iFOLIO®

REPORT ON iFOLIO LLC’S DESCRIPTION OF DIGITAL ENGAGEMENT PLATFORM SYSTEM AND ON THE SUITABILITY OF THE DESIGN OF ITS CONTROLS RELEVANT TO SECURITY AS OF SEPTEMBER 15, 2021

Pursuant to Reporting on System and Organization Controls 2 (SOC 2) Type 1 examination performed under AT-C 205

HA&C HANCOCK ASKEW & CO LLP
ACCOUNTANTS & ADVISORS

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: iFOLIO, LLC

Scope

We have examined iFOLIO, LLC's (iFOLIO or the Company) accompanying description of its Digital Engagement Platform System found in Section 3 titled "iFOLIO, LLC's Description of its Digital Engagement Platform System" as of September 15, 2021 (description) 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 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of September 15, 2021, to provide reasonable assurance that iFOLIO'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 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

iFOLIO 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 iFOLIO's service commitments and system requirements were achieved. In Section 2, iFOLIO has provided the accompanying assertion titled "Assertion of iFOLIO, LLC Management" (assertion) about the description and the suitability of design of controls stated therein. iFOLIO 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 of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed 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 of controls involves:

- 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.
- 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.
- evaluating the overall presentation of the description.

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

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 informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects:

a. the description presents iFOLIO, LLC’s Digital Engagement Platform System that was designed and implemented as of September 15, 2021, in accordance with the description criteria.

b. the controls stated in the description were suitably designed as of September 15, 2021, to provide reasonable assurance that iFOLIO, LLC’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of iFOLIO, LLC’s controls as of that date.

Restricted Use

This report is intended solely for the information and use of iFOLIO, LLC.; user entities of iFOLIO, LLC's Digital Engagement Platform System as of September 15, 2021; business partners of iFOLIO, LLC subject to risks arising from interactions with the Digital Engagement Platform 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.

Hancock Askew & Co., LLP

Peachtree Corners, Georgia
October 15, 2021

SECTION 2

ASSERTION OF IFOLIO, LLC MANAGEMENT

ASSERTION OF IFOLIO, LLC MANAGEMENT

October 15, 2021

We have prepared the accompanying description of iFOLIO's Digital Engagement Platform System titled iFOLIO, LLC's Description of its Digital Engagement Platform System as of September 15, 2021 (description) 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 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the Digital Engagement Platform System that may be useful when assessing the risks arising from interactions with of iFOLIO's system, particularly information about system controls that of iFOLIO 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 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

iFOLIO uses AWS, a subservice organization, to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at iFOLIO, to achieve iFOLIO's service commitments and system requirements based on the applicable trust services criteria. The description presents iFOLIO's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of iFOLIO's controls. The description does not disclose the actual controls at the subservice organization.

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

1) The description presents iFOLIO's Digital Engagement Platform System that was designed and implemented as of September 15, 2021 in accordance with the description criteria.

2) The controls stated in the description were suitably designed as of September 15, 2021 to provide reasonable assurance that iFOLIO's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of iFOLIO's controls.

/s/ Hap Richardson
Hap Richardson
Chief Financial Officer
iFOLIO, LLC

SECTION 3

IFOLIO, LLC'S DESCRIPTION OF ITS DIGITAL ENGAGEMENT PLATFORM SYSTEM AS OF SEPTEMBER 15, 2021

OVERVIEW OF OPERATIONS

Company Background

iFOLIO was founded in 2016 to help enterprises, students, and athletes connect, engage, and convert with digital storytelling. The organization is based in Atlanta, GA with team members contributing all over the world.

iFOLIO is WBENC certified and has received the following awards and honors:

- *50 On Fire Award: Inno & Atlanta Business Chronicle (2021)*
- *Ava Digital Award, Silver Winner (2021)*
- *Ava Digital Award, Gold Winner (2021)*
- *Hashtag Sports Award Finalist, 2020*
- *Hashtag Sports Award Finalist, 2021*
- *Top 10 Artificial Intelligence Solution Providers, Education Technology Insights, 2018*

Industries served by IFOLIO include Financial Services, Higher Education, Legal Services, Corporate Sales Teams, High Achieving Students, and others who want to provide an innovative digital experience.

