosted Software Information Security Framework, which is an addendum to the MSA. System requirements are also communicated in Enablon's information security policies and procedures, and system design documentation. Some key system requirements include the following:

- Tone at the top is permeated across the business lines and activities providing discipline and structure and communicated to personnel.

- Risks are identified, addressed, investigated and resolved, and changes in internal and external factors are reevaluated to support an ongoing culture of risk management.

- Logical and physical access to programs, data and information assets, including data transmissions between the service organization and its user entities and other outside entities (e.g., business partners, customers, subservice organizations), is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

- Application and system processing is authorized and executed, and deviations, problems and errors are identified, tracked, recorded and resolved.

- Changes to application programs and related data management systems are authorized, tested, documented, approved and implemented.

- Configuration and administration of security tools and techniques, as well as monitoring controls, are designed to identify and respond to security violations in a timely manner and mitigate risks to the achievement of objectives to acceptable levels.

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 hosted solution.

Components of the System Used to Provide the Service

Infrastructure and Software

The following table describes the applications and related systems within the scope of this report:

Application/System	Process/Transactions	Purchased or Developed	Platform and Operating System	Data Environment
Enablon Solution	The integrated platform for EH&S and risk compliance software solutions	Developed	Microsoft Windows 2012 R2 and Windows 2016	SQL Server 2012 and 2016

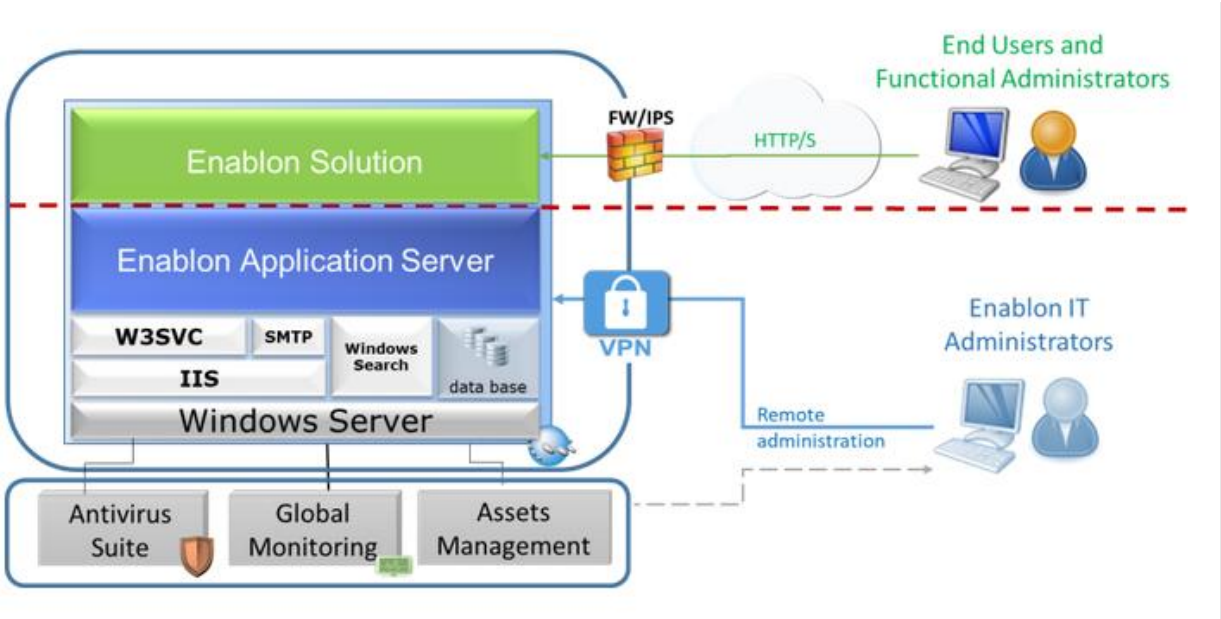
The additional applications/utilities listed below are mentioned in Sections III and IV of this report and may support some facets of the delivery of the services described. These utilities are covered within the scope of the report to the extent that they support achieving the criteria and were not within the boundaries of the system.

Application/System	Process/Transactions	Purchased or Developed	Platform and Operating System	Data Environment
Helpdesk	Ticketing system used for tracking, monitoring and resolving customer support issues in the production environment (Helpdesk is available to customers through a web interface, as well as internally to customer support and IT personnel. Helpdesk is also the inventory system for the management of customer instances and allows direct linking of tickets to a customer instance.), as well as enhancement requests	Developed	Microsoft Windows	SQL Server

Application/System	Process/Transactions	Purchased or Developed	Platform and Operating System	Data Environment
GLPI	Asset management and issue tracking system used by IT personnel for maintaining an inventory of Enablon's IT assets, including hardware and software inventory (IT personnel also use GLPI to track the activities of IT personnel when working on nonapplication development activities.)	Purchased	Linux	MySQL
Microsoft Azure DevOps Services/Git	Source code repository and development tool used by application development personnel for creating and modifying the source code supporting the Enablon solution (Git is a free option provided by Azure DevOps, which is the source code repository for the Enablon solution.)	Purchased	Microsoft Windows	SQL Server
SOFTWARE	Workflow management system used by research and development personnel to document and track development and quality assurance activities related to the Enablon application	Developed	Microsoft Windows	SQL Server
RISE	An instance of the Enablon solution that is used internally by Enablon personnel to manage and track Enablon's activities related to compliance, audit, internal control, risk and improvement action plans (This instance of the Enablon solution does not contain customer data and is restricted to internal users.)	Developed	Microsoft Windows	SQL Server
Atlassian Confluence	A content management tool used to help teams collaborate and share knowledge efficiently (Teams and users can create pages and blogs that can be commented on and edited by all members of the team.)	Purchased	Microsoft Windows	PostgreSQL
Enablon Client Portal	Comprehensive product documentation is available and delivered via the Enablon Client Portal (hosted by Enablon on Atlassian Confluence Server).	Purchased	Microsoft Windows	NA
Sophos UTM	A Unified Threat Management (UTM) tool that provides the network security package, including firewall, IPS/intrusion detection system (IDS), VPN, etc., in a single modular appliance.	Purchased	N/A	N/A

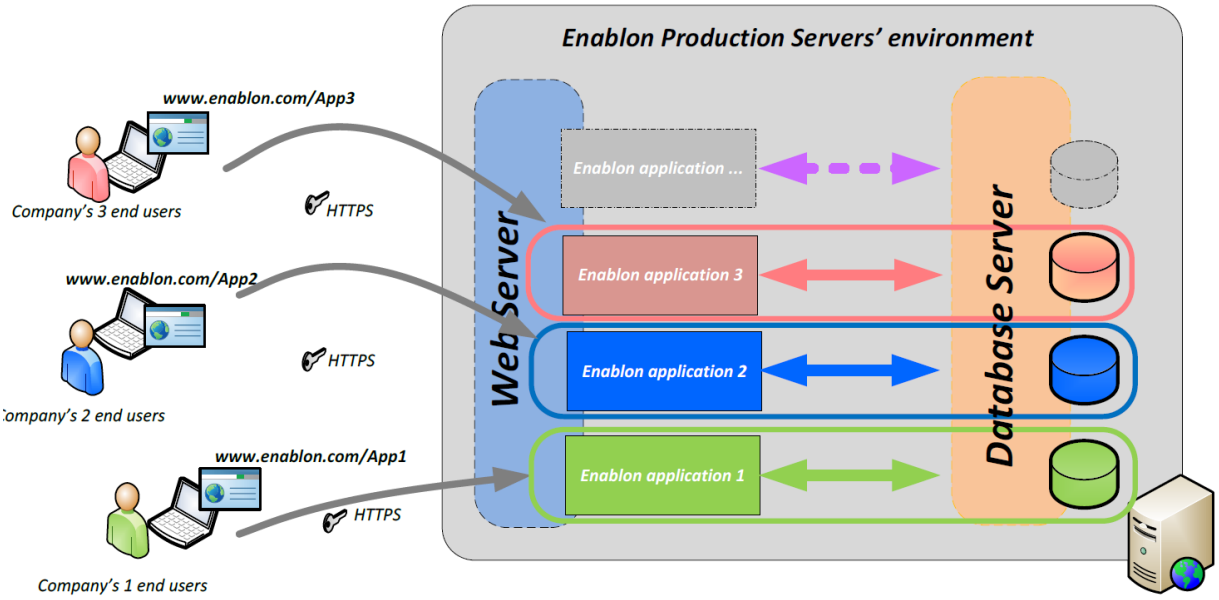
Application/System	Process/Transactions	Purchased or Developed	Platform and Operating System	Data Environment
Antivirus Windows McAfee	This service provides an antivirus engine and updated signatures to endpoints to ensure that systems can detect and remove malicious code from workstations.	Purchased	Windows	NA
CrowdStrike Falcon	Enables enterprises to protect against malware, detect advanced adversaries, providing attribution when applicable, and defend against targeted attacks on servers.	Purchased	Windows / MacOS	NA
Rainier (ServiceNow)	Ticketing system used for tracking, monitoring and resolving IT issues, security incidents, access requests, etc.	Purchased	Windows	SQL

The following diagram provides a summary overview of the Enablon solution architecture and the specific aspects of the system that internal and external users may access. Application users access the Enablon solution through a secured HTTPS connection that first authenticates users through a firewall and IPS layer. Enablon's IT administrators access the application servers and underlying infrastructure through a secured VPN connection.



Enablon uses different operating systems and databases to support the hosted environment. The Enablon platform itself uses Microsoft Windows 2012 R2 and 2016 servers to support the environment; other secondary services (e.g., monitoring tools, asset management programs) use a Linux environment. Data is stored in SQL 2012 and 2016 databases on physical servers. Once customers connect to the hosted environment, they are directed to their specific instance of the Enablon application and have a dedicated database environment.

The following diagram describes how customers are redirected to their specific instance of Enablon after a secure connection and authentication to the application web server has been completed:



People

The groups supporting Enablon's operations include, but are not limited to, the following:

- Executive management—The vice president and managing director, Corporate Performance and Environmental, Social & Governance (CPESG) of Enablon, and members of the Enablon leadership team; responsible for overseeing Enablon's activities, establishing and accomplishing goals, and overseeing objectives; located in both NAM and EMEA.
- Research and development team—Responsible for the assessment, development, quality assurance (QA) and flow of changes through the system development life cycle (SDLC); located in both NAM and EMEA.
- Sales—Responsible for developing new contacts and establishing new client relationships; located in both NAM and EMEA.
- Professional services—Responsible for establishing new customer setups, initial delivery of services, troubleshooting first-level customer questions and coordinating service requests for product development and enhancements; also performing minor configuration changes within the Enablon application to meet customer requests (i.e., renaming fields within a standard form to match customer terminology); located in both NAM and EMEA.
- IT—Responsible for information systems, IT architecture, logical access administration and server maintenance and operating security elements (firewalls, IPS, advanced threat protection, encryption and other security items); located in both NAM and EMEA.
- HR—Responsible for hiring, training and performance management practices that determine whether Wolters Kluwer employees possess the required skills and are meeting desired expectations in support of Enablon.
- Global information security (GIS)—Responsible for overseeing the development and implementation of information security policies and standards. GIS also supports Wolters Kluwer business unit personnel in implementing the information security plan and providing education about information security. The information security group is also responsible for defining security requirements, controlling and auditing information systems in the Enablon Cloud Solution.

Procedures

Wolters Kluwer has implemented a Global IT security policy, which is utilized by Enablon. Security policies and guidelines have been documented and communicated throughout the organization. Wolters Kluwer's policy on information security addresses the following:

- Information classification
- Special rules for restricted information
- Clean desk and clear screen policy
- Destruction of information, data and media
- Password management
- Communication systems
- Viruses and malicious software
- Encryption
- Logging and monitoring
- Third-party information disclosure
- Change management
- Reporting a problem
- Disciplinary action
- Sensitive information defined
- Handling of sensitive information
- Printing, copying and fax transmission
- Access management
- Physical security of computers
- Remote access
- Establishing network connections
- Firewalling
- Third-party access and outsourced services
- Privacy
- Employee awareness
- Incident response

Additionally, management has documented a whistleblower policy (speak up policy) with contact information to anonymously report employee concerns. The policy is available to employees on the intranet, and reported issues are directed to the compliance department.

The responsibility for maintaining the corporate information security policies and procedures and updating the guidance, as needed, is assigned to the Wolters Kluwer corporate team. The responsibility for maintaining the Enablon information security policies and procedures and updating the guidance, as needed, is assigned to Enablon's information security director. Policies are reviewed by management annually, and changes are communicated to employees.

Data

Wolters Kluwer has a written policy for data classification and handling that identifies how to disclose information to authorized parties, classifies types of data and identifies what level of protection is required and how data classifications are monitored and updated over time. The data classification policy documents data handling and customer communication requirements based on the type of data under control. Wolters Kluwer defines confidential data as information in which unauthorized disclosure, compromise or destruction could have an adverse impact on Wolters Kluwer, its members, customers or employees.

Enablon defines data as information entered into the application by end users and stored in the hosted environment. Customer data stored in the hosted environment consists of the information provided directly by end users, and depending on the customer use, may include technical diagrams, financial and audit working papers, environmental data, proprietary information and/or personally identifiable information. As such, the MSA defines all customer data as confidential, as well as any nonpublic, confidential information either marked as such or, in the relevant circumstances, data that should be understood to be confidential information.

After authenticating to the system, customers can input information to the Enablon application by using direct manual input through the application interface or uploading documents that can be mapped to existing forms within the application or attached to the customer's database. Enablon's customer support personnel, upon authorization from the customer, can customize forms within the customer's instance of the system and designate certain fields as required to collect the necessary information. Application sessions are secured through HTTPS and TLS encryption to secure data in transit.

