A-LIGN

1WorldSync

Type 2 SOC 3

2024

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

July 1, 2023 to June 30, 2024

Table of Contents

SECTION 1

ASSERTION OF 1WORLDSYNC MANAGEMENT

ASSERTION OF 1WORLDSYNC MANAGEMENT

July 15, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within 1WorldSync's ('the Company') Item Management, Product Introduction, Digital Asset, User Management, Communications Hub, Data Sync Direct PIM, IM Integration Gateway, and Product Bundles Services System throughout the period July 1, 2023 to June 30, 2024, to provide reasonable assurance that 1WorldSync's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "1WorldSync's Description of Its Item Management, Product Introduction, Digital Asset, User Management, Communications Hub, Data Sync Direct PIM, IM Integration Gateway, and Product Bundles Services System throughout the period July 1, 2023 to June 30, 2024" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2023 to June 30, 2024, to provide reasonable assurance that 1WorldSync's service commitments and system requirements were achieved based on the trust services criteria. 1WorldSync's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "1WorldSync's Description of Its Item Management, Product Introduction, Digital Asset, User Management, Communications Hub, Data Sync Direct PIM, IM Integration Gateway, and Product Bundles Services System throughout the period July 1, 2023 to June 30, 2024".

1WorldSync uses Cyxtera Technologies, Inc ('Cyxtera' or 'subservice organization') to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at 1WorldSync, to achieve 1WorldSync's service commitments and system requirements based on the applicable trust services criteria. The description presents 1WorldSync's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of 1WorldSync's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve 1WorldSync's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of 1WorldSync's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2023 to June 30, 2024 to provide reasonable assurance that 1WorldSync's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of 1WorldSync's controls operated effectively throughout that period.

Julio DalMonte

Julio DalMonte
Chief Information Security Officer
1WorldSync

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

A-LIGN

INDEPENDENT SERVICE AUDITOR'S REPORT

To 1WorldSync:

Scope

We have examined 1WorldSync's accompanying assertion titled "Assertion of 1WorldSync Management" (assertion) that the controls within 1WorldSync's Item Management, Product Introduction, Digital Asset, User Management, Communications Hub, Data Sync Direct PIM, IM Integration Gateway, and Product Bundles Services System were effective throughout the period July 1, 2023 to June 30, 2024, to provide reasonable assurance that 1WorldSync's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in AICPA *Trust Services Criteria*.

1WorldSync uses Cyxtera to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at 1WorldSync, to achieve 1WorldSync's service commitments and system requirements based on the applicable trust services criteria. The description presents 1WorldSync's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of 1WorldSync's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at 1WorldSync, to achieve 1WorldSync's service commitments and system requirements based on the applicable trust services criteria. The description presents 1WorldSync's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of 1WorldSync's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

1WorldSync 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 1WorldSync's service commitments and system requirements were achieved. 1WorldSync has also provided the accompanying assertion (1WorldSync assertion) about the effectiveness of controls within the system. When preparing its assertion, 1WorldSync is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

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

Our examination included:

- Obtaining an understanding of the system and 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 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

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

Independence and Ethical Responsibilities

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

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that 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 and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within 1WorldSync's Item Management, Product Introduction, Digital Asset, User Management, Communications Hub, Data Sync Direct PIM, IM Integration Gateway, and Product Bundles Services System were suitably designed and operating effectively throughout the period July 1, 2023 to June 30, 2024, to provide reasonable assurance that 1WorldSync's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of 1WorldSync's controls operated effectively throughout that period.

