

ITHAKA

# SOC 3 Report

ITHAKA

August 16, 2023 to November 15, 2023

An Independent Service Auditor's Report on Controls Relevant to Security



**AUDIT AND ATTESTATION BY**

**PRESCIENT  
ASSURANCE**

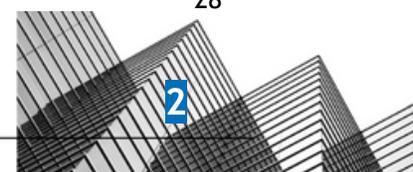


Prescient Assurance LLC.  
1100 Market Street Suite 600  
Chattanooga, TN 37402

[www.prescientassurance.com](http://www.prescientassurance.com)  
[info@prescientassurance.com](mailto:info@prescientassurance.com)  
+1 646 209 7319

## Table of Contents

|  |           |
|--|-----------|
| <b>Management's Assertion</b>  | <b>5</b>  |
| <b>Independent Service Auditor's Report</b>  | <b>8</b>  |
| Scope  | 8         |
| Service Organization's Responsibilities  | 8         |
| Service Auditor's Responsibilities   | 9         |
| Inherent Limitations   | 9         |
| Opinion  | 10        |
| Restricted Use   | 10        |
| <b>System Description</b>  | <b>12</b> |
| DC 1: Company Overview and Types of Products and Services Provided   | 13        |
| DC 2: The Principal Service Commitments and System Requirements  | 15        |
| DC 3: The Components of the System Used to Provide the Services  | 16        |
| 3.1 On-Premises Infrastructure   | 16        |
| 3.2 Cloud Infrastructure   | 18        |
| 3.3 Software   | 19        |
| 3.4 People   | 20        |
| 3.5 Data   | 21        |
| 3.6 Processes and Procedures   | 22        |
| 3.6.1 Physical Security  | 22        |
| 3.6.2 Logical Access   | 23        |
| 3.6.3 Computer Operations - Backups  | 23        |
| 3.6.4 Computer Operations - Availability   | 23        |
| 3.6.5 Change Management  | 23        |
| 3.6.6 Data Communications  | 24        |
| 3.7 Boundaries of the System   | 24        |
| DC 4: Disclosures About Identified Security Incidents  | 25        |
| DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved | 25        |
| 5.1 Integrity and Ethical Values   | 25        |
| 5.2 Commitment to Competence   | 26        |
| 5.3 Management's Philosophy and Operating Style  | 26        |
| 5.4 Organizational Structure and Assignment of Authority and Responsibility  | 26        |
| 5.5 HR Policies and Practices  | 27        |
| 5.6 Risk Assessment Process  | 27        |
| 5.7 Integration with Risk Assessment   | 27        |
| 5.8 Information and Communication Systems  | 28        |
| 5.9 Monitoring Controls  | 28        |
| 5.9.1 On-Going Monitoring  | 28        |