Enablon maintains separate database instances that are assigned to specific customers to prevent the co-mingling of data and maintain the security of customer data. Databases are either logically or physically segregated within the production environment. Clients either subscribe to a shared server where multiple client databases are located within a shared SQL Server instance, or a dedicated server, where clients are physically segregated from other clients. Data is stored in the hosted environment, and direct access to the databases is restricted to database administrators. The database servers reside at the subservice organizations, Deft or Equinix, and Enablon personnel are required to establish a VPN connection to access the database servers.

System outputs consist of screen displays, customized reports available through the application, and data files and documents transmitted to third parties on behalf of the customers. Some customers may use Enablon to securely transmit reports, claims or forms to third parties (such as insurance carriers) on their behalf. Data transmissions to third parties are encrypted during transit using the TLS protocol.

System Incidents

Enablon has a defined policy and procedures to monitor, identify and classify system events and incidents related to the security of the Enablon hosted system. Enablon did not experience any system incidents that resulted in a significant failure in the achievement of one or more of the service commitments and system requirements described within this report. No such incidents occurred during the report period. Enablon enacted its security incident management protocol, as required within the report period. In each instance, the security incident protocol was followed from identification through communication and resolution. In no instances were WK's commitments impacted.

Changes to the System During the Period

There were no relevant changes that are likely to affect report users' understanding of how the Enablon hosted solution is used to provide the service during the period from May 1, 2022, through April 30, 2023.

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

Control Environment

Enablon's internal control environment has been developed by the information audit department to include the areas of the business, such as IT, operations and compliance. Enablon's information audit director is responsible for maintaining a master listing of internal controls, including those pertaining to the security of the Enablon platform.

Wolters Kluwer maintains a supervisory board that is responsible for overseeing the activities of the organization. Formalized bylaws are documented and outline the supervisory board's responsibility for the oversight of management. The supervisory board's bylaws are reviewed annually. The supervisory board meets a minimum of six times per year and maintains meeting minutes. The supervisory board aims to have its members independent from the company and possess the necessary skills and expertise to carry out their responsibilities. Expertise and experience in the following areas of relevance should be represented on the supervisory board: General management, audits and accounting, social policy, organization and management development, legal, commercial and marketing, IT and cybersecurity, business and the community

Organizational Structure and Assignment of Authority and Responsibility

An Enablon organizational chart is in place to define the organizational structure, reporting lines, authorities and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system. Organizational roles and reporting structure are maintained within the Workday system, and are updated during the normal course of business, when necessary.

Roles and responsibilities are defined in documented position descriptions and are updated, as needed, by management. Performance reviews are conducted annually to evaluate personnel on performance in meeting their job responsibilities.

Management has assigned the responsibility for the information security program to the Enablon information security director. The vice president of information security is responsible for implementing and monitoring security policies and communicating changes and updates to those policies with employees. Additionally, the vice president of information security also coordinates with the global information security (GIS) representative for WKL&R. The formal assignment is documented in the job description.

Management Oversight

The Enablon security board meets on a quarterly basis to review open and upcoming projects related to security initiatives and to discuss the overall IT strategy, as well as evaluate impacts of environmental, regulatory and technological changes and their effects on the security of the Enablon platform.

Regional IT meetings occur on a weekly basis to review all incoming presales, incoming project delivery, urgent customer escalations and incoming deliveries from engineering. The meeting is run by the head of professional services and includes department leaders responsible for delivery to customers.

Customer executive board meetings occur on a weekly basis to review accounts based on input from executives, customer satisfaction managers or any customer-facing function. The meeting is run by the global director of customer success and includes members of the customer executive committee.

Quarterly management calls occur between the Enablon executive leadership team and the management team to review main key performance indicators (KPIs) that drive the business. Attendees include line managers in the business, including, but not limited to, finance, operations, IT and HR.

Divisional reporting meetings occur, based on the annual schedule, to review reporting on the main KPIs and business trends to the division. The meeting is run by the division chief executive officer (CEO) and attendees include Enablon's CEO, chief financial officer (CFO) and leaders of each division. Corrective action plans are created if warranted.

Personnel Practices

A background check and criminal history searches are performed on full-time employees working on Enablon hosted software and hosting infrastructure prior to employment (subject to limits under applicable law). HR operations is responsible for initiating background checks in the hiring process. Adverse results are managed through a formal adjudication process with the Wolters Kluwer legal team. The final hiring determination is made by Enablon management and is based on the adjudication of any findings in partnership with legal, the hiring manager and HR.

New hires are provided company policies that document employee responsibilities, including the code of conduct, upon hire. At the time of hire, personnel are required to review and affirm the personnel policies. The Wolters Kluwer employee handbook is utilized by Enablon and provides employees with guidance on basic work rules and standards of conduct. Employees globally are expected to comply with the Wolters Kluwer code of business ethics. Wolters Kluwer's company values are documented and communicated to employees via the intranet.

Enablon requires employees to participate in regular corporate compliance training, including ethics and compliance training. Employees are required to complete ethics and compliance training at the time of hire and annually to understand their obligations and responsibilities to comply with the code of business ethics. Employees are also required to complete security awareness training, which includes topics regarding the responsibilities for the security of data and workforce conduct standards. Security training references the policies and procedures related to data classification and security, the information life cycle, user identification and password confidentiality.

Risk Assessment Process

Enablon performs several practices to monitor and manage business risks, including the following:

- A risk assessment is conducted annually to identify potential risks, vulnerabilities and threats related to the entity, IT, fraud, third parties (i.e., vendors and business partner relationships) and significant changes (e.g., changes in the external environment, business model, leadership, systems and technology, as well as vendor and business partner relationships). Upon the completion of the risk assessment, management identifies whether the risk is adequately mitigated by current controls or if additional procedures are needed. The results are presented to the security board. Management uses RISE to track controls; Microsoft Excel was previously used to track the results of the risk assessment and identify controls to mitigate the identified risks.

- Prior to engaging a third party, Enablon completes third-party management program procedures, including conducting due diligence, signing confidentiality or nondisclosure agreements and/or an alternate contract agreement that requires the third party to implement reasonable security practices and a right to audit, and signing the supplier code of conduct or providing an equivalent standard. There were no new third-party suppliers during the period May 1, 2022, through April 30, 2023.

- Background screening checks are performed on new vendors and business partners prior to entering into contract.

- Monthly vulnerability scans are performed by the information security team to assess the security of the network. Management reviews the monthly scan results and creates a ticket in the relevant ticketing system (SOFTWARE, GLPI or Rainier [ServiceNow]) to document, track and remediate high- and medium-risk items. Tickets are closed by infrastructure or research and development (R&D) personnel upon completion of the remediation activities.

- An annual penetration test of the Enablon application is performed to identify potential vulnerabilities. The information security team coordinates the exercise with an independent third-party provider. High-risk issues identified during the scan are documented in Rainier (ServiceNow), GLPI or SOFTWARE tickets and assigned to the appropriate personnel for corrective action.

- The IT department tracks system components and servers, including software and hardware, in the GLPI, BigFix, McAfee EPO and AD applications, and reviews the hardware inventory annually.

- A speak up policy, with contact information to report employee concerns and suspected violations to company policies, is documented and available to employees on the intranet. The policy is reviewed and approved by Wolters Kluwer management annually.

- The information audit director performs assessments annually. Results are reported to the security board quarterly.

- Enablon maintains insurance policies to offset the financial impact of loss events that would otherwise impair the ability to meet its objectives.

Information and Communication Systems

Information

The Wolters Kluwer information security policy helps employees understand their individual roles and responsibilities concerning processing and controls to make sure that significant events are communicated in a timely manner. The policy includes formal and informal training programs and the use of email to communicate time-sensitive information and processes for security purposes that notify key personnel in the event of problems.

External User Communication

A comprehensive help guide is available to users of the Enablon solution online through Confluence. The help guide includes details on the design of the system, including system boundaries, and specific responsibilities of the users for controlling system security to aid users in their understanding of the system.

The entity's security commitments and the associated system requirements are defined and communicated to external users in a standard MSA. Security commitments for Enablon include information security, support obligations and confidential information obligations. Information is also available in the Enablon Customer Support Services Welcome Guide.

Issues submitted by customers through the Helpdesk web interface are automatically logged in Helpdesk tickets. Professional services personnel reviewing these issues assign a severity rating based on the description of the issue and resolve the issue.

When changes to existing systems are deployed that are relevant to external users, including changes that may impact user responsibilities and requirements, Enablon provides release notes to external users. The release notes are available to users in Confluence.

Internal User Communication

In addition to the materials available to external users, management has documented a network map that diagrams the external access points, flow of data and organization of infrastructure within the boundaries of the Enablon network and platform. The network map is available to relevant employees through the IT shared drive.

Enablon notifies internal users by email and release notes on the intranet of system updates or changes that may impact security commitments, user responsibilities or system requirements.

A documented incident response process includes procedures for reporting security incidents within the organization, as well as notifying customers of critical incidents that may affect the system. The incident response process is available to internal users within the Corporate Incident Management Plan and Crisis Communication Playbook published on the corporate intranet. There is also an IT incident management section within the Wolters Kluwer GIS policy. The document is reviewed and approved by Wolters Kluwer management and is available on the company intranet. Security incidents are also managed through the customer support Helpdesk ticketing process. Internal and external users can access the Helpdesk tool to submit complaints, requests and security incidents. The customer support team ensures that customer administrators know how to access the Helpdesk tool through presentations or support guide.

Monitoring Controls

Security Board

The security board meets quarterly to monitor security and operations. The security board membership consists of the vice president and managing director, CPESG of Enablon, the information security director, the information audit director and select management personnel. Topics covered during the quarterly security board meetings include existing and emerging IT risks, evaluating impacts of environmental, regulatory and technological changes and their effects on the security of the Enablon platform, IT strategic plans and security initiatives, the results of security assessments, monitoring activities, and the status of new and existing projects.

Ongoing Monitoring

The information audit director performs a series of audits annually based on organization needs and the results of the annual risk assessment. The audits are planned at the beginning of the fiscal year and tracked against the plan throughout the year. Results of the audits are discussed during security board meetings and formally communicated to Enablon management through audit reports.

Management utilizes control frameworks, such as AICPA TSP 100 and General Data Protection Regulation, to manage and monitor internal controls and processes related to IT, finance, operations and compliance departments. If any issues are identified regarding IT or business processes, control activities are designed and developed to mitigate the risks to the achievement of objectives.

The information audit director monitors compliance deviations and violations that result in deficiencies in internal control. Monitoring takes place such that deficiencies are ultimately resolved by management in a timely manner.

The information audit director maintains a master listing of internal controls in RISE, including those pertaining to the security of the Enablon solution. As part of the annual audit planning cycle, the information audit director reviews and updates the master listing of internal controls. The master listing of controls also includes a self-assessment of whether the control has been designed, implemented and executed based on the compliance tasks recorded. The information audit director reviews progress of the control environment.

Monitoring of Third-Party Vendors

Management has implemented a vendor management program to define the requirements for vendor performance and due diligence procedures prior to vendor acceptance. The program also includes reviews of vendors using a risk-based rating program to evaluate high-risk vendors annually and lower-risk vendors less frequently.

The third-party management program also includes onboarding, monitoring and termination of vendors and business partners. The third-party management program policy and procedures are reviewed by management on an annual basis.

The information audit director also collects System and Organization Controls (SOC) reports for key vendors, as available, on an annual basis to review the results of the reports and map them to Enablon’s controls. If any deviations are identified, corrective action is taken as warranted.

Controls Applicable to the Common Criteria

Physical Access

Facility Security

Physical access to the Enablon facilities in Chicago, Illinois, and Bois-Colombes, France, are restricted to authorized individuals by a keycard system. Personnel are assigned keycards that allow access to specific areas of the facilities. The computer rooms that house the local internal IT resources, servers and related hardware are located within the Enablon facilities and physical access is controlled and managed by IT management. In Bois-Colombes, the computer room is secured by a physical key that is restricted to authorized individuals. In Chicago, the computer room is secured using the same keycard system as the main entry to the facility, but is restricted to only those authorized IT users for entry to the IT server room. Personnel working from remote locations require a separate badge to access the Chicago, Illinois, or Bois-Colombes, France, offices and/or do not have physical access to the facility.

User access requests for physical access to the Enablon offices are documented on a standard access request form and require manager approval prior to being granted access. Upon approval, the office manager assigns the new employee a keycard and logs the associated access rights in the keycard system.

Annually, office managers perform a review of personnel with physical access to their respective Enablon office in either Chicago, Illinois, or Bois-Colombes, France. The review also reconciles the current listing of active badges to the current listing of active workers from HR to validate that access is restricted to authorized and appropriate personnel. Modifications to access are made as a result of the review, as needed.

Employee offboarding emails or tickets are completed by management upon employee termination and document the request and removal of physical access.

Third-Party Data Center Security

The data centers housing production servers for the Enablon solution are managed and maintained by the subservice organizations, Deft and Equinix. The information audit director performs an annual review of Deft and Equinix by reviewing their SOC 2 reports. Enablon personnel are granted access to the subservice providers' facilities on an as-needed basis. Physical access to the Enablon co-location facilities is authorized by management and tracked within a log maintained by Deft and Equinix, respectively. A review of the physical access activity log is performed on a semiannual basis by management.

Logical Access

Security Administration

A formal user access management policy documents the procedures for logical access to systems, including access provisioning, access modifications and access revocations and is available to IT employees on Confluence. The user management policies are reviewed by Enablon IT on an annual basis and updated, as needed.