The SOC logo for Service Organizations on 1WorldSync's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of 1WorldSync, user entities of 1WorldSync's Item Management, Product Introduction, Digital Asset, User Management, Communications Hub, Data Sync Direct PIM, IM Integration Gateway, and Product Bundles Services System during some or all of the period July 1, 2023 to June 30, 2024, business partners of 1WorldSync subject to risks arising from interactions with the Item Management, Product Introduction, Digital Asset, User Management, Communications Hub, Data Sync Direct PIM, IM Integration Gateway, and Product Bundles Services System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

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

A-LIGN ASSURANCE

Tampa, Florida
July 15, 2024

SECTION 3

1WORLDSYNC'S DESCRIPTION OF ITS ITEM MANAGEMENT, PRODUCT INTRODUCTION, DIGITAL ASSET, USER MANAGEMENT, COMMUNICATIONS HUB, DATA SYNC DIRECT PIM, IM INTEGRATION GATEWAY, AND PRODUCT BUNDLES SERVICES SYSTEM THROUGHOUT THE PERIOD JULY 1, 2023 TO JUNE 30, 2024

OVERVIEW OF OPERATIONS

Company Background

1WorldSync was established in 2012 and reorganized in 2019 with the objective of providing solutions to create, manage, syndicate, and optimize product content using the platform suite of services. These solutions are delivered to customers via web-based applications and application program interfaces. The organization is based in Chicago, Illinois, with cloud data centers sites in Illinois, New Jersey, Virginia, and Iowa.

Industries served by 1WorldSync include thousands of companies in Consumer Packaged Goods (CPG), Do It Yourself (DIY), Electronics and Hardlines, Electronic Retailing (E-tailing), Food Services and Healthcare sectors.

Description of Services Provided

1WorldSync provides product content orchestration platform services globally. The Company was founded in 2012 and reorganized in 2019 providing the assets, technologies, and processes supporting 1WorldSync's Item Management & Content Management (IMCM) suite of solutions including: Item Management, Product Introduction, Digital Asset, User Management, Communications Hub, Data Sync Direct PIM, IM Integration Gateway, and Product Bundles Services System to its customers.

1WorldSync's IMCM platform is a multiuser, transactional web-based set of applications. The IMCM platform applications provide a platform for the creation, management, optimization, and syndication of product content including:

- Item Management
- Product Introduction
- Digital Asset
- User Management
- Communications Hub
- Data Sync Direct PIM
- IM Integration Gateway
- Product Bundling

Customers utilize these services to create, manage, validate, and syndicate product content against retailer requirements and ensure that content is compliant with global data synchronization standards (GDSN).

Information is shared with user entities via secured websites, Application programming interfaces (APIs), and Applicability Statement 2 (AS2) systems.

Principal Service Commitments and System Requirements

1WorldSync designs its processes and procedures related to IMCM to meet its objectives for its product content orchestration platform. Those objectives are based on the service commitments that 1WorldSync. makes to user entities, the laws and regulations that govern the provision of product management and content syndication platform, and the financial, operational, and compliance requirements that 1WorldSync has established for the services.

The product content orchestration platform of 1WorldSync and its Information Security Management System (ISMS) are subject to the privacy and security laws and regulations in the jurisdictions in which 1WorldSync operates.

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

- Security principles within the fundamental designs of the IMCM services that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- The use of encryption technologies to protect customer data both at rest and in transit

1WorldSync establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in 1WorldSync's system policies and procedures, system design documentation, and contracts with customers.

1WorldSync's ISMS defines 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 services.

Components of the System

Infrastructure

Primary infrastructure used to provide 1WorldSync's Item Management, Product Introduction, Digital Asset, User Management, Communications Hub, Data Sync Direct PIM, IM Integration Gateway, and Product Bundles Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Virtual machine hypervisors, Database servers	HP DL360 Dell R650 Dell R750	Hosts, web, application, database, and component systems that support the companies Software as a Service (SaaS) applications in Colocation data centers
Firewalls	Palo Alto 450 Cisco Meraki	Filter traffic into and out of private networks for both commercial and corporate networks
Networking switches	Ruckus	Connect and control packet traffic between devices on all corporate and commercial networks
Google Cloud, AWS virtual machines, Kubernetes containers, platform services	Various	Provide various components of the IMCM Suite of services in a hybrid cloud model