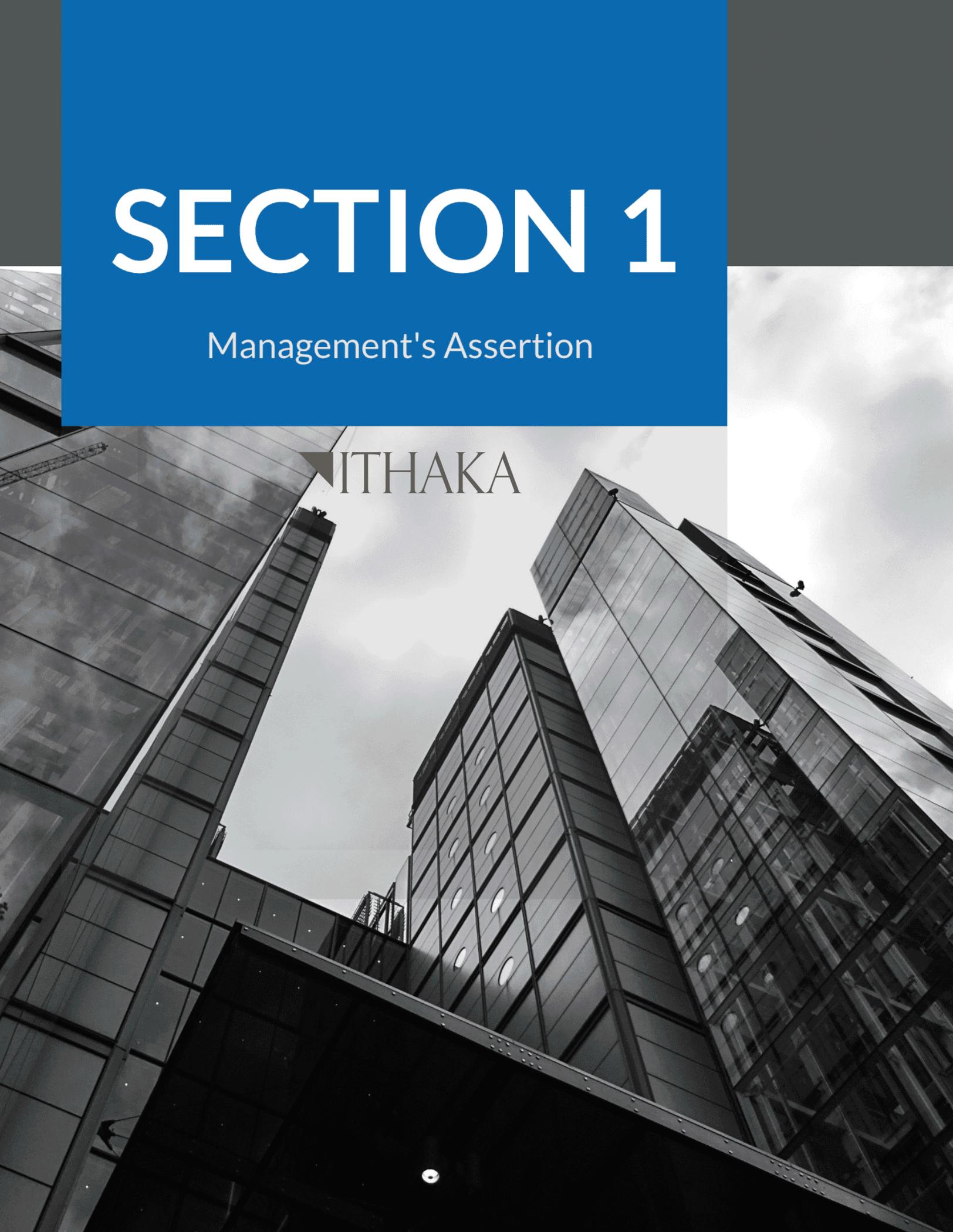
|  |           |
|--|-----------|
| 5.10 Reporting Deficiencies  | 28        |
| DC 6: Complementary User Entity Controls (CUECs)   | 29        |
| DC 7: Complementary Subservice Organization Controls (CSOCs)   | 30        |
| DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant | 31        |
| DC 9: Disclosures of Significant Changes in Last 1 Year  | 31        |
| <b>Testing Matrices</b>  | <b>32</b> |
| Tests of Operating Effectiveness and Results of Tests  | 33        |
| Scope of Testing   | 33        |
| Types of Tests Generally Performed   | 33        |
| General Sampling Methodology   | 34        |
| Reliability of Information Provided by the Service Organization  | 35        |
| Test Results   | 35        |



# SECTION 1

Management's Assertion

ITHAKA



## Management's Assertion

We have prepared the accompanying description of ITHAKA's system throughout the period August 16, 2023 to November 15, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 3® Report. The description is intended to provide report users with information about ITHAKA's system that may be useful when assessing the risks arising from interactions with ITHAKA's system, particularly information about system controls that ITHAKA 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 set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

ITHAKA uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ITHAKA, to achieve ITHAKA's service commitments and system requirements based on the applicable trust services criteria. The description presents ITHAKA's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ITHAKA'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, along with controls at ITHAKA, to achieve ITHAKA's service commitments and system requirements based on the applicable trust services criteria. The description presents ITHAKA's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ITHAKA's controls.