Description of Services Provided

iFOLIO is a digital marketing platform designed to help companies grow and make work easier. The cloud-based SaaS platform has patented technology and is hosted by Amazon Web Services. Services and features of the platform include customizable landing pages with custom URLs, private digital presentations, text message campaigns, email marketing, QR codes, html embeds, digital business cards all with the patented analytics.

Digital engagement is more important than ever as the digital transformation continues. iFOLIO released version 2.0, the iFOLIO Cloud Platform, in early 2021. The original platform still exists with over 10,000 users and the Cloud platform provides exciting enhancements. In May 2021, The US Patent and Trademark Office awarded iFOLIO a patent on analytics to help clients measure web engagement. Patent No. US 10,996,033 B2. iFOLIO platform has over 300 million seconds of engagement.

Principal Service Commitments and System Requirements

Client's trust is iFOLIO's top priority. The Company delivers technical solutions to active users in over 50 countries, by working with large enterprises, educational institutions, and professional sports teams. iFOLIO uses Hypertext Transfer Protocol Secure (HTTPS) + Transport Layer Security (TLS) to encrypt the transported data. Security is achieved by data transfer encryption, multilevel access control, users' actions audit, automated logs monitoring with multiple triggers alerting iFOLIO support about any suspicious events

Components of the System

iFOLIO is a cloud based SAAS digital marketing platform using the following technologies. They have segregated the backend and front-end environments which makes complete iFOLIO functionality available for 3rd party integrations.

Frontend Technologies:

- Framework: React
- State manager: redux (redux-toolkit)
- Routing: react-router-dom
- Building: webpack (webpack-dev-server) + libraries for copying and cleaning of build folder
- Transpiler: babel + dynamic import, optional chaining
- Code Analysis: eslint
- Code formatting: prettier
- Async queries: axios (http client which uses Promises)
- Dates management: dayjs
- Tooltips: rc-tooltip
- Components styling: styled-components
- react-hooks

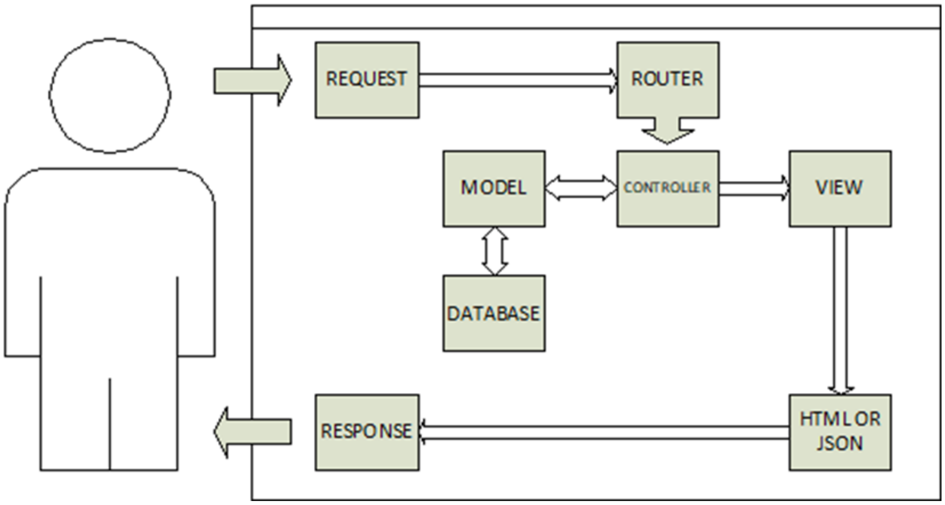
Frontend Codebase structure

- assets – static files
- components - reusable components
- config - constants, config file for base urls and api methods
- hooks – custom hooks
- icons - icons storage
- modules - reusable blocks
- pages – site pages
- reducers – redux reducers
- routes – routing map
- store – redux store configuration
- styles – scss styles (used only for fonts usage, since the only limitation of styled-components is fonts caching)