Software

Primary software used for 1WorldSync's Item Management, Product Introduction, Digital Asset, User Management, Communications Hub, Data Sync Direct PIM, IM Integration Gateway, and Product Bundles Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Item Management	Linux	Product Information
Product Introduction	Linux	Product Introduction
User Management	Linux	User Administration
Communications Hub	Linux	Machine to Machine upload
Digital Asset Management	Linux	Product Digital Assets
Data Sync Direct PIM	Windows	Product Information Management
IM Integration Gateway	Linux	Product Information Management
Product Bundles	Linux	Automated Cross-sell Bundling

People

1WorldSync has a staff of approximately 500 employees organized in the following functional areas:

- *Corporate Departments*. Chief Executive Officer (CEO) and Departmental Executives for Finance, Human Resources, Marketing and Customer Success, Sales, Product, Integration, Operations, Customer Experience, Research and Development (R&D) Engineering, and Technology Operations. Staff in these departments provide functional processes to ensure the smooth running of 1WorldSync as a business.

The departments specifically and directly engaged with the creation, maintenance, delivery, security, strategy, and functionality of the IMCM (approx. 40 people) are as follows:

- *Product*. Product Management, product definition, project management, and requirements definition:
    - Product staff are knowledgeable on the use of IMCM, provide strategy, and prioritize functional enhancements
    - Product staff may utilize IMCM tools to report on and or provide data to customers at their request and or may utilize IMCM to demonstrate its functionality
- *R&D Engineering*. Engineering, Quality Assurance, DevOps:
    - Engineering staff develop IMCM applications in development environments, ensure the quality of the software released to production, and ensure that the software development lifecycle (SDLC) processes they utilize meet ISMS requirements
    - The Engineer staff develops and maintains the custom software that makes up the IMCM system and its supporting utilities. The staff includes software developers, software quality assurance, and technical writers
    - Engineering staff may utilize IMCM tools to create BI reports, provide data reporting to customers as needed, or manage the applications and deploy releases in the application environments
- *Technology Operations.* Infrastructure, Security:
    - Technology Operations staff deliver hosting services, administer systems, databases, and networks, and secure the IMCM platform in alignment with ISMS requirements
    - The Technology Operations staff typically have no direct use of the IMCM

- The security staff supports the IMCM directly by monitoring internal and external security threats, hardening systems, security scanning, using a defense in depth approach that aligns with 1WorldSync's ISMS
- The infrastructure staff maintain the inventory of Information Technology (IT) assets

Data

Data, as defined by 1WorldSync, constitutes the following:

- Item Management data
- Digital Catalog data
- Transaction processing data
- Output reports
- System files
- Error logs

Transaction processing for Item Management is initiated by the customer via encrypted machine to machine and or https web-based upload. It may also be input via the Data Sync Direct PIM, or the IM Integration Gateway. These tools provide an interface to manage and input Item Management data into the IMCM. Customers may also utilize API based services to access their data content and or digital assets. Data can be published to recipients via syndication tools within the IMCM system.

1WorldSync maintains transactional processing data that document arrival and processing of Item data from customers.

Output reports can be created within the IMCM system.

System and error log data is monitored via security information and event management (SIEM) and alerting mechanisms to ensure the smooth operation of the IMCM system.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the 1WorldSync policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any 1WorldSync team member.

Physical Security

1WorldSync maintains and Information Security Management System (ISMS) that has policies in place covering the 114 controls of ISO 27001 Annex A. The 114 controls are grouped into 14 control categories and 1WorldSync maintains procedures that align to these controls and include policies and procedures relating to physical security, logical access, computer operations, change control, and data communication standards, among others.

All teams are expected to adhere to the 1WorldSync policies and procedures that define how services should be delivered. Relevant policies are shared with staff, and they are reviewed annually.

The in-scope system and supporting infrastructure is hosted by Cyxtera. As such, Cyxtera is responsible for the physical security controls for the in-scope system. Refer to the "Subservice Organizations" section below for controls managed by the subservice organization.