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

- a. The description presents ITHAKA's system that was designed and implemented throughout the period August 16, 2023 to November 15, 2023 in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period August 16, 2023 to November 15, 2023, to provide reasonable assurance that ITHAKA'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 organization and user entities applied the complementary controls assumed in the design of ITHAKA's controls during that period.
- c. The controls stated in the description operated effectively throughout the period August 16, 2023, to November 15, 2023, to provide reasonable assurance that ITHAKA's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of ITHAKA's controls operated effectively throughout the period.

DocuSigned by:

*Michelle Lee*

114Q75324DBF468.....

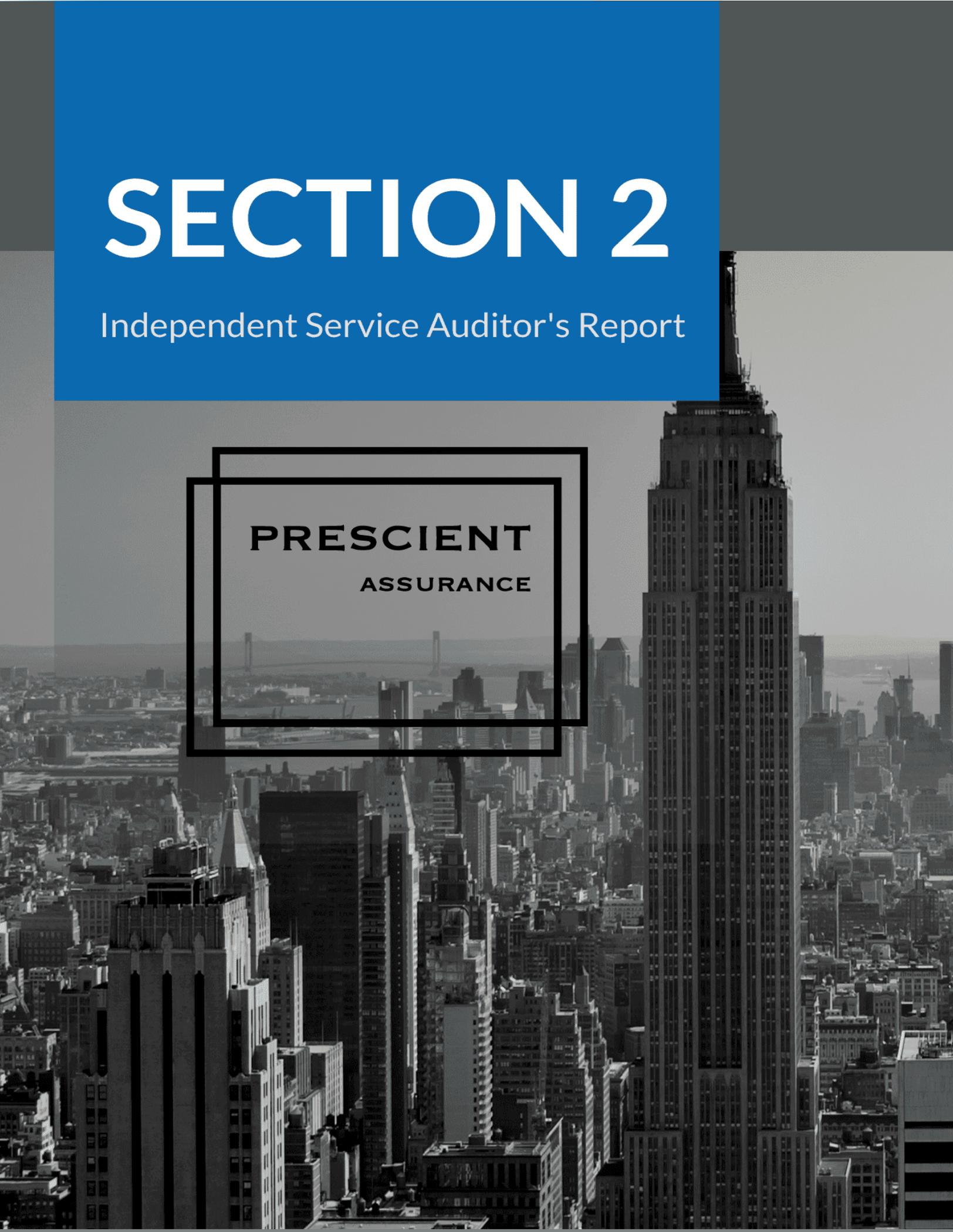
Michelle Lee  
CTO  
ITHAKA



# SECTION 2

Independent Service Auditor's Report

**PRESCIENT**  
**ASSURANCE**



## Independent Service Auditor's Report

To: ITHAKA

### Scope

We have examined ITHAKA's ("ITHAKA") accompanying description of its JSTOR, Arstor, Portico, and ITHAKA S+R system found in Section 3, titled ITHAKA System Description throughout the period August 16, 2023, to November 15, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 3® Report, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period August 16, 2023, to November 15, 2023, to provide reasonable assurance that ITHAKA's service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

ITHAKA uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ITHAKA, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents ITHAKA's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ITHAKA'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 certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at ITHAKA, to achieve ITHAKA's service commitments and system requirements based on the applicable trust services criteria. The description presents ITHAKA's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ITHAKA'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 complementary user entity controls.