Internal Access and User Authentication

A username and password are required to authenticate and access the network (Active Directory), the VPN and the production and database servers. An authentication certificate is also required to access the VPN and production and database servers. Password parameters require the following:

- Complexity requirements (uppercase, lowercase, number and special character)
- Minimum password length of eight characters
- Maximum password age of 365 days
- Minimum history requirement of six prior passwords
- Invalid password account lockout threshold after five incorrect attempts

Due to the COVID-19 pandemic and increase in remote workers, internal network password parameters were updated during the report period 365 days to expand the password expiration requirements after obtaining appropriate approvals and documenting exceptions. IT administrators are required to comply with the 90-day password age to access the production servers. Requests for user access, including new and modifications to existing accounts within the Enablon system and its components, are documented on a standard access request form and require manager approval prior to access being provisioned.

User access reviews are conducted by management on a quarterly basis to review the Active Directory users. The information audit director is responsible for coordinating with department owners to perform the review. Necessary access modifications are performed based on the results of the review.

Administrative access to the production servers requires a connection to the data center environment (Deft or Equinix) through a secure VPN. It is limited to authorized Enablon personnel and requires the use of a separate set of credentials. Enablon employees have a set of credentials that give them access to resources in the “Enablon” internal domain. IT/cloud hosting personnel are required to have an additional separate set of credentials to connect to the IT domain hosting customer environments.

Access to the production servers is reviewed by IT management on a quarterly basis, and updates to user access are made based on the results of the review.

Employee offboarding emails or tickets are completed by management upon employee termination and document the request and removal of logical access.

Database Access

User access to the production databases is restricted to a subset of Enablon personnel designated as IT hosting administrators. Access to the databases is controlled through Active Directory group assignments and users require membership in the designated group to access the databases. Database administrator access is reviewed by management quarterly for appropriateness.

External Access

During the customer setup process, clients identify which members of their team have administrative access to the Enablon solution; these client administrators have access to create and remove access for users in their specific instance of the application. Client administrators are responsible for creating user accounts, setting access levels for user accounts and removing user access for all users of their environment, including Enablon and integration partner users (if any).

External users access the Enablon solution through a web interface that requires authentication. Authentication to the application is controlled by a username and password. Access is denied if an invalid user ID and/or password is submitted during the login process. Customers are responsible for configuring the specific password requirements to meet their organization’s information security requirements.

Network Security

Dual external firewalls are configured to prevent unauthorized access to the internal network. Firewalls have been implemented to segment the internal network and systems from direct access to the internet. The firewalls are configured so that systems are allocated an IP address within the IP range associated with the subnetwork they are connected to using Dynamic Host Configuration Protocol (DHCP) or static allocation. Firewall configurations are reviewed by management monthly to determine whether configurations are appropriate. Any issues noted are investigated and resolved.

A combination IPS and IDS is in place to prevent and detect unauthorized network events and analyze logged events for potential security incidents. The IPS and IDS are configured to alert management via emails in the event that a critical security breach is detected in the internal network. Management records and tracks the remediation of security incidents in the GLPI and Rainier ticketing systems.

Remote access to the internal network requires an encrypted VPN connection. Users authenticate to the environment with a username and password, and an authentication certificate to establish an encrypted VPN session. The connection is controlled through a VPN application installed on the user's workstation.

Standard end user workstations are configured with CyberArk End Point Privilege Manager to prevent installation of banned software, allow installation of authorized software, and log elevated privileges actions. This applies to all standard workstations and is configured during the setup and asset hardening process.

Data Security Measures

Web application sessions are encrypted using TLS encryption to secure user activity and encrypt data transmissions between the user and production environment.

Employee workstations and laptops are secured with disk encryption management software. Additionally, employee email messages are configured to automatically encrypt during transmission.

Enablon has an overarching data classification and handling standard as part of the GIS policy. The standard identifies how to disclose information to authorized parties, classify types of data, what level of protection is required, and how data classifications are monitored and updated over time.

Data stored on information and technology assets (e.g., workstations, laptops, servers) and physical media (e.g., paper, USB drives, tapes, smartcards, removable disk drives, CDs, DVDs) is erased and physically destroyed when retired from use. A certified data erasure process third-party tool is utilized, if possible, before the device is physically destroyed. There were no assets disposed during the report period of May 1, 2022, to April 30, 2023.

Daily backups are written to tape on a weekly basis and stored in a secure location until they are rotated off-site at month-end. Backup tapes are automatically encrypted upon creation.

Virus Detection and Prevention

Enablon production servers are secured with the McAfee antivirus program and are configured to automatically update definitions on an hourly basis. Automated alerts are sent to the IT team when a virus has been detected.

McAfee anti-malware software is in place on Enablon workstations to protect the workstations from malicious software and is configured to automatically update definitions on an hourly basis. Enablon IT management performs a weekly review of noncompliant workstations, as well as detected security events or threats, to enforce consistent updates to employee workstations.

Incident Management

Incident Response Program

Wolters Kluwer has a documented security incident response plan in place. The plan includes procedures for reporting security violations, suspected breaches and complaints within the organization, and for notifying customers of security, availability and confidentiality incidents that may have affected their data or applications. Alerts from the security monitoring devices are logged, evaluated and escalated based on the criticality of the alert. A root cause analysis is conducted to evaluate the event and what changes, if any, need to be implemented to prevent and detect recurrences.

Security incidents are reviewed by the technical personnel, tracked in incident response tickets and escalated to management to address the issue and develop corrective measures. The information security officer is part of the incident response process and is informed of potential or actual incidents through ongoing communications during the identification, tracking and resolution of incidents. If a security incident impacts a customer or their data, the incident response plan defines the steps necessary to document, communicate, mitigate and resolve the security incident with that customer.

A root cause analysis is prepared and reviewed for critical security and availability incidents that require remediation. Critical incidents affecting customers are communicated to customers within several business days. Incidents affecting customers are communicated to customers through the assigned customer service representative, who maintains contact information for each assigned client contact. There were no critical incidents or incidents affecting customers identified during the report period of May 1, 2022, to April 30, 2023.

The Enablon incident response plan and recovery procedures are tested on an annual basis. Annual testing may be conducted as a strategic incident exercise or a tabletop review of an incident. The test results are reviewed by management and the plans and systems are revised, if necessary.

System Monitoring and Incident Response

Enablon maintains an incident management process that is communicated to external users via the MSA.

The automated tools that Enablon has implemented to monitor the Enablon hosted solution also provide detective measures for identifying security events and security incidents. Critical alerts generated by the IPS and IDS are reviewed by IT personnel to determine whether corrective action is needed.

Firewall and IPS is utilized to protect and monitor security event activity of the network devices and servers. Logs are reviewed on a monthly basis to detect potential fraud, IT security violations and attacks. Any issues are investigated and resolved.

Change Management

Enablon follows change management procedures for Enablon platform development, infrastructure updates, operating system changes and network patching. The Enablon application is fully developed by Enablon personnel and third-party contractors. Other systems and infrastructure components are developed by vendors, and Enablon’s role is limited to the patching of and security updates, maintenance updates, and upgrades to those systems. Due to the nature of the system, clients are responsible for the data within the system and, as such, are able to make data changes directly through the Enablon Solution interface.

Separate environments have been created and designated for specific activities, including development and quality assurance, user acceptance testing and production. Users are granted access to environments based on job responsibilities, and management reviews user access to the environments annually to validate the appropriateness of user access and whether segregation of duties are effective.

Management identifies the need for changes to systems through multiple sources. The most common sources are through customer requests for enhancements or additional features, as well as requests from the product manager. Other sources include issues raised during the annual IT risk assessment and security or bug fixes identified through security testing. Changes to application, software, data and infrastructure are documented in tickets and approved by management prior to implementation. A detailed overview of the change process for the various systems is provided below.

Application Change Management

Management maintains a formal documented SDLC policy for Enablon application changes. The SDLC policy addresses procedures for the design, acquisition, implementation, configuration, testing, modification, and maintenance of system components. The SDLC policy is reviewed annually by Enablon management and is available to internal users on Confluence.

Enablon has two main types of application changes: enhancements and maintenance changes. Enhancements are considered changes or modifications to functional or technical capabilities where maintenance changes and updates to the current version keep it running as expected.

R&D backlog meetings are held every two weeks to discuss the status of the change backlog, upcoming projects and overall development strategy for the current sprint affecting the Enablon application. During these backlog meetings, R&D personnel approve new requests for application development and gather the requirements for the backlog items. Approved backlog items are assigned to a developer during sprint planning or while the sprint is ongoing.

Enablon uses a source code repository for development and QA testing activities for the change. When a change is ready for testing, a pull request triggers required or optional validations, including functional reviews (such as product owner validation), technical reviews (such as peer review by another R&D developer), manual and automated testing of the individual change, along with various automated checks. Completion of the testing validation is documented in the ticketing system. At the completion of development and testing activities for an individual change, the change is compiled with the other changes of the two-week sprint into a build. Source code resulting from the merge of the individual changes is compiled into a build that is ready for release using the version control system. Dedicated QA personnel perform manual tests to complete functional and technical reviews of the build before authorizing the build for release into production. Automated tests are also run on the integrated build prior to approval for release into production. Completion of the QA review and approval is documented and validated in the ticketing system. The infrastructure team moves validated builds into production using information communicated to them by QA personnel.

Once a build has been compiled, it cannot be modified. If there were to be an issue with the build, then the build would be rejected and a new one fixing the issue would be required to go through the entire QA validation process.

Enablon maintains distinct environments for development, testing and production to support the product management and secure software development life cycle. Segregation of duties exists between R&D personnel, who are responsible for developing application changes, and the CloudOps team, who are responsible for promoting releases into the production environment. The version control software maintains the integrity of program source code and enforces segregation of duties throughout the source code development life cycle to ensure that developers cannot change code outside of the development environment. An automated tool within the version control system is used to compile code from the development environment and push it to the test and production environments. Users with access to modify source code and users with access to promote source code into production, are reviewed by Enablon management on a quarterly basis to validate that access is limited to authorized users. Necessary access modifications are performed based on the results of the review.

Emergency Changes

Emergency changes follow the same process described in the application change management section above in an expedited fashion. These types of changes will be classified with a priority of “Immediate” and have a checkmark next to the emergency patch descriptor within the ticket, such that they are treated and implemented quicker than other maintenance-related changes. Emergency changes can be made as the result of the monthly vulnerability scanning, annual penetration testing, identified security incidents or customer-identified security issues.

Database and Infrastructure Change Management

Enablon performs patch management, system upgrades and the setup configuration of new hardware used to support the hosted systems. Patches and upgrades are received from vendors and are implemented by infrastructure personnel. The setup of new servers and workstations is performed by infrastructure personnel in accordance with the information security policy, as well as in accordance with a baseline configuration of IT and control systems that has been created and maintained. This is used when setting up and configuring new IT assets, such as application and database servers. Management has established a checklist for the setup and configuration of security for new devices added to the network to meet the organization’s minimum-security requirements. The checklist is maintained for new devices to outline the setup requirements.

The IT department tracks server hardware on an ongoing basis through the GLPI, BigFix, McAfee EPO and AD applications. IT management performs an annual review of the hardware lists to determine whether items are accurately reflected on the listings.

A patch management policy is in place with the information systems group that governs the timing and strategy for testing and releasing patches to internal and production systems. Enablon is responsible for patching the servers, network and operating systems supporting the hosted environment. The policy is reviewed annually by Enablon management and is available to internal users.

Infrastructure patches, including security updates for Windows and Enablon application server components, are managed and documented by the infrastructure team using a staging approach to test and release into internal and production systems.

Complementary Subservice Organization Controls

Enablon uses subservice organizations to perform various functions to support the delivery of services. The scope of this report does not include the controls and related control objectives at the subservice organizations. The following is a description of services the subservice organizations provided:

Subservice Organization	Service Provided
Deft	Deft hosts production servers, provides maintenance and support of the infrastructure and maintains physical security and environmental protection controls of the data center facilities. The data center is located near Chicago, Illinois, and hosts systems for NAM customers of Enablon by default.
Equinix	Equinix hosts production servers, provides maintenance and support of the infrastructure and maintains physical security and environmental protection controls of the data center facilities. The data center is located in the Paris area (Courbevoie), France, and hosts systems for EMEA customers of Enablon by default.

Below are the applicable trust services criteria that are impacted by the subservice organizations and the controls expected to be implemented at the subservice organizations.

Applicable Criteria	Controls Expected to be Implemented
Common Criteria 6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	• Access to the facility hosting production systems is restricted to personnel or visitors authorized by the tenant. • Access to the facility hosting production systems is not granted to personnel or visitors unless authorized by the tenant previously. • Access to the facility hosting production systems is removed/disabled upon tenant notification. • Access to the facility is controlled via keycard system or other preventative access control systems. • Access to entrances and sensitive areas are monitored and/or recorded by security cameras. • Access to the facility is periodically reviewed.
Common Criteria 7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. Common Criteria 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. Common Criteria 7.5 The entity identifies, develops and implements activities to recover from identified security incidents.	• A documented procedure that defines and communicates the process for employees and customers to report suspected security violations and other security issues has been documented and communicated. • Security incidents are reported to Enablon, as needed, to assist with resolution. • Security incidents are communicated to Enablon. Documentation of the communication, impact and resolution of the incident is retained in an enterprise ticketing system. • A root cause analysis is prepared and reviewed for critical security incidents that require remediation.

IV. Trust Services Criteria, Enablon's Related Controls, and RSM US LLP's Tests of Controls and Results of Tests

Relevant trust services criteria and Enablon's related controls are an integral part of management's system description and are included in this section for presentation purposes. RSM US LLP included the description of the tests performed to determine whether the controls were operating with sufficient effectiveness to achieve the specified service commitments and system requirements based on the applicable criteria and the results of tests of controls, as specified below.