Logical Access

1WorldSync uses a role-based access control approach that requires users of 1WorldSync systems to be identified and authenticated prior to the use of any system resources. 1WorldSync distinguishes access into corporate and commercial access.

1Worldsync maintains policies and procedures to ensure that newly hired and transferred employees or contractors are educated on their role within the company, the company culture, and their information security responsibilities. The employee is provided with access to assets in accordance with their job responsibilities on a least privileged basis.

The Human Resources (HR) department utilizes a set of cloud-based platforms for the hiring process. Job descriptions are posted and all job posting undergo an approval process that includes analysis of compensation for comparable positions for the location. Processing the applicants through the steps to become an employee is completed via a purpose build cloud-based platform.

All steps for onboarding an employee have workflow built into the employee management system that notify appropriate personnel of the steps needed to prepare for the employee. Background checks, signing of 1WorldSync non-disclosure policy are required before an employee can start. Processes are in place to ensure that a new employee is given sufficient orientation to become productive in a timely manner.

Offboarding checklists are maintained by HR in a cloud-based system that has specific completion steps by the various teams to ensure access is removed and equipment is returned.

All employees and certain contractors get some level of corporate systems access depending on their job role. That access is governed by the onboarding process. The principal access initially granted to the employee is a 1WorldSync Google Workspace account. User account requirements in Google Workspace include use of strong passwords with defined minimum characters and a multi-factor authentication requirement. That account credential is then used as the primary single sign on credential for most other corporate platform tools that a user may access in their job function.

Commercial systems access is limited via a least privilege model based on role-based access control processes. Commercial systems access is in two forms. Access to the IMCM applications front end, i.e., access the IMCM offering as a user of that system, and access to the IMCM applications back end, i.e., access to the IMCM offering as an administrator, developer, or product analyst.

Role-based access groups are defined that clearly determine the environments and privileges that a person in that role may get. Individualized access is not permitted. A defined onboarding process exists for obtaining inclusion in one of these groups and the responsible manager must request that access be granted to the individual before it is granted.

Role-based access groups are reviewed quarterly and the configuration of all servers and systems associated are reviewed quarterly to ensure access corresponds to the policy.

Employees accessing the IMCM system from outside the 1WorldSync network are required to use a virtual private network (VPN). VPN authentication is tied to the employees Google Workspace or AD account via single sign-on (SSO) and requires multi factor access to connect.

Customers access the IMCM system via web-based https, API, or AS2 based connection.

Customers can manage the access of their staff using the User Management system incorporated into IMCM. Passwords must conform to password configuration requirements configured in the user management system. Federation to the customers user management system can be provisioned on request.

Computer Operations - Backups

1WorldSync uses cloud-based platform services to provide the systems and tools used to operate. Employees can access and utilize these tools securely from remote locations. 1WorldSync is fully able to operate from remote locations and is not reliant on any office location or in house system to complete its business objectives. Vendors of these services are reviewed annually to ensure they have adequate systems in place to ensure the restorability of the platform and its data.

All IMCM systems are recoverable in the event of application failures, data corruption, data loss or disasters.

The recovery methodology used is dependent on the system, where it is hosted, and the underlying technologies that are available for the specific system, data, or asset. The methodologies include local and remote snapshots, replication, and use various backup models. Core recovery procedures utilize a multiple solution approach that provides local and remote recovery options from the loss of and or corruption of data. All technologies used are monitored to ensure they are operational, and any issues are investigated and resolved by administrative personnel.

All data is moved via private point to point networks links between geographically disparate 1WorldSync datacenters and is not stored offsite.

Successful disaster recovery tests are completed at least bi-annually. The success of a disaster recovery is measured by confirming full functionality of IMCM applications in the remote disaster recovery (DR) datacenter within the recovery time objective (RTO) and recovery point objective (RPO) requirements. The RTO requirement is less than 4 hours and the RPO requirement is less than 15 minutes.