### Service Organization's Responsibilities

ITHAKA 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 ITHAKA's service commitments and system requirements were achieved. In Section 1, ITHAKA has provided the accompanying assertion titled "Management's Assertion of ITHAKA" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. ITHAKA 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 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 the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
2. 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.
3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
4. 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.
5. 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.
6. 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 examination 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 report users may consider important to meet their informational needs. There are inherent limitations in 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 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

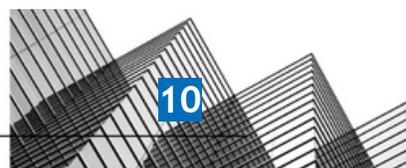
In our opinion, in all material respects:

- a. The description presents ITHAKA's system that was designed and implemented throughout the period August 16, 2023, to November 15, 2023, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period August 16, 2023, to November 15, 2023, to provide reasonable assurance that ITHAKA'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 organization and user entities applied the complementary controls assumed in the design of ITHAKA's controls throughout the period.
- c. The controls stated in the description operated effectively throughout the period August 16, 2023, to November 15, 2023, to provide reasonable assurance that ITHAKA'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 ITHAKA's controls operated effectively throughout the period.

## Restricted Use

This report is intended solely for the information and use of ITHAKA, user entities of ITHAKA's system during some or all of the period August 16, 2023 to November 15, 2023, business partners of ITHAKA subject to risks arising from interactions with the 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:

1. The nature of the service provided by the service organization.
2. How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
3. Internal control and its limitations.
4. 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.
5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. 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.

Prescient Assurance LLC

DocuSigned by:  
*John D Wallace*  
F5ADFA3569EA450.....