Tests of the control environment, risk assessment, information and communication, and monitoring included inquiry of appropriate management, supervisory and staff personnel, observation of Enablon's activities and operations, and inspection of Enablon's documents and records. The results of those tests were considered in planning the nature, timing and extent of RSM US LLP's testing of the controls designed to achieve the service commitments and system requirements based on the relevant trust services criteria. As inquiries were performed for substantially all of Enablon's controls and for the testing of the completeness and accuracy of information produced for populations and key reports utilized for control testing, these tests are not listed individually for every control listed in the tables below.

Criteria Common to the Security Category

CC1 Control Environment

CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
Provided by Enablon		***Provided by RSM US LLP***	
Control		**Test Performed**	**Test Results**
CC1.1.1	New hires are provided company policies that document employee responsibilities, including the code of conduct, upon hire. At the time of hire, personnel are required to review and affirm personnel policies.	Inspected onboarding policy acknowledgements and certificates of delivery of documents for a sample of new hires to determine whether company policies were provided to and affirmed by new employees, if applicable, at the time of hire.	Exception noted. For one of 14 new hires selected, the employee did not review and affirm the personnel policies in a timely manner.

CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
Provided by Enablon		**Provided by RSM US LLP**	
	Control	**Test Performed**	**Test Results**
CC1.1.2	Prior to engaging a third-party, Enablon requires the following third-party management program procedures: • Conduct due diligence. • Sign confidentiality or nondisclosure agreements and/or alternate contract agreement that requires the third party to implement reasonable security practices and a right to audit. • Sign the supplier code of conduct or provide an equivalent standard.	Inspected the system-generated report of new third-party suppliers to determine whether any third parties with access to the Enablon system were added during the report period.	No tests of the control were performed, because the circumstances that warrant the operation of the control did not occur during the report period.
CC1.1.3	A speak up policy with contact information to anonymously report employee concerns is documented and available to employees on the intranet. The policy is reviewed and approved by management annually.	Inspected the speak up policy and corporate intranet site to determine whether the policy documented contact information to anonymously report employee concerns, was made available to employees on the intranet, and was reviewed and approved by management annually.	No exceptions noted.
CC1.1.4	Performance reviews are conducted annually to evaluate personnel on performance in meeting job responsibilities.	Inspected performance reviews for a sample of personnel to determine whether management evaluated employees for performance in meeting job responsibilities.	No exceptions noted.
CC1.1.5	Vendor management's responsibilities and accountabilities are documented within the Third-Party Risk Management Standard. The standard outlines due diligence requirements for new and existing vendors, based on the risk of the vendor's services. The information security council reviews the Third-Party Risk Management Standard annually.	Inspected the Third-Party Risk Management Standard to determine whether the standard documented vendor management's responsibilities and accountabilities, due diligence procedures for new and existing vendors, and the standard was reviewed annually by the information security council.	No exceptions noted.
CC1.1.6	Wolters Kluwer has a values statement that is communicated to employees via the intranet and updated by management, as needed.	Inspected the Wolters Kluwer intranet to determine whether Wolters Kluwer had a values statement that was communicated to employees via the intranet.	No exceptions noted.

CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC1.1.7	The Wolters Kluwer code of business ethics defines employee conduct standards, including anticorruption policies, the company values statement and business principles. Employees are required to complete annual ethics and compliance training to understand their obligations and responsibilities and acknowledge their agreement with the code of business ethics.	Inspected the code of business ethics to determine whether the code of business ethics was documented and defined employee conduct standards, including anticorruption policies, the company values statement and business principles.	No exceptions noted.
		Inspected the ethics and compliance training reports for a sample of employees to determine whether employees completed annual ethics and compliance training to understand their obligations and responsibilities and acknowledge their agreement with the code of business ethics.	No exceptions noted.

COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC1.2.1	The security board meets on a quarterly basis to review open and upcoming projects, discuss overall IT strategies, review current system performance and evaluate the impacts of environmental, regulatory and technological changes and their effect on the security of the Enablon platform.	Inspected the minutes and invites from meetings between top management and members of the security board for a sample of quarters to determine whether the meetings were held to review open and upcoming projects, discuss overall IT strategies, review current system security performance and evaluate the impacts of environmental, regulatory and technological changes and their effect on the security of the Enablon platform.	No exceptions noted.
CC1.2.2	Regional IPP (IT, product, professional services) meetings occur on a weekly basis to review urgent customer escalations and incoming deliveries from engineering. The meeting is run by department leaders responsible for delivery to customers. Corrective action plans are created if warranted.	Inspected the regional IPP meeting minutes for a sample of weeks to determine whether the regional IPP reviewed urgent customer escalations and incoming deliveries from engineering, and corrective action plans were created if warranted.	No exceptions noted.
CC1.2.3	Customer executive board meetings occur on a weekly basis to review accounts based on input from executives, customer satisfaction managers, or any customer-facing function. The meeting is run by the global director of customer success and includes members of the customer executive committee.	Inspected the customer executive board meeting minutes for a sample of weeks to determine whether the customer executive board reviewed customer account issues and remediation status.	No exceptions noted.

COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC1.2.4	Quarterly management calls occur between the Enablon executive leadership team and the management team to review the main KPIs that drive the business. Attendees include line managers in the business, including but not limited to, finance, operations, IT and HR.	Inspected the performance call meeting minutes for a sample of quarters to determine whether the Enablon executive leadership team met with the management team to review the main KPIs that drive the business, which included finance, operations, IT and HR departments.	No exceptions noted.
CC1.2.5	Divisional reporting meetings occur, based on the annual schedule, to review reporting on the main KPIs and business trends to the division. The meeting is run by the division CEO and attendees include Enablon's CEO, CFO and leaders of each division. Corrective action plans are created if warranted.	Inspected the meeting minutes for a sample of divisional reporting meetings to determine whether divisional reporting on the main KPIs and business trends were reviewed, and corrective action plans were created if warranted.	No exceptions noted.
CC1.2.6	The supervisory board bylaws define the responsibilities of board members, including oversight of the business, management and the risk management and internal control systems.	Inspected the supervisory board bylaws to determine whether the responsibilities of board members, including oversight of the business, management and the risk management and internal control systems, were documented.	No exceptions noted
CC1.2.7	An evaluation of supervisory board members, including the audit committee, regarding independence from management and relevant areas of expertise is completed and tracked in the supervisory board charter within calendar year.	Inspected the supervisory board meeting minutes to determine whether the annual evaluation of supervisory board members, including the audit committee, regarding independence from management and relevant areas of expertise was completed.	No exceptions noted

CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines and appropriate authorities and responsibilities in the pursuit of objectives.			
Provided by Enablon		***Provided by RSM US LLP***	
Control		**Test Performed**	**Test Results**
CC1.3.1	Organizational roles and structures are maintained within the Workday system, and are updated during the normal course of business, when necessary.	Inspected the organizational chart to determine whether organizational roles and structures were maintained and updated during the normal course of business, when necessary.	No exceptions noted.
CC1.3.2	The vice president of information security has been assigned the responsibility for the information security program. The formal assignment is documented in the job description.	Inspected the job description for the vice president of information security to determine whether he/she had been assigned the responsibility for the information security program.	No exceptions noted.
CC1.3.3	Job descriptions document the roles, requirements and expectations for positions supporting the system, and have been assigned to personnel.	Inspected the job descriptions for a sample of employees to determine whether personnel roles and responsibilities were documented.	No exceptions noted.
CC1.3.4	Vendor management's responsibilities and accountabilities are documented within the Third-Party Risk Management Standard. The standard outlines due diligence requirements for new and existing vendors, based on the risk of the vendor's services. The information security council reviews the Third-Party Risk Management Standard annually.	Inspected the Third-Party Risk Management Standard to determine whether the standard documented vendor management's responsibilities and accountabilities, due diligence procedures for new and existing vendors, and the standard was reviewed annually by the information security council.	No exceptions noted.

COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
Provided by Enablon		***Provided by RSM US LLP***	
Control		**Test Performed**	**Test Results**
CC1.4.1	Prior to engaging a third-party, Enablon requires the following third-party management program procedures: • Conduct due diligence. • Sign confidentiality or nondisclosure agreements and/or alternate contract agreement that requires the third party to implement reasonable security practices and a right to audit. • Sign the supplier code of conduct or provide an equivalent standard.	Inspected the system-generated report of new third-party suppliers to determine whether any third parties with access to the Enablon system were added during the report period.	No tests of the control were performed, because the circumstances that warrant the operation of the control did not occur during the report period.

COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC1.4.2	Security awareness training is completed annually by Enablon personnel.	Inspected the training records for a sample of employees to determine whether annual security awareness training was completed.	No exceptions noted.
CC1.4.3	Performance reviews are conducted annually to evaluate personnel on performance in meeting job responsibilities.	Inspected the performance reviews for a sample of personnel to determine whether management evaluated employees for performance in meeting job responsibilities.	No exceptions noted.
CC1.4.4	Prior to hire, background checks are performed on full-time employees working on Enablon hosted software and hosting infrastructure (subject to limits under applicable law).	Inspected the results of background checks and prehire education and identity screening verifications for a sample of new hires to determine whether the assessment was completed prior to employment.	No exceptions noted.
CC1.4.5	Vendor management's responsibilities and accountabilities are documented within the Third-Party Risk Management Standard. The standard outlines due diligence requirements for new and existing vendors, based on the risk of the vendor's services. The information security council reviews the Third-Party Risk Management Standard annually.	Inspected the Third-Party Risk Management Standard to determine whether the standard documented vendor management's responsibilities and accountabilities, due diligence procedures for new and existing vendors, and the standard was reviewed annually by the information security council.	No exceptions noted.
CC1.4.6	New hires are required to complete security awareness training within 30 days of starting employment. Management tracks completion of the training in the HR system, and HR follows up with employees until the training is completed.	Inspected the security awareness training documentation for a sample of newly hired employees to determine whether the employees were required to complete security awareness training within 30 days of hire, or HR followed up with employees until the training was completed.	No exceptions noted.

COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC1.5.1	Performance reviews are conducted annually to evaluate personnel on performance in meeting job responsibilities.	Inspected the performance reviews for a sample of personnel to determine whether management evaluated employees for performance in meeting job responsibilities.	No exceptions noted.
CC1.5.2	Customer executive board meetings occur on a weekly basis to review accounts based on input from executives, customer satisfaction managers, or any customer-facing function. The meeting is run by the global director of customer success and includes members of the customer executive committee.	Inspected the customer executive board meeting minutes for a sample of weeks to determine whether the customer executive board reviewed customer account issues and remediation status.	No exceptions noted.
CC1.5.3	Quarterly management calls occur between the Enablon executive leadership team and the management team to review the main KPIs that drive the business. Attendees include line managers in the business, including but not limited to, finance, operations, IT and HR.	Inspected the performance call meeting minutes for a sample of quarters to determine whether the Enablon executive leadership team met with the management team to review the main KPIs that drive the business, which included finance, operations, IT and HR departments.	No exceptions noted.
CC1.5.4	Divisional reporting meetings occur, based on the annual schedule, to review reporting on the main KPIs and business trends to the division. The meeting is run by the division CEO and attendees include Enablon's CEO, CFO and leaders of each division. Corrective action plans are created if warranted.	Inspected the meeting minutes for a sample of divisional reporting meetings to determine whether divisional reporting on the main KPIs and business trends were reviewed, and corrective action plans were created if warranted.	No exceptions noted.

CC2 Communication and Information

COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC2.1.1	Quarterly management calls occur between the Enablon executive leadership team and the management team to review the main KPIs that drive the business. Attendees include line managers in the business, including but not limited to, finance, operations, IT and HR.	Inspected the performance call meeting minutes for a sample of quarters to determine whether the Enablon executive leadership team met with the management team to review the main KPIs that drive the business, which included finance, operations, IT and HR departments.	No exceptions noted.
CC2.1.2	Divisional reporting meetings occur, based on the annual schedule, to review reporting on the main KPIs and business trends to the division. The meeting is run by the division CEO and attendees include Enablon's CEO, CFO and leaders of each division. Corrective action plans are created if warranted.	Inspected the meeting minutes for a sample of divisional reporting meetings to determine whether divisional reporting on the main KPIs and business trends were reviewed, and corrective action plans were created if warranted.	No exceptions noted.
CC2.1.3	The IT department tracks end user hardware in ServiceNow and reviews annually.	Inspected the inventory listing to determine whether the IT department tracked end user system components, including end user hardware.	No exceptions noted.
		Inspected the evidence of a review of end user system components, including end user hardware, to determine whether the IT department reviewed them on an annual basis.	No exceptions noted.

COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC2.2.1	Management has documented the external access points, flow of data and organization of the infrastructure within the Enablon network and platform. The network map is available for employee reference on a shared network file share.	Inspected the network diagram and its location to determine whether the external access points, flow of data and organization of the infrastructure were documented and available for employee reference on a shared network file share.	No exceptions noted.

COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
Provided by Enablon		***Provided by RSM US LLP***	
Control		**Test Performed**	**Test Results**
CC2.2.2	A help guide is available to internal and external users of the Enablon platform through the Confluence site and documents the system boundaries and operation of the Enablon platform.	Inspected the Enablon help guide to determine whether it was available to internal and external users through the Confluence site, and whether it documented the system boundaries and operations of the Enablon platform.	No exceptions noted.
CC2.2.3	New hires are provided company policies that document employee responsibilities, including the code of conduct, upon hire. At the time of hire, personnel are required to review and affirm personnel policies.	Inspected the onboarding policy acknowledgements and certificates of delivery of documents for a sample of new hires to determine whether company policies were provided to and affirmed by new employees, if applicable, at the time of hire.	Exception noted. For one of 14 new hires selected, the employee did not review and affirm the personnel policies in a timely manner.
CC2.2.4	A speak up policy with contact information to anonymously report employee concerns is documented and available to employees on the intranet. The policy is reviewed and approved by management annually.	Inspected the speak up policy and corporate intranet site to determine whether the policy documented contact information to anonymously report employee concerns, was made available to employees on the intranet, and was reviewed and approved by management annually.	No exceptions noted.
CC2.2.5	The data classification policy documents data handling and customer communication requirements based on the type of data under control. The policy is reviewed by management annually and made available to employees on the corporate intranet site.	Inspected the data classification policy and corporate intranet site to determine whether the policy documented data handling and customer communication requirements based on the type of data under control, and the policy was reviewed by management annually and made available to employees on the corporate intranet site.	No exceptions noted.
CC2.2.6	Information security policies are reviewed by Wolters Kluwer management annually, and changes are communicated to internal users. Policies are located on the corporate intranet to communicate security commitments to internal users to enable them to carry out their responsibilities.	Inspected the global information security policies and their location on the intranet to determine whether they were communicated to internal users.	No exceptions noted.
		Inspected the information security policies to determine whether they were reviewed by Wolters Kluwer management annually.	No exceptions noted.

COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
Provided by Enablon		***Provided by RSM US LLP***	
Control		**Test Performed**	**Test Results**
CC2.2.7	The security incident response plan outlines the responsibilities of employees to report identified incidents, as well as the procedures for reporting security incidents within the organization and notifying customers of incidents that may have affected their data. Management performs an annual review of the security incident response plan and updates the procedures, as necessary. The security incident response plan is communicated to authorized personnel on the corporate intranet site.	Inspected the security incident response plan and corporate intranet site to determine whether the responsibilities of employees to report identified incidents, as well as the procedures for reporting security incidents within the organization and notifying internal customers of incidents that may have affected their data were documented, the plan was reviewed by management annually, and communicated to authorized personnel on the corporate intranet site.	No exceptions noted.
CC2.2.8	Security awareness training is completed annually by Enablon personnel.	Inspected the training records for a sample of employees to determine whether annual security awareness training was completed.	No exceptions noted.
CC2.2.9	Enablon provides release notes to internal and external users for releases that constitute changes in the system and are identified as relevant to internal and external users and the security of the Enablon platform.	Inspected the release notes for a sample of application production server releases to determine whether changes that may affect the security of the system were communicated to internal and external users.	No exceptions noted.

COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
Provided by Enablon		***Provided by RSM US LLP***	
Control		**Test Performed**	**Test Results**
CC2.3.1	A help guide is available to internal and external users of the Enablon platform through the Confluence site and documents the system boundaries and operation of the Enablon platform.	Inspected the Enablon help guide to determine whether it was available to internal and external users through the Confluence site, and whether it documented the system boundaries and operations of the Enablon platform.	No exceptions noted.
CC2.3.2	The entity's security commitments and the associated system requirements are defined and communicated to external users in a standard MSA.	Inspected the MSA for a sample of new customers to determine whether the entity's security commitments and the associated system requirements were defined within.	No exceptions noted.
CC2.3.3	Information on how to report systems failures, incidents, concerns and other complaints to Enablon personnel is communicated to external users via the MSA.	Inspected the MSA for a sample of new customers to determine whether information on how to report systems failures, incidents, concerns and other complaints to Enablon personnel was communicated to external users.	No exceptions noted.

COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC2.3.4	External users can access the Helpdesk tool through the application to submit complaints, requests and security incidents. The customer support team ensures customer administrators know how to access the Helpdesk tool through presentations or support guide.	Inspected the user access to the Helpdesk tool through the application to determine whether they had the ability to submit complaints, requests and security incidents.	No exceptions noted.
		Inspected the Welcome Guide to determine whether a support guide is provided to instruct customers on how to access the Helpdesk.	No exceptions noted.
CC2.3.5	Enablon provides release notes to internal and external users for releases that constitute changes in the system and are identified as relevant to internal and external users and the security of the Enablon platform.	Inspected the release notes for a sample of application production server releases to determine whether changes that may affect the security of the system were communicated to internal and external users.	No exceptions noted.
CC2.3.6	Prior to engaging a third-party, Enablon requires the following third-party management program procedures: • Conduct due diligence. • Sign confidentiality or nondisclosure agreements and/or alternate contract agreement that requires the third party to implement reasonable security practices and a right to audit. • Sign the supplier code of conduct or provide an equivalent standard.	Inspected the system-generated report of new third-party suppliers to determine whether any third parties with access to the Enablon system were added during the report period.	No tests of the control were performed, because the circumstances that warrant the operation of the control did not occur during the report period.

CC3 Risk Assessment

COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC3.1.1	Management utilizes control frameworks to manage and monitor internal controls and processes related to IT, finance, operations and compliance departments. If any issues are identified regarding IT or business processes, control activities are designed and developed to mitigate the risks to the achievement of objectives.	Inspected the RISE compliance register to determine whether management utilized a framework to manage and monitor internal controls and developed control activities for any issues identified.	No exceptions noted.
CC3.1.2	Divisional reporting meetings occur, based on the annual schedule, to review reporting on the main KPIs and business trends to the division. The meeting is run by the division CEO and attendees include Enablon's CEO, CFO and leaders of each division. Corrective action plans are created if warranted.	Inspected the meeting minutes for a sample of divisional reporting meetings to determine whether divisional reporting on the main KPIs and business trends were reviewed, and corrective action plans were created if warranted.	No exceptions noted.
CC3.1.3	The Wolters Kluwer risk objectives and assessment of risk are defined in the overall Wolters Kluwer risk management policy. The policy includes ownership of risks and defines how risks are identified, monitored and tracked through resolution. The policy is made available to employees and reviewed and approved by management annually.	Inspected the Wolters Kluwer risk management policy and corporate intranet site to determine whether it defined the overall risk management program, including the ownership of risks and how risks are identified, monitored and tracked through resolution, was made available to employees and was reviewed by management annually.	No exceptions noted.

COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC3.2.1	Vendor management's responsibilities and accountabilities are documented within the Third-Party Risk Management Standard. The standard outlines due diligence requirements for new and existing vendors, based on the risk of the vendor's services. The information security council reviews the Third-Party Risk Management Standard annually.	Inspected the Third-Party Risk Management Standard to determine whether the standard documented vendor management's responsibilities and accountabilities, due diligence procedures for new and existing vendors, and the standard was reviewed annually by the information security council.	No exceptions noted.
CC3.2.2	A risk assessment is conducted annually to identify potential risks, vulnerabilities and threats related to the entity, IT, fraud, third parties (i.e., vendors and business partner relationships), and significant changes (e.g., changes in external environment, business model, leadership, systems and technology, vendor and business partner relationships, etc.). Upon the completion of the risk assessment, management identifies whether the risk is adequately mitigated by current controls or if additional procedures are needed. The results are presented to the security board.	Inspected the risk assessment to determine whether it was conducted annually to identify potential risks, vulnerabilities and threats related to the entity, IT, fraud, third parties (i.e., vendors and business partner relationships), and significant changes (e.g., changes in external environment, business model, leadership, systems and technology, vendor and business partner relationships, etc.), and whether upon the completion of the risk assessment, management identified whether the risk was adequately mitigated by current controls or if additional procedures were needed.	No exceptions noted.
		Inspected the security board meeting minutes to determine whether the annual risk assessment results were presented to the security board.	No exceptions noted.
CC3.2.3	The IT department tracks end user hardware in ServiceNow and reviews annually.	Inspected the inventory listing to determine whether the IT department tracked end user system components, including end user hardware.	No exceptions noted.
		Inspected the evidence of a review of end user system components, including end user hardware, to determine whether the IT department reviewed them on an annual basis.	No exceptions noted.

CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC3.3.1	A risk assessment is conducted annually to identify potential risks, vulnerabilities and threats related to the entity, IT, fraud, third parties (i.e., vendors and business partner relationships), and significant changes (e.g., changes in external environment, business model, leadership, systems and technology, vendor and business partner relationships, etc.). Upon the completion of the risk assessment, management identifies whether the risk is adequately mitigated by current controls or if additional procedures are needed. The results are presented to the security board.	Inspected the risk assessment to determine whether it was conducted annually to identify potential risks, vulnerabilities and threats related to the entity, IT, fraud, third parties (i.e., vendors and business partner relationships), and significant changes (e.g., changes in external environment, business model, leadership, systems and technology, vendor and business partner relationships, etc.), and whether upon the completion of the risk assessment, management identified whether the risk was adequately mitigated by current controls or if additional procedures were needed.	No exceptions noted.
		Inspected the security board meeting minutes to determine whether the annual risk assessment results were presented to the security board.	No exceptions noted.
CC3.3.2	The security board meets on a quarterly basis to review open and upcoming projects, discuss overall IT strategies, review current system performance and evaluate the impacts of environmental, regulatory and technological changes and their effect on the security of the Enablon platform.	Inspected the minutes and invites from meetings between top management and members of the security board for a sample of quarters to determine whether the meetings were held to review open and upcoming projects, discuss overall IT strategies, review current system security performance and evaluate the impacts of environmental, regulatory and technological changes and their effect on the security of the Enablon platform.	No exceptions noted.

CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC3.4.1	The security board meets on a quarterly basis to review open and upcoming projects, discuss overall IT strategies, review current system performance and evaluate the impacts of environmental, regulatory and technological changes and their effect on the security of the Enablon platform.	Inspected the minutes and invites from meetings between top management and members of the security board for a sample of quarters to determine whether the meetings were held to review open and upcoming projects, discuss overall IT strategies, review current system security performance and evaluate the impacts of environmental, regulatory and technological changes and their effect on the security of the Enablon platform.	No exceptions noted.
CC3.4.2	A risk assessment is conducted annually to identify potential risks, vulnerabilities and threats related to the entity, IT, fraud, third parties (i.e., vendors and business partner relationships), and significant changes (e.g., changes in external environment, business model, leadership, systems and technology, vendor and business partner relationships, etc.). Upon the completion of the risk assessment, management identifies whether the risk is adequately mitigated by current controls or if additional procedures are needed. The results are presented to the security board.	Inspected the risk assessment to determine whether it was conducted annually to identify potential risks, vulnerabilities and threats related to the entity, IT, fraud, third parties (i.e., vendors and business partner relationships), and significant changes (e.g., changes in external environment, business model, leadership, systems and technology, vendor and business partner relationships, etc.), and whether upon the completion of the risk assessment, management identified whether the risk was adequately mitigated by current controls or if additional procedures were needed.	No exceptions noted.
		Inspected the security board meeting minutes to determine whether the annual risk assessment results were presented to the security board.	No exceptions noted.
CC3.4.3	Annually, management conducts reviews of key vendors, which includes a review of SOC reports for the subservice organizations. If any deviations are identified, corrective action is taken as warranted.	Inspected the vendor SOC report evaluation memos for the subservice organizations to determine whether management conducted an annual review of SOC reports and if any deviations were identified, corrective action was taken as warranted.	No exceptions noted.

CC4 Monitoring Activities

CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
	Provided by Enablon	***Provided by RSM US LLP***	
	Control	**Test Performed**	**Test Results**
CC4.1.1	The information audit director establishes an audit schedule and performs internal reviews annually. Results and action plans are reported to the security board.	Inspected the results of internal audits to determine whether the information audit director performed the audits annually.	No exceptions noted.
		Inspected the annual security board meeting minutes to determine whether the information audit director reported the results to the security board.	No exceptions noted.
CC4.1.2	Monthly external vulnerability scans are performed by the information security team. Management reviews the monthly scan results and uses tickets to document and track the resolution of critical and severe issues.	Inspected the results of the external vulnerability scan for a sample of months to determine whether it was performed, reviewed by management, and critical and severe issues identified were tracked and resolved, if applicable.	No exceptions noted.
CC4.1.3	An annual penetration test is performed to identify potential vulnerabilities in the software. The resolution of high-risk items is documented and tracked in the ticketing system.	Inspected the results of the annual penetration test to determine whether it was completed, and high-risk issues observed were documented and tracked within the ticketing system, if applicable.	No exceptions noted.
CC4.1.4	Quarterly management calls occur between the Enablon executive leadership team and the management team to review the main KPIs that drive the business. Attendees include line managers in the business, including but not limited to, finance, operations, IT and HR.	Inspected the management meeting minutes for a sample of quarters to determine whether the Enablon executive leadership team met with the management team to review the main KPIs that drive the business, which included finance, operations, IT and HR departments.	No exceptions noted.
CC4.1.5	Divisional reporting meetings occur, based on the annual schedule, to review reporting on the main KPIs and business trends to the division. The meeting is run by the division CEO and attendees include Enablon's CEO, CFO and leaders of each division. Corrective action plans are created if warranted.	Inspected the meeting minutes for a sample of divisional reporting meetings to determine whether divisional reporting on the main KPIs and business trends were reviewed, and corrective action plans were created if warranted.	No exceptions noted.

CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
	Provided by Enablon	***Provided by RSM US LLP***	
	Control	**Test Performed**	**Test Results**
CC4.2.1	The information audit director establishes an audit schedule and performs internal reviews annually. Results and action plans are reported to the security board.	Inspected the results of internal audits to determine whether the information audit director performed the audits annually.	No exceptions noted.
		Inspected the annual security board meeting minutes to determine whether the information audit director reported the results to the security board.	No exceptions noted.
CC4.2.2	The information audit director monitors compliance deviations and violations that result in deficiencies in internal control. Monitoring takes place such that deficiencies are ultimately resolved by management in a timely manner.	Inspected the documentation to determine whether the information audit director monitors compliance deviations and violations that result in deficiencies in internal control, and whether monitoring takes place such that deficiencies are ultimately resolved by management in a timely manner.	No exceptions noted.
CC4.2.3	The security board meets on a quarterly basis to review open and upcoming projects, discuss overall IT strategies, review current system performance and evaluate the impacts of environmental, regulatory and technological changes and their effect on the security of the Enablon platform.	Inspected the minutes and invites from meetings between top management and members of the security board for a sample of quarters to determine whether the meetings were held to review open and upcoming projects, discuss overall IT strategies, review current system security performance and evaluate the impacts of environmental, regulatory and technological changes and their effect on the security of the Enablon platform.	No exceptions noted.