Computer Operations - Availability

1WorldSync's IMCM systems are maintained in colocation and cloud data centers facilities that ensure the high availability of space, cooling, power used by 1WorldSync systems. Component systems within those data center locations have high availability purpose built into their design. Networking components and connections that move data are all redundant end to end. Systems are clustered and utilize high availability technologies.

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

1WorldSync monitors the capacity utilization of physical and computing infrastructure of the IMCM systems to ensure that service delivery matches service level agreements. 1WorldSync evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center rack space, power, and cooling
- Disk storage
- Computing capacity
- Network bandwidth

1WorldSync has implemented a patch management process to ensure IMCM systems and 1WorldSync corporate end point devices are patched in accordance with vendor recommended operating system patches.

1WorldSync Technology Operations security personnel utilize a suite of tools to identify, assess, and remediate vulnerabilities applicable to organization's information assets.

1WorldSync completes daily scans of end point devices. Web application security scans are completed daily and scanning of new releases of components of the IMCM system is required for any release as part of the SDLC process.

1WorldSync maintains a web application firewall on its in-scope production applications. The web application firewalls are configured to protect against and block attacks before they reach the systems.

1WorldSync completes third-party penetration tests at least annually and these reports are reviewed by the Security team to address any vulnerabilities that are identified.

Reporting procedures are documented for any vulnerability that employees think may exist and they are made aware of their responsibilities via training and the employee security policy that they must acknowledge annually. The security team personnel are required to investigate any issues reported.

The in-scope system and supporting infrastructure is hosted by Cyxtera. As such, Cyxtera is responsible for the environmental security controls for the in-scope system. Refer to the "Subservice Organizations" section below for controls managed by the subservice organization.

Change Control

1WorldSync maintains documented SDLC policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing results are documented and maintained with the associated change request. Development and testing are performed in an environment that is physically and logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

1WorldSync has implemented a patch management process to ensure all infrastructure systems are patched in accordance with vendor recommended operating system patches. Patching of all systems proceeds through the same change control process and the change is introduced in the development environment and proceeds to other environments accordingly.

Data Communications

Firewall systems are in place in all offices and IMCM data centers to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. 1WorldSync firewalls utilize intrusion detection system (IDS) and intrusion prevention system (IPS) technologies to detect and prevent intrusion. That data is logged and reviewed by security team personnel for any events of note.

Office locations do not host have any services on the internal local area networks (LANs) that need to be reached from outside of the 1WorldSync LAN. Trusted and Guest networks are maintained in all office locations and data is segregated via virtual local area networks (VLANs).

IMCM colocation data centers utilize a demilitarized zone (DMZ) model where any component system subject to untrusted connectivity sits in a DMZ and is safeguarded by Firewall with IDS / IPS.

All network equipment is protected from unauthorized access, hardened and redundant. Network security controls include the following:

- Oversight and approval for all network architecture implementation decisions. Network architecture requirements are documented and reviewed annually
- Redundant components and communications paths
- Allowable network protocols are defined
- Review and approval for any network port presented
- Administrative services are protected, and access is controlled and logged
- Multi-factor authentication (MFA) required for components and services
- Full segregation between networks / environments

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. If a primary system fails, the redundant hardware is configured to take its place.

Third-party penetration testing is conducted at least annually to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible.

1WorldSync uses cloud-based scanning technologies and utilizes third-party vulnerability scanning in combination. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on at least a quarterly basis.

Boundaries of the System

The scope of this report includes the Item Management, Product Introduction, Digital Asset, User Management, Communications Hub, Data Sync Direct PIM, IM Integration Gateway, and Product Bundles Services System performed in the Elk Grove Village, Illinois; Piscataway, New Jersey; Ashburn, Virginia, Council Bluffs, Iowa, Dublin, Ireland, St. Ghislain Belgium.

This report does not include the data center hosting services provided by Cyxtera at the regional facilities.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to u user entities in the 12 months preceding the end of the review period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common / Security, Availability, and Confidentiality criteria were applicable to the 1WorldSync Item Management, Product Introduction, Digital Asset, User Management, Communications Hub, Data Sync Direct PIM, IM Integration Gateway, and Product Bundles Services System.