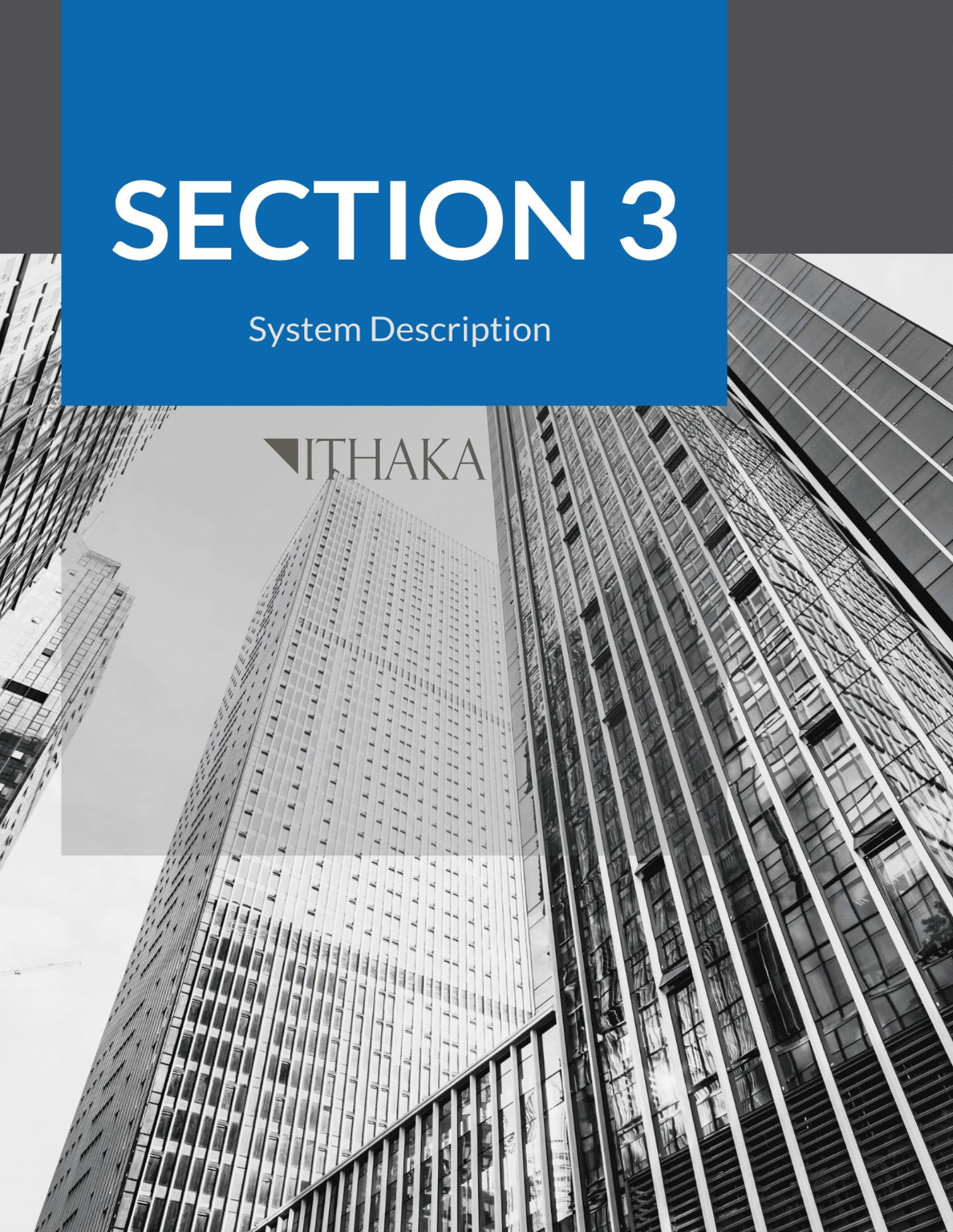
John D. Wallace, CPA  
Chattanooga, TN  
January 9, 2024



# SECTION 3

System Description

 ITHAKA



## DC 1: Company Overview and Types of Products and Services Provided

### Company Background

Ithaka Harbors, Inc. d/b/a ITHAKA is a nonprofit with a mission to improve access to knowledge and education for people around the world. We believe education is key to the well-being of individuals and society, and we work to make it more effective and affordable.

We help make higher education and access to knowledge more affordable; we improve outcomes for students and researchers; and we preserve knowledge for future generations.

### Description of services overview or services provided

JSTOR provides access to more than 12 million journal articles, books, images, and primary sources in 75 disciplines.