CC5 Control Activities

CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC5.1.1	A risk assessment is conducted annually to identify potential risks, vulnerabilities and threats related to the entity, IT, fraud, third parties (i.e., vendors and business partner relationships), and significant changes (e.g., changes in external environment, business model, leadership, systems and technology, vendor and business partner relationships, etc.). Upon the completion of the risk assessment, management identifies whether the risk is adequately mitigated by current controls or if additional procedures are needed. The results are presented to the security board.	Inspected the risk assessment to determine whether it was conducted annually to identify potential risks, vulnerabilities and threats related to the entity, IT, fraud, third parties (i.e., vendors and business partner relationships), and significant changes (e.g., changes in external environment, business model, leadership, systems and technology, vendor and business partner relationships, etc.), and whether upon the completion of the risk assessment, management identified whether the risk was adequately mitigated by current controls or if additional procedures were needed.	No exceptions noted.
		Inspected the security board meeting minutes to determine whether the annual risk assessment results were presented to the security board.	No exceptions noted.
CC5.1.2	Management utilizes control frameworks to manage and monitor internal controls and processes related to IT, finance, operations and compliance departments. If any issues are identified regarding IT or business processes, control activities are designed and developed to mitigate the risks to the achievement of objectives.	Inspected the RISE compliance register to determine whether management utilized a framework to manage and monitor internal controls and developed control activities for any issues identified.	No exceptions noted.
CC5.1.3	The information audit director maintains a master listing of internal controls in RISE, including those pertaining to the security of the Enablon platform. As part of the annual audit planning cycle, the information audit director reviews and updates the master listing of internal controls.	Inspected the master listing of internal controls in RISE to determine whether the information audit director reviewed and updated the master listing annually.	No exceptions noted.

CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC5.2.1	The information audit director maintains a master listing of internal controls in RISE, including those pertaining to the security of the Enablon platform. As part of the annual audit planning cycle, the information audit director reviews and updates the master listing of internal controls.	Inspected the master listing of internal controls in RISE to determine whether the information audit director reviewed and updated the master listing annually.	No exceptions noted.
CC5.2.2	The security board meets on a quarterly basis to review open and upcoming projects, discuss overall IT strategies, review current system performance and evaluate the impacts of environmental, regulatory and technological changes and their effect on the security of the Enablon platform.	Inspected the minutes and invites from meetings between top management and members of the security board for a sample of quarters to determine whether the meetings were held to review open and upcoming projects, discuss overall IT strategies, review current system security performance and evaluate the impacts of environmental, regulatory and technological changes and their effect on the security of the Enablon platform.	No exceptions noted.
CC5.2.3	A risk assessment is conducted annually to identify potential risks, vulnerabilities and threats related to the entity, IT, fraud, third parties (i.e., vendors and business partner relationships), and significant changes (e.g., changes in external environment, business model, leadership, systems and technology, vendor and business partner relationships, etc.). Upon the completion of the risk assessment, management identifies whether the risk is adequately mitigated by current controls or if additional procedures are needed. The results are presented to the security board.	Inspected the risk assessment to determine whether it was conducted annually to identify potential risks, vulnerabilities and threats related to the entity, IT, fraud, third parties (i.e., vendors and business partner relationships), and significant changes (e.g., changes in external environment, business model, leadership, systems and technology, vendor and business partner relationships, etc.), and whether upon the completion of the risk assessment, management identified whether the risk was adequately mitigated by current controls or if additional procedures were needed.	No exceptions noted.
		Inspected the security board meeting minutes to determine whether the annual risk assessment results were presented to the security board.	No exceptions noted.

CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC5.3.1	Information security policies are reviewed by Wolters Kluwer management annually, and changes are communicated to internal users. Policies are located on the corporate intranet to communicate security commitments to internal users to enable them to carry out their responsibilities.	Inspected the global information security policies and their location on the intranet to determine whether they were communicated to internal users.	No exceptions noted.
		Inspected the information security policies to determine whether they were reviewed by Wolters Kluwer management annually.	No exceptions noted.
CC5.3.2	The data classification policy documents data handling and customer communication requirements based on the type of data under control. The policy is reviewed by management annually and made available to employees on the corporate intranet site.	Inspected the data classification policy and corporate intranet site to determine whether the policy documented data handling and customer communication requirements based on the type of data under control, and the policy was reviewed by management annually and made available to employees on the corporate intranet site.	No exceptions noted.
CC5.3.3	The security incident response plan outlines the responsibilities of employees to report identified incidents, as well as the procedures for reporting security incidents within the organization and notifying customers of incidents that may have affected their data. Management performs an annual review of the security incident response plan and updates the procedures, as necessary. The security incident response plan is communicated to authorized personnel on the corporate intranet site.	Inspected the security incident response plan and corporate intranet site to determine whether the responsibilities of employees to report identified incidents, as well as the procedures for reporting security incidents within the organization and notifying internal customers of incidents that may have affected their data were documented, the plan was reviewed by management annually, and communicated to authorized personnel on the corporate intranet site.	No exceptions noted.
CC5.3.4	A formal user access management policy documents the procedures for logical access to systems. The policy is reviewed by Enablon IT on an annual basis and updated, as needed. Additionally, the policy and related procedures are available to internal users.	Inspected the user access management policy to determine whether it documented the procedures for administering logical access to systems, and whether the user management policies were reviewed by IT annually and updated, as needed.	No exceptions noted.
		Inspected the company intranet to determine whether the user access management policy and related procedures were made available to internal users.	No exceptions noted.
CC5.3.5	A patch management policy is in place with the information systems group that governs the timing and strategy for testing and releasing patches into internal and production systems. The policy is reviewed annually by Enablon management and is available to internal users.	Inspected the patch management policy to determine whether a policy was in place with the information systems group that governs the timing and strategy for testing and releasing patches into internal and production systems, and the policy was reviewed by Enablon management annually.	No exceptions noted.
		Inspected the Confluence site to determine whether the patch management policy was made available to internal users.	No exceptions noted.

CC6 Logical and Physical Access Controls

CC6.1 The entity implements logical access security software, infrastructure and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
Provided by Enablon		***Provided by RSM US LLP***	
Control		**Test Performed**	**Test Results**
CC6.1.1	A username and password are required to authenticate and access the Enablon systems, including the network, VPN and the production servers. Password parameters require the following: • Complexity requirements enabled • Minimum password length of eight characters • Maximum password age of 365 days • Minimum history requirement of six prior passwords • Account lockout threshold after five failed login attempts	Inspected the password configurations for the Enablon network, VPN and production servers to determine whether authentication parameters were required to include the following: • Complexity requirements enabled • Minimum password length of eight characters • Maximum password age of 365 days • Minimum history requirement of six prior passwords • Account lockout threshold after five failed login attempts	No exceptions noted.
CC6.1.2	Firewalls have been implemented to segment the internal network and systems from direct access to the internet. The firewalls are configured so that systems are allocated an IP address within the IP range associated with the subnetwork they are connected to using DHCP or static allocation.	Inspected the firewall configurations to determine whether they had been implemented to segment the internal network and systems from direct access to the internet, and whether firewalls were configured to restrict access based on the assigned IP address.	No exceptions noted.
CC6.1.3	A combination IPS and IDS is in place to prevent and detect unauthorized connections to the network.	Inspected the IPS and IDS configurations to determine whether a combination IPS and IDS was in place to prevent and detect unauthorized connections to the network.	No exceptions noted.
CC6.1.4	Management has established a checklist for the setup and configuration of security for new devices added to the network. The checklist is maintained as a standard for new devices to outline the setup to meet minimum security requirements.	Inspected the device hardening checklists for a sample of new servers to determine whether checklists had been completed and maintained for new devices to document setup and adherence to baseline security requirements.	No exceptions noted.
CC6.1.5	The IT department tracks server hardware in the GLPI application and performs an annual review of the hardware list.	Inspected the GLPI application to determine whether the IT department tracked server hardware and performed an annual review of the hardware list.	No exceptions noted.

CC6.1 The entity implements logical access security software, infrastructure and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC6.1.6	Remote access to the production environment requires users to authenticate with a username, password and authentication certificate to establish an encrypted VPN session.	Inspected the VPN configurations to determine whether the VPN required a user ID and password for remote authentication to the production environment.	No exceptions noted.
CC6.1.7	Databases are either logically or physically segregated within the production environment to prevent the co-mingling of data between customers. Clients either subscribe to a shared server where multiple client databases are located within a shared SQL Server instance, or a dedicated server where clients are physically segregated from other clients.	Inspected the database security configurations to determine whether databases were either logically or physically segregated within the production environment to prevent the co-mingling of data between customers.	No exceptions noted.
CC6.1.8	Company laptops and workstations are secured with disk encryption management software.	Inspected the encryption status for a sample of laptops and workstations to determine whether company laptops and workstations were secured with disk encryption management software.	No exceptions noted.
CC6.1.9	Employee email messages are configured to automatically encrypt during transmission.	Inspected the email configurations to determine whether email messages were configured to automatically encrypt during transmission.	No exceptions noted.
CC6.1.10	Web application sessions are encrypted using TLS encryption.	Inspected the web application security settings to determine whether web application sessions were encrypted using TLS encryption.	No exceptions noted.
CC6.1.11	User workstations are configured to prevent the installation of software.	Inspected the global user workstation configuration to determine whether it was configured to prevent the installation of software.	No exceptions noted.
		Observed an attempt to install a prohibited application to determine whether the application was automatically blocked.	No exceptions noted.
CC6.1.12	Management has documented the external access points, flow of data and organization of the infrastructure within the Enablon network and platform. The network map is available for employee reference on a shared network file share.	Inspected the network diagram and its location to determine whether the external access points, flow of data and organization of the infrastructure were documented and available for employee reference on a shared network file share.	No exceptions noted.
CC6.1.13	Backups are scheduled to run daily and are automatically encrypted.	Inspected the configurations for the backup software to determine whether backups were scheduled to occur daily, and tapes were automatically encrypted.	No exceptions noted.

CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
Provided by Enablon		***Provided by RSM US LLP***	
Control		**Test Performed**	**Test Results**
CC6.2.1	Requests for internal access to the Enablon systems (e.g., network and production servers and databases) require manager and/or HR approval prior to access being granted.	Inspected the access request forms for a sample of new users to the Enablon systems to determine whether manager and/or HR approval was required prior to being granted access.	Exception noted. For one of 14 new users selected, access was not approved by management prior to being granted
CC6.2.2	Upon employee termination, management removes the employee's logical access to the Enablon systems (network, application, database and server). Logical access is disabled within 30 business days of employee's termination for standard accounts and within 24 hours of employee's termination for administrative accounts.	Inspected the account clearing logs for a sample of terminated employees to determine whether access to the Enablon systems was disabled or removed within 30 business days of employee's termination for standard accounts and within 24 hours of employee's termination for administrative accounts	Exceptions noted. For three of 15 terminated employees selected, logical access was not removed timely.
CC6.2.3	Reviews of internal users with access to the Active Directory are conducted by management quarterly. Necessary access modifications are performed based on results of the review.	Inspected management's Active Directory internal user access reviews for a sample of quarters to determine whether management performed the review, and necessary access modifications were performed based on the results of the review.	No exceptions noted.
CC6.2.4	Administrative access to the production servers and databases is limited to authorized internal users and reviewed by management quarterly. Necessary access modifications are performed based on the results of the review.	Inspected management's production server and database user access reviews for a sample of quarters to determine whether management performed the reviews, and necessary access modifications were performed based on the results of the reviews.	No exceptions noted.

CC6.3 The entity authorizes, modifies or removes access to data, software, functions and other protected information assets based on roles, responsibilities or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC6.3.1	Requests for internal access to the Enablon systems (e.g., network and production servers and databases) require manager and/or HR approval prior to access being granted.	Inspected the access request forms for a sample of new users to the Enablon systems to determine whether manager and/or HR approval was required prior to being granted access.	Exception noted. For one of 14 new users selected, access was not approved by management prior to being granted
CC6.3.2	Upon employee termination, management removes the employee's logical access to the Enablon systems (network, application, database and server). Logical access is disabled within 30 business days of employee's termination for standard accounts and within 24 hours of employee's termination for administrative accounts.	Inspected the account clearing logs for a sample of terminated employees to determine whether access to the Enablon systems was disabled or removed within 30 business days of employee's termination for standard accounts and within 24 hours of employee's termination for administrative accounts	Exceptions noted. For three of 15 terminated employees selected, logical access was not removed timely.
CC6.3.3	Reviews of internal users with access to the Active Directory are conducted by management quarterly. Necessary access modifications are performed based on results of the review.	Inspected management's Active Directory internal user access reviews for a sample of quarters to determine whether management performed the review, and necessary access modifications were performed based on the results of the review.	No exceptions noted.
CC6.3.4	Administrative access to the production servers and databases is limited to authorized internal users and reviewed by management quarterly. Necessary access modifications are performed based on the results of the review.	Inspected management's production server and database user access reviews for a sample of quarters to determine whether management performed the reviews, and necessary access modifications were performed based on the results of the reviews.	No exceptions noted.

CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.			
Provided by Enablon		***Provided by RSM US LLP***	
Control		**Test Performed**	**Test Results**
CC6.4.1	Physical access to the Enablon corporate facilities in Chicago, Illinois, and Bois-Colombes, France, including the computer room containing the internal IT hardware, is restricted to authorized individuals by a keycard system.	Observed the physical access to the Enablon corporate facilities in Bois-Colombes, France, and Chicago, Illinois, including the computer room, to determine whether access was restricted by a keycard system.	No exceptions noted.
CC6.4.2	A review of users with physical access to the Enablon corporate facilities and computer rooms in Chicago, Illinois, and Bois-Colombes, France, is performed annually by management. Necessary access modifications are performed based on the results of the review.	Inspected management's annual physical access review for the Enablon facilities in Bois-Colombes, France, and Chicago, Illinois, to determine whether management performed the review and necessary access modifications were performed based on the results of the review.	No exceptions noted.
CC6.4.3	Requests for physical access to the Enablon facilities in Chicago, Illinois, and Bois-Colombes, France, require manager approval prior to being granted access.	Inspected the access request forms for a sample of new employees to determine whether access requests were documented and approved by management prior to being granted access.	No exceptions noted.
CC6.4.4	Employee offboarding emails/notifications are sent to the office manager by management upon employee termination and document the request and removal of physical access.	Inspected the offboarding emails/notifications for a sample of terminated internal users to determine whether offboarding tasks were completed by management upon employee termination and document the removal of physical access.	No exceptions noted.
		Inspected the cardholder access listings or cardholder properties to the Enablon corporate facilities, computer rooms and co-location data centers for a sample of terminated employees to determine whether physical access to the Enablon facilities was disabled or removed.	No exceptions noted.
CC6.4.5	A review of the physical access activity log is performed on a semiannual basis by management. Necessary access modifications are performed based on the results of the review.	Inspected management's co-location facility physical access activity log review for a sample of semiannual reviews to determine whether management reviewed the physical access activity log and abnormal activity was investigated and resolved.	No exceptions noted.
CC6.4.6	Physical access to the Enablon co-location facilities is authorized by management and tracked within a log maintained by the third party that manages the facility.	Inspected the access tickets for a sample of new users to determine whether physical access to the Enablon co-location facilities was authorized by management.	No exceptions noted.

CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC6.5.1	Data is erased utilizing a certified data erasure process third-party tool before the device is physically destroyed.	Inspected the system-generated report of decommissioned assets to determine whether any physical assets were disposed of during the report period.	No tests of the control were performed, because the circumstances that warrant the operation of the control did not occur during the report period.
CC6.5.2	The IT department tracks server hardware in the GLPI application and performs an annual review of the hardware list.	Inspected the GLPI application to determine whether the IT department tracked server hardware and performed an annual review of the hardware list.	No exceptions noted.
CC6.5.3	The data classification policy documents data handling and customer communication requirements based on the type of data under control. The policy is reviewed by management annually and made available to employees on the corporate intranet site.	Inspected the data classification policy and corporate intranet site to determine whether the policy documented data handling and customer communication requirements based on the type of data under control, and the policy was reviewed by management annually and made available to employees on the corporate intranet site.	No exceptions noted.

CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC6.6.1	A combination IPS and IDS is in place to prevent and detect unauthorized connections to the network.	Inspected the IPS and IDS configurations to determine whether a combination IPS and IDS was in place to prevent and detect unauthorized connections to the network.	No exceptions noted.
CC6.6.2	The IPS and IDS are configured to alert management via emails in the event that a potential security incident is detected on the network. Critical alerts are reviewed by management monthly to determine whether corrective action is needed. Any issues are investigated and resolved.	Inspected the IPS and IDS configurations, and an example alert, to determine whether they were configured to alert management via emails in the event that a potential security incident was detected on the network.	No exceptions noted.
		Inspected the IPS logs for a sample of months to determine whether management reviewed the critical alerts, and any issues were investigated and resolved.	No exceptions noted.

CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
Provided by Enablon		***Provided by RSM US LLP***	
Control		**Test Performed**	**Test Results**
CC6.6.3	Remote access to the production environment requires users to authenticate with a username, password and authentication certificate to establish an encrypted VPN session.	Inspected the VPN configurations to determine whether the VPN required a user ID and password for remote authentication to the production environment.	No exceptions noted.
CC6.6.4	Firewalls have been implemented to segment the internal network and systems from direct access to the internet. The firewalls are configured so that systems are allocated an IP address within the IP range associated with the subnetwork they are connected to using DHCP or static allocation.	Inspected the firewall configurations to determine whether they had been implemented to segment the internal network and systems from direct access to the internet, and whether firewalls were configured to restrict access based on the assigned IP address.	No exceptions noted.
CC6.6.5	Antivirus software is installed on production servers and is configured to update on an hourly basis. The software sends automated alerts to the IT team when a threat has been detected.	Inspected the antivirus configurations to determine whether antivirus software was installed on production servers and configured to update definitions for servers on an hourly basis.	No exceptions noted.
		Inspected the antivirus configurations and an example alert to determine whether antivirus software was configured to automatically alert the IT team when a threat was detected.	No exceptions noted.
CC6.6.6	Anti-malware software is installed on Enablon workstations. Enablon IT management performs a weekly review of noncompliant workstations.	Inspected the anti-malware configurations to determine whether anti-malware software was installed on Enablon workstations.	No exceptions noted.
		Inspected management's anti-malware reviews for a sample of weeks to determine whether management reviewed for noncompliant workstations.	No exceptions noted.

CC6.7 The entity restricts the transmission, movement and removal of information to authorized internal and external users and processes, and protects it during transmission, movement or removal to meet the entity's objectives.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC6.7.1	Company laptops and workstations are secured with disk encryption management software.	Inspected the encryption status for a sample of laptops and workstations to determine whether company laptops and workstations were secured with disk encryption management software.	No exceptions noted.
CC6.7.2	Employee email messages are configured to automatically encrypt during transmission.	Inspected the email configurations to determine whether email messages were configured to automatically encrypt during transmission.	No exceptions noted.
CC6.7.3	Web application sessions are encrypted using TLS encryption.	Inspected the web application security settings to determine whether web application sessions were encrypted using TLS encryption.	No exceptions noted.
CC6.7.4	Management has established a checklist for the setup and configuration of security for new devices added to the network. The checklist is maintained as a standard for new devices to outline the setup to meet minimum security requirements.	Inspected the device hardening checklists for a sample of new servers to determine whether checklists had been completed and maintained for new devices to document setup and adherence to baseline security requirements.	No exceptions noted.
CC6.7.5	Remote access to the production environment requires users to authenticate with a username, password and authentication certificate to establish an encrypted VPN session.	Inspected the VPN configurations to determine whether the VPN required a user ID and password for remote authentication to the production environment.	No exceptions noted.
CC6.7.6	Backups are scheduled to run daily and are automatically encrypted.	Inspected the configurations for the backup software to determine whether backups were scheduled to occur daily, and tapes were automatically encrypted.	No exceptions noted.
CC6.7.7	Data loss prevention (DLP) technologies are in place within email configurations to alert the sender if Social Security numbers, Individual Taxpayer Identification Numbers, U.S./U.K. passport numbers, credit card numbers or ABA routing numbers are present in outbound communications in order to protect key confidential data from being transmitted outside of the organization.	Observed an email being sent with sensitive information to determine whether the system alerted the sender to protect key confidential data from being transmitted outside of the organization.	No exceptions noted.
		Inspected the DLP/email configurations to determine whether configurations were set to alert the sender and encrypt the message if Social Security numbers, Individual Taxpayer Identification Numbers, U.S./U.K. passport numbers, credit card numbers, ABA routing numbers or driver's license numbers were present.	No exceptions noted.
CC6.7.8	Data at rest is encrypted.	Inspected the encryption settings/configurations to determine whether data at rest was encrypted.	No exceptions noted.

CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC6.8.1	Antivirus software is installed on production servers and is configured to update on an hourly basis. The software sends automated alerts to the IT team when a threat has been detected.	Inspected the antivirus configurations to determine whether antivirus software was installed on production servers and configured to update definitions for servers on an hourly basis.	No exceptions noted.
		Inspected the antivirus configurations and an example alert to determine whether antivirus software was configured to automatically alert the IT team when a threat was detected.	No exceptions noted.
CC6.8.2	Anti-malware software is installed on Enablon workstations. Enablon IT management performs a weekly review of noncompliant workstations.	Inspected the anti-malware configurations to determine whether anti-malware software was installed on Enablon workstations.	No exceptions noted.
		Inspected management's anti-malware reviews for a sample of weeks to determine whether management reviewed for noncompliant workstations.	No exceptions noted.
CC6.8.3	Monthly external vulnerability scans are performed by the information security team. Management reviews the monthly scan results and uses tickets to document and track the resolution of critical and severe issues.	Inspected the results of the external vulnerability scan for a sample of months to determine whether it was performed, reviewed by management, and critical and severe issues identified were tracked and resolved, if applicable.	No exceptions noted.
CC6.8.4	An annual penetration test is performed to identify potential vulnerabilities in the software. The resolution of high-risk items is documented and tracked in the ticketing system.	Inspected the results of the annual penetration test to determine whether it was completed, and high-risk issues observed were documented and tracked within the ticketing system, if applicable.	No exceptions noted.
CC6.8.5	User workstations are configured to prevent the installation of software.	Inspected the global user workstation configuration to determine whether it was configured to prevent the installation of software.	No exceptions noted.
		Observed an attempt to install a prohibited application to determine whether the application was automatically blocked.	No exceptions noted.
CC6.8.6	A combination IPS and IDS is in place to prevent and detect unauthorized connections to the network.	Inspected the IPS and IDS configurations to determine whether a combination IPS and IDS was in place to prevent and detect unauthorized connections to the network.	No exceptions noted.

CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC6.8.7	The IPS and IDS are configured to alert management via emails in the event that a potential security incident is detected on the network. Critical alerts are reviewed by management monthly to determine whether corrective action is needed. Any issues are investigated and resolved.	Inspected the IPS and IDS configurations, and an example alert, to determine whether they were configured to alert management via emails in the event that a potential security incident was detected on the network.	No exceptions noted.
		Inspected the IPS logs for a sample of months to determine whether management reviewed the critical alerts, and any issues were investigated and resolved.	No exceptions noted.
CC6.8.8	Firewall activity logs, including changes to firewall rules and firewall security configurations are reviewed by management monthly to determine whether firewall configurations are appropriate. Modifications are made as a result of the review, if necessary.	Inspected management's firewall reviews for a sample of months to determine whether management reviewed the firewall activity logs and modifications were made as a result of the review, if necessary.	No exceptions noted.
CC6.8.9	Management maintains a formal SDLC policy that documents the requirements for approving, testing, reviewing and authorizing application changes. The SDLC policy is reviewed annually by Enablon management and is available to internal users.	Inspected the SDLC policy to determine whether it documented the requirements for approving, testing, reviewing and authorizing application changes and the policy was reviewed by management annually.	No exceptions noted.
		Inspected the Confluence site to determine whether the SDLC policy was made available to internal users.	No exceptions noted.

CC7 System Operations

CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities and (2) susceptibilities to newly discovered vulnerabilities.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC7.1.1	Monthly external vulnerability scans are performed by the information security team. Management reviews the monthly scan results and uses tickets to document and track the resolution of critical and severe issues.	Inspected the results of the external vulnerability scan for a sample of months to determine whether it was performed, reviewed by management, and critical and severe issues identified were tracked and resolved, if applicable.	No exceptions noted.
CC7.1.2	An annual penetration test is performed to identify potential vulnerabilities in the software. The resolution of high-risk items is documented and tracked in the ticketing system.	Inspected the results of the annual penetration test to determine whether it was completed, and high-risk issues observed were documented and tracked within the ticketing system, if applicable.	No exceptions noted.
CC7.1.3	A baseline configuration of IT and control systems is created and maintained.	Inspected the patch management and imaging procedure for IT and control systems to determine whether it was created and maintained.	No exceptions noted.
CC7.1.4	Firewall activity logs, including changes to firewall rules and firewall security configurations are reviewed by management monthly to determine whether firewall configurations are appropriate. Modifications are made as a result of the review, if necessary.	Inspected management's firewall reviews for a sample of months to determine whether management reviewed the firewall activity logs and modifications were made as a result of the review, if necessary.	No exceptions noted.
CC7.1.5	Management has established a checklist for the setup and configuration of security for new devices added to the network. The checklist is maintained as a standard for new devices to outline the setup to meet minimum security requirements.	Inspected the device hardening checklists for a sample of new servers to determine whether checklists had been completed and maintained for new devices to document setup and adherence to baseline security requirements.	No exceptions noted.

CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
Provided by Enablon		***Provided by RSM US LLP***	
Control		**Test Performed**	**Test Results**
CC7.2.1	Firewalls have been implemented to segment the internal network and systems from direct access to the internet. The firewalls are configured so that systems are allocated an IP address within the IP range associated with the sub-network they are connected to using DHCP or static allocation.	Inspected the firewall configurations to determine whether they had been implemented to segment the internal network and systems from direct access to the internet, and whether firewalls were configured to restrict access based on the assigned IP address.	No exceptions noted.
CC7.2.2	The IPS and IDS are configured to alert management via emails in the event that a potential security incident is detected on the network. Critical alerts are reviewed by management monthly to determine whether corrective action is needed. Any issues are investigated and resolved.	Inspected the IPS and IDS configurations, and an example alert, to determine whether they were configured to alert management via emails in the event that a potential security incident was detected on the network.	No exceptions noted.
		Inspected the IPS logs for a sample of months to determine whether management reviewed the critical alerts, and any issues were investigated and resolved.	No exceptions noted.
CC7.2.3	Firewall activity logs, including changes to firewall rules and firewall security configurations are reviewed by management monthly to determine whether firewall configurations are appropriate. Modifications are made as a result of the review, if necessary.	Inspected management's firewall reviews for a sample of months to determine whether management reviewed the firewall activity logs and modifications were made as a result of the review, if necessary.	No exceptions noted.