Subservice Organizations

This report does not include the data center hosting services provided by Cyxtera at the regional facilities.

Subservice Description of Services

Cyxtera provides data center hosting services, which includes implementing physical security controls for the housed in-scope systems. Controls include but are not limited to requiring visitor sign ins, requiring badges for authorized personnel, and monitoring and logging of physical access to the facilities.

Complementary Subservice Organization Controls

1WorldSync's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all the trust services criteria related to 1WorldSync's services to be solely achieved by 1WorldSync control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of 1WorldSync.

The following subservice organization controls have been implemented by Cyxtera included in this report to provide additional assurance that the trust services criteria are met:

Subservice Organization - Cyxtera		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Physical security policies and procedures are in place to guide personnel in the following areas: Data center access for employees, contractors, and visitors; security monitoring; security assessments and access activity review.
		Security access controls are utilized to protect areas that contain information and information processing facilities.
		Control mechanisms are in place to limit physical access to restricted data center areas such as the raised floor equipment rooms, transport areas and critical power and mechanical infrastructure.
		Data center badge access requests for Company employees and contractors require a completed badge access request approved by site authorizers.
		Data center security personnel undergo a certification process upon hire and annually thereafter to maintain awareness and help ensure adherence to current physical security policies and procedures.
		Data center access for Company personnel is revoked as a component of the employee termination process.
		Visitor logs are maintained for at least 90 days to document visitor activity to the data centers.
		Visitors are required to be escorted by an authorized Company employee or authorized customer representative at all times while in the data center.
		Persons entering the data centers must present valid government-issues photo ID or display and use a valid Company photo access badge prior to entering the facility.
		CCTV surveillance video and/or ACS activity logs are retained for a minimum of 90 calendar days.
		Data center security personnel and the PSCC monitor access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.

Subservice Organization - Cyxtera		
Category	**Criteria**	**Control**
		An inventory of access badge and metal keys designated for loan to employees, customers, or contractors, as applicable by locations, is performed at least once per day to account for all badge and keys.
		Badge access reviews are performed annually to help ensure that access to the data center facilities is restricted to authorized personnel.
		Data center security personnel and the PSCC monitor access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.
Availability	A1.2	Environmental security policies and procedures are in place to guide personnel in the following areas: Equipment specifications and operating instructions; equipment specifications and operating instructions; preventative maintenance schedules (internal and external maintenance activities).
		A BMS is configured to monitor data center equipment including, but not limited to, the following: Fire detections and suppression systems, as applicable; HVAC units; generators, as applicable; electrical systems, as applicable.
		The BMS is configured to notify data center staff via on-screen and e-mail alerts when predefined thresholds are exceeded on monitored devices.
		Power management equipment is in place at each data center.
		Third-part specialists inspect power management systems according to a predefined maintenance schedule.
		Fire detection and suppression equipment is in place at each data center.
		Third-party specialists inspect fire detection and suppression systems on an annual basis.
		HVAC systems are in place at each data center.
		Third-party specialists inspect HVAC systems and water detection sensors, as applicable, according to a predefined maintenance schedule.
		The GRC team performs remote reviews of the data centers based on threat vulnerability risk assessment on an annual basis to ensure physical and environmental security policies and procedures are followed, finding of noncompliance are reported to data center security personnel or facility management personnel for remediation.

1WorldSync management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, 1WorldSync performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by the subservice organization.
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization.

COMPLEMENTARY USER ENTITY CONTROLS

1WorldSync's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to 1WorldSync's services to be solely achieved by 1WorldSync control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of 1WorldSync's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to 1WorldSync.
2. User entities are responsible for notifying 1WorldSync of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of 1WorldSync services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize 1WorldSync services.
6. User entities are responsible for providing 1WorldSync with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying 1WorldSync of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.