JSTOR helps you explore a wide range of scholarly content through a powerful research and teaching platform. We collaborate with the academic community to help libraries connect students and faculty to vital content while lowering costs and increasing shelf space, provide independent researchers with free and low-cost access to scholarship, and help publishers reach new audiences and preserve their content for future generations.

Artstor is the most extensive image resource for educational and scholarly use. We bring together more than 2 million images from top museums, archives, scholars, and artists – all rights-cleared for education and research – and provide tools for teaching and learning with visual materials.

Ithaka S+R helps academic and cultural communities serve the public good and navigate economic, technological, and demographic change. Our work aims to broaden access to quality postsecondary education, improve student outcomes, and advance research and knowledge.

Ithaka S+R's strategic advice and support services help institutions improve their performance and further their missions. We generate action-oriented research for institutional decision-making and act as a hub to promote and guide collaboration across the communities we serve. With our partners, we design and evaluate projects that make higher education, scholarly communication, and cultural collections more accessible to diverse populations.

ITHAKA's mission is to improve access to knowledge and education for people around the world. We believe education is key to the well-being of individuals and society. Through our work, we make higher education and access to knowledge more affordable, improve outcomes for students and researchers, and preserve knowledge for future generations. Our services include: JSTOR, Artstor, Portico, and Ithaka S+R.

JSTOR provides a platform for discovering and connecting research, images, and primary sources. We partner with libraries, museums, and publishers to reduce costs, extend access, and preserve



scholarship for the future. JSTOR includes content from over 2,000 organizations and serves 11,000+ universities, schools, and institutions in 176 nations.

Ithaka S+R provides collaborative strategies and research for higher education and the arts. We partner with foundations, consortia, and individual institutions to seek solutions and inform policies in a rapidly changing environment. We generate action-oriented research for institutional decision-making and act as a hub to promote and guide collaboration across the communities we serve. With our partners, we design and evaluate projects that make higher education, scholarly communication, and cultural collections more accessible to diverse populations. Our extensive, freely accessible library includes 200+ research reports and issue briefs, and 500+ blog posts.

The Artstor Digital Library ("ADL") is the most extensive online image resource for educational and scholarly use. We bring together media from top museums, archives, scholars, and artists, with a specialized suite of tools for teaching and learning with visual materials – all rights-cleared for education and research. ADL includes 2.5+ million high-quality images from 280+ contributors and serves nearly 2,000 universities, schools, and museums in 56 countries.

Portico is a community-supported preservation archive that safeguards access to e-journals, e-books, and digital collections. Portico's unique, trusted process ensures that the content will remain accessible and usable for researchers, scholars, and students in the future. Over 1,200 libraries support Portico to preserve content from over 1,000 publishers.

Constellate is a service for teaching, learning, and performing text analysis with scholarly and primary source content from JSTOR, Portico, and partners. It allows instructors to easily and confidently incorporate text analysis into their curricula.



## DC 2: The Principal Service Commitments and System Requirements

ITHAKA designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that ITHAKA makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that ITHAKA has established for the services. The system services are subject to the Security commitments established internally for its services.

ITHAKA's commitments to users are communicated through the Terms and Conditions of Use, Service Level Agreements (SLAs) or Master Service Agreements (MSAs), online Privacy Policy, and in the description of the service offering provided online.

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and annual penetration test over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal
- Providing security training and orientation to staff
- Up time availability of production systems



## DC 3: The Components of the System Used to Provide the Services

### 3.1 People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

ITHAKA has a staff of approximately 400 organized in the following functional areas:

**Management:** Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment. This includes:

- President - Kevin Guthrie
- General Counsel - Nancy Kopans
- COO - Nathalie Udo
- CFO & Treasurer - Arielle Ali
- VP, Product & Design - Matt MacQueen
- Co-CTO's - Michelle Lee and Dale Myers
- Outreach - Rebecca Seger
- Marketing - Harmony Faust

**Engineering:** engineering and product teams for the services ITHAKA provides (see "Description of services overview or services provided" above) are responsible for developing, maintaining, and operating the applications of those services, and the cloud and some on-premises infrastructure those applications run on. Responsible for testing, deployment, and maintenance of the source code of those systems.