CC7.3 The entity evaluates security events to determine whether they could result or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
Provided by Enablon		***Provided by RSM US LLP***	
Control		**Test Performed**	**Test Results**
CC7.3.1	Security incidents are classified, tracked, monitored and resolved by management. If incidents affect customers, they are communicated to those respective customers within two business days.	Inspected the system-generated report of incidents to determine whether any security incidents that affected customers occurred during the report period.	No tests of the control were performed, because the circumstances that warrant the operation of the control did not occur during the report period.
CC7.3.2	The security board, which includes the information security director, reviews security events and any potential critical incidents during the board's quarterly meetings.	Inspected the security board meeting minutes for a sample of quarters to determine whether the security board reviewed security events and any potential critical incidents.	No exceptions noted.
CC7.3.3	The IPS and IDS are configured to alert management via emails in the event that a potential security incident is detected on the network. Critical alerts are reviewed by management monthly to determine whether corrective action is needed. Any issues are investigated and resolved.	Inspected the IPS and IDS configurations, and an example alert, to determine whether they were configured to alert management via emails in the event that a potential security incident was detected on the network.	No exceptions noted.
		Inspected the IPS logs for a sample of months to determine whether management reviewed the critical alerts, and any issues were investigated and resolved.	No exceptions noted.
CC7.3.4	Firewall activity logs, including changes to firewall rules and firewall security configurations are reviewed by management monthly to determine whether firewall configurations are appropriate. Modifications are made as a result of the review, if necessary.	Inspected management's firewall reviews for a sample of months to determine whether management reviewed the firewall activity logs and modifications were made as a result of the review, if necessary.	No exceptions noted.

CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate and communicate security incidents, as appropriate.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC7.4.1	The security incident response plan outlines the responsibilities of employees to report identified incidents, as well as the procedures for reporting security incidents within the organization and notifying customers of incidents that may have affected their data. Management performs an annual review of the security incident response plan and updates the procedures, as necessary. The security incident response plan is communicated to authorized personnel on the corporate intranet site.	Inspected the security incident response plan and corporate intranet site to determine whether the responsibilities of employees to report identified incidents, as well as the procedures for reporting security incidents within the organization and notifying internal customers of incidents that may have affected their data were documented, the plan was reviewed by management annually, and communicated to authorized personnel on the corporate intranet site.	No exceptions noted.
CC7.4.2	Security incidents are classified, tracked, monitored and resolved by management. If incidents affect customers, they are communicated to those respective customers within two business days.	Inspected the system-generated report of incidents to determine whether any security incidents that affected customers occurred during the report period.	No tests of the control were performed, because the circumstances that warrant the operation of the control did not occur during the report period.
CC7.4.3	The security board, which includes the information security director, reviews security events and any potential critical incidents during the board's quarterly meetings.	Inspected the security board meeting minutes for a sample of quarters to determine whether the security board reviewed security events and any potential critical incidents.	No exceptions noted.

CC7.5 The entity identifies, develops and implements activities to recover from identified security incidents.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC7.5.1	The security incident response plan outlines the responsibilities of employees to report identified incidents, as well as the procedures for reporting security incidents within the organization and notifying customers of incidents that may have affected their data. Management performs an annual review of the security incident response plan and updates the procedures, as necessary. The security incident response plan is communicated to authorized personnel on the corporate intranet site.	Inspected the security incident response plan and corporate intranet site to determine whether the responsibilities of employees to report identified incidents, as well as the procedures for reporting security incidents within the organization and notifying internal customers of incidents that may have affected their data were documented, the plan was reviewed by management annually, and communicated to authorized personnel on the corporate intranet site.	No exceptions noted.
CC7.5.2	A root cause analysis is prepared and reviewed for critical security incidents that require remediation.	Inspected the system-generated report of incidents to determine whether any critical security incidents occurred during the report period.	No tests of the control were performed, because the circumstances that warrant the operation of the control did not occur during the report period.
CC7.5.3	The security incident response plan is tested by management annually to evaluate the effectiveness to respond to, understand, contain, remediate and communicate security incidents.	Inspected the results of the security incident response plan annual test to determine whether the security incident response plan was tested by management annually to evaluate the effectiveness to respond, understand, contain, remediate and communicate security incidents.	No exceptions noted.
CC7.5.4	Quarterly backup restoration tests are performed to ensure the data it contains is still readable, that the procedures are still valid, and that staff is adequately trained to perform a restore when necessary.	Inspected the backup restoration test tickets for a sample of quarters to determine whether backup restoration tests were performed.	No exceptions noted.

CC8 Change Management

CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves and implements changes to infrastructure, data, software and procedures to meet its objectives.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC8.1.1	Management maintains a formal SDLC policy that documents the requirements for approving, testing, reviewing and authorizing application changes. The SDLC policy is reviewed annually by Enablon management and is available to internal users.	Inspected the SDLC policy to determine whether it documented the requirements for approving, testing, reviewing and authorizing application changes and the policy was reviewed by management annually.	No exceptions noted.
		Inspected the Confluence site to determine whether the SDLC policy was made available to internal users.	No exceptions noted.
CC8.1.2	R&D sprint planning meetings are held on a biweekly basis to authorize and assign product backlog items for development in the upcoming sprint.	Inspected the meeting dashboards for a sample of biweekly R&D sprint planning meeting occurrences to determine whether the meetings were held to assign product backlog items in SOFTWARE for development in the upcoming sprint.	No exceptions noted.
CC8.1.3	Management has established a checklist for the setup and configuration of security for new devices added to the network. The checklist is maintained as a standard for new devices to outline the setup to meet minimum security requirements.	Inspected the device hardening checklists for a sample of new servers to determine whether checklists had been completed and maintained for new devices to document setup and adherence to baseline security requirements.	No exceptions noted.
CC8.1.4	Security patches, including security updates for Windows server components, are managed and documented by the infrastructure team using a staging approach to test and release into internal and production systems.	Inspected the patching logs and Microsoft Update Catalogs for a sample of infrastructure changes to determine whether patches, including security updates, were managed documented by the infrastructure team using a staging approach to test and release into internal and production systems.	No exceptions noted.
CC8.1.5	Firewall activity logs, including changes to firewall rules and firewall security configurations are reviewed by management monthly to determine whether firewall configurations are appropriate. Modifications are made as a result of the review, if necessary.	Inspected management's firewall reviews for a sample of months to determine whether management reviewed the firewall activity logs and modifications were made as a result of the review, if necessary.	No exceptions noted.
CC8.1.6	A patch management policy is in place with the information systems group that governs the timing and strategy for testing and releasing patches into internal and production systems. The policy is reviewed annually by Enablon management and is available to internal users.	Inspected the patch management policy to determine whether a policy was in place with the information systems group that governs the timing and strategy for testing and releasing patches into internal and production systems, and the policy was reviewed by Enablon management annually.	No exceptions noted.
		Inspected the Confluence site to determine whether the patch management policy was made available to internal users.	No exceptions noted.

CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves and implements changes to infrastructure, data, software and procedures to meet its objectives.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC8.1.7	Application emergency changes are documented in SOFTWARE tickets and tested and approved prior to deployment into production.	Inspected the SOFTWARE tickets for a sample of emergency changes to determine whether they were tested and approved prior to deployment into production.	No exceptions noted.
CC8.1.8	Application change requests are approved by product owners prior to development.	Inspected the SOFTWARE tickets/workflows, build validations and Azure DevOps workflows for a sample of application changes to determine whether they were documented and approved prior to development.	No exceptions noted.
CC8.1.9	Segregation of duties exist between users with access to develop and test application changes and users with access to promote releases to the production environment. Annually, management completes a review of internal user access as it relates to segregation of duties within the change environments. Necessary access modifications are performed based on the results of the review.	Inspected management's annual segregation of duties review of users with access to develop and test application changes and users with access to promote releases to the production environment to determine whether management completed the review and necessary access modifications were performed based on the results of the review.	No exceptions noted.
CC8.1.10	Internal users with access to Enablon source code are reviewed by Enablon management on a quarterly basis to validate that access is limited to authorized users. Necessary access modifications are performed based on the results of the review.	Inspected management's source code access reviews for a sample of quarters to determine whether management performed the review and necessary access modifications were performed based on the results of the reviews.	No exceptions noted.
CC8.1.11	R&D personnel combine the changes into a build that is ready for release. QA personnel test the build before authorizing the build for release into production.	Inspected the SOFTWARE tickets and/or Azure DevOps workflows for a sample of application changes to determine whether R&D personnel combined the changes into a build, and QA personnel tested the build before authorizing for release into production.	No exceptions noted.
CC8.1.12	Infrastructure changes and patches, including security updates for Enablon application server components, are managed and documented by the infrastructure team using a staging approach to test, approve and release into internal and production systems.	Inspected the change tickets for a sample of infrastructure changes to determine whether changes were documented by the infrastructure team using a staging approach to test and release into internal and production systems.	No exceptions noted.

CC9 Risk Mitigation

CC9.1 The entity identifies, selects and develops risk mitigation activities for risks arising from potential business disruptions.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC9.1.1	The security incident response plan is tested by management annually to evaluate the effectiveness to respond to, understand, contain, remediate and communicate security incidents.	Inspected the results of the security incident response plan annual test to determine whether the security incident response plan was tested by management annually to evaluate the effectiveness to respond, understand, contain, remediate and communicate security incidents.	No exceptions noted.
CC9.1.2	Wolters Kluwer maintains a cybersecurity insurance policy to mitigate the impact of security incidents and renews the policy annually.	Inspected the Wolters Kluwer cybersecurity certificate of insurance to determine whether Wolters Kluwer had a cybersecurity insurance policy in place to mitigate the impact of security incidents and the policy was renewed annually.	No exceptions noted.

CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC9.2.1	Annually, management conducts reviews of key vendors, which includes a review of SOC reports for the subservice organizations. If any deviations are identified, corrective action is taken as warranted.	Inspected the vendor SOC report evaluation memos for the subservice organizations to determine whether management conducted an annual review of SOC reports and if any deviations were identified, corrective action was taken as warranted.	No exceptions noted.
CC9.2.2	A risk assessment is conducted annually to identify potential risks, vulnerabilities and threats related to the entity, IT, fraud, third parties (i.e., vendors and business partner relationships), and significant changes (e.g., changes in external environment, business model, leadership, systems and technology, vendor and business partner relationships, etc.). Upon the completion of the risk assessment, management identifies whether the risk is adequately mitigated by current controls or if additional procedures are needed. The results are presented to the security board.	Inspected the risk assessment to determine whether it was conducted annually to identify potential risks, vulnerabilities and threats related to the entity, IT, fraud, third parties (i.e., vendors and business partner relationships), and significant changes (e.g., changes in external environment, business model, leadership, systems and technology, vendor and business partner relationships, etc.), and whether upon the completion of the risk assessment, management identified whether the risk was adequately mitigated by current controls or if additional procedures were needed.	No exceptions noted.
		Inspected the security board meeting minutes to determine whether the annual risk assessment results were presented to the security board.	No exceptions noted.

CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
Provided by Enablon		*Provided by RSM US LLP*	
Control		**Test Performed**	**Test Results**
CC9.2.3	Vendor management's responsibilities and accountabilities are documented within the Third-Party Risk Management Standard. The standard outlines due diligence requirements for new and existing vendors, based on the risk of the vendor's services. The information security council reviews the Third-Party Risk Management Standard annually.	Inspected the Third-Party Risk Management Standard to determine whether the standard documented vendor management's responsibilities and accountabilities, due diligence procedures for new and existing vendors, and the standard was reviewed annually by the information security council.	No exceptions noted.
CC9.2.4	Prior to engaging a third-party, Enablon requires the following third-party management program procedures: • Conduct due diligence. • Sign confidentiality or nondisclosure agreements and/or alternate contract agreement that requires the third party to implement reasonable security practices and a right to audit. • Sign the supplier code of conduct or provide an equivalent standard.	Inspected the system-generated report of new third-party suppliers to determine whether any third parties with access to the Enablon system were added during the report period.	No tests of the control were performed, because the circumstances that warrant the operation of the control did not occur during the report period.

V. Other Information Provided by Enablon

The information included in this section of the report is presented by Enablon to provide additional information to user organizations and is not a part of Enablon's description of controls placed in operation. The information in this section has not been subjected to the procedures applied in the examination of the description of controls applicable to the processing of transactions for user organizations and, accordingly, we express no opinion on it.

Management Responses to Testing Exceptions

Control #	Control	Test Results	Management's Response
CC1.1.1 CC2.2.3	New hires are provided company policies that document employee responsibilities, including the code of conduct, upon hire. At the time of hire, personnel are required to review and affirm personnel policies.	Exception noted. For one of 14 new hires selected, the employee did not review and affirm the personnel policies in a timely manner.	The new hire reviewed and affirmed the personnel policies immediately after he was reminded this had to be done 47 days after hire. In addition to this control, the employment contract that employees must sign prior to starting work for Wolters Kluwer contains a statement that requires compliance with corporate policies.
CC6.2.1 CC6.3.1	Requests for internal access to the Enablon systems (e.g., network and production servers and databases) require manager and/or HR approval prior to access being granted.	Exception noted. For one of 14 new users selected, access was not approved by management prior to being granted	Access was granted to a legitimate user. However, documentation of formal management approval was missing. Teams have been reminded that the process requires a ticket to be created and approved prior to granting access.
CC6.2.2 CC6.3.2	Upon employee termination, management removes the employee's logical access to the Enablon systems (network, application, database and server). Logical access is disabled within 30 business days of employee's termination for standard accounts and within 24 hours of employee's termination for administrative accounts.	Exceptions noted. For three of 15 terminated employees selected, logical access was not removed timely.	Access removal is still partially a manual process. An ongoing initiative aims at expanding the scope of automation between HR and IT systems to introduce greater reliability in timely access removal. Note that, when possible, based on the timing of the individual terminations and the subsequent user access review date, terminated user exceptions were identified and resolved via quarterly user access reviews, which demonstrates the effectiveness of these reviews.