**Information Technology Services (IT Services):** Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

**Information Technology Infrastructure (ITI):** Responsible for managing on-premises networking, including VPN access for remote employees and wi-fi in offices, provisioning and management of Unix systems, Windows systems and hardware, some Domain Name Service administration, and works jointly with Engineering on the communications to and from ITHAKA's AWS footprint. Members of the engineering team may also be members of the operations team.

**Product Development:** Responsible for the product development, design and research into users in support of product development and organizational goals. Responsible for the product life cycle, including adding additional product functionality.

**Outreach:** The Outreach & Participation Services (OPS) team is responsible for growing and maintaining library participation in JSTOR, Artstor and Portico worldwide. The team talks to current and potential participants on a daily basis about the JSTOR platform and Portico preservation services. The team

regularly exhibits at community conferences, hosts informational webinars, and visits school campuses. The main mission is to spread participation as broadly as possible.

**Marketing:** ITHAKA's Marketing team leads our organizational efforts to tell ITHAKA's story, history, and mission, and to create awareness, leads, and loyalty for our products and services.

**Financial Services** supports ITHAKA's mission by maintaining healthy fiscal operations. Financial Services supports budget management, invoicing, and staff reimbursements, and supports decision-making with financial reporting, analysis, and financial guidance and advice.

**Legal:** The Legal Team uses its expertise to enable ITHAKA and support its day-to-day and long-term needs in ways that are efficient, effective, and strategically-minded.

### 3.2 Processes and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

### 3.3 Boundaries of the System

The boundaries of the JSTOR, Artstor, Portico, and Ithaka S+R are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the JSTOR, Artstor, and Ithaka S+R.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.



## DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

### 5.1 Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of ITHAKA's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of ITHAKA's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

### 5.2 Commitment to Competence

ITHAKA's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.



### 5.3 Management's Philosophy and Operating Style

The ITHAKA management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way ITHAKA can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require ITHAKA to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with ITHAKA's core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

### 5.4 Organizational Structure and Assignment of Authority and Responsibility

ITHAKA's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

ITHAKA's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

### 5.5 HR Policies and Practices

ITHAKA's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at



maximum efficiency. ITHAKA's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation at the time of hire or engagement.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

## 5.6 Risk Assessment Process

ITHAKA's risk assessment process identifies and manages risks that could potentially affect ITHAKA's ability to provide reliable and secure services to our customers. As part of this process, ITHAKA maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular ITHAKA product development process so they can be dealt with predictably and iteratively.

ITHAKA presents a risk assessment report to its board of trustees (or an applicable committee of the Board) annually that includes information about privacy and security risks if relevant for that year.

## 5.7 Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of ITHAKA's system; as well as the nature of the components of the system result in risks that the criteria will not be met. ITHAKA addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, ITHAKA's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

## 5.8 Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

## DC 7: Complementary Subservice Organization Controls (CSOCs)

### Subservice Organizations

This report does not include the Cloud Hosting Services provided by cloud hosting providers at multiple facilities.

### Subservice Description of Services

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entities services.

### Complementary Subservice Organization Controls

ITHAKA'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 of the trust services criteria related to ITHAKA's services to be solely achieved by ITHAKA control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of ITHAKA.

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

| AWS      |          |   |
|----------|----------|---|
| Category | Criteria | Control   |
| Security | CC6.4    | Physical access to data centers is approved by an authorized individual.  |
| Security | CC6.4    | Physical access is revoked within 24 hours of the employee or vendor record being deactivated.  |
| Security | CC6.4    | Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.  |
| Security | CC6.4    | Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations. |
| Security | CC6.4    | Access to server locations is managed by electronic access control devices.   |

ITHAKA's management, along with the subservice provider, 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, ITHAKA performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

## DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant

All Common Criteria/Security, Security criteria were applicable to the ITHAKA's JSTOR, Artstor, Portico, and Ithaka S+R system.