Layout Manager + Widgets

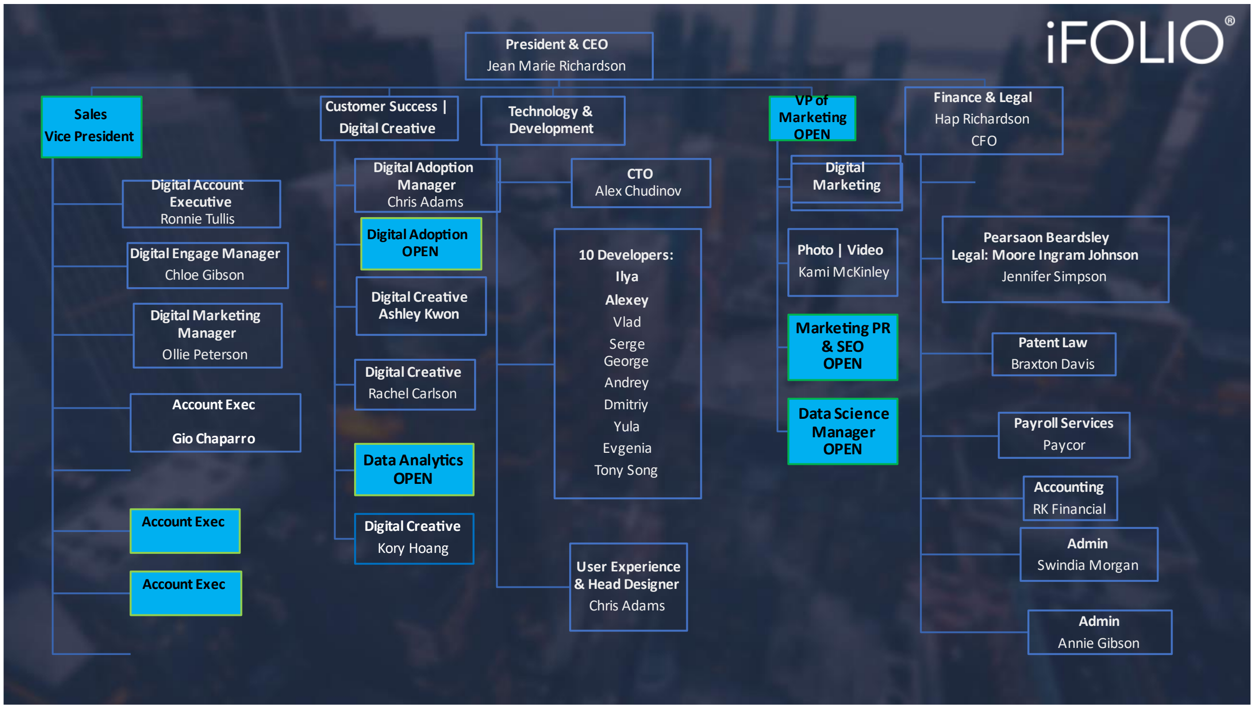
Instead of implementing dozens of components for every possible layout the Company uses a universal approach with Layout Manager which generates any layout with placeholders based on JSON config and then specific widgets are inserted in placeholders.

Layout Manager configuration workflow is presented below.



People

IFOLIO's organizational structure consists of five departments: Development, Design, Sales, Marketing, and Legal. The following org chart represents the team as of October 2021. The team is constantly evolving, and management reviews this chart on a monthly basis.



- Development: There are multiple teams of software engineers working on the iFOLIO platform. They are responsible for new product features, system maintenance and bug fixes. The front end and back-end environments are completely segregated so new product development is performed in a production environment using dummy data before going live. The CTO is responsible for all bug fixes and reviews all updates before they are live.
- Design: A team of graphic designers and front-end developers work on the iFOLIO platform. They are client facing, working with existing users so that they are aware of the capabilities of iFOLIO as well as new features. They perform a roll out session with each new client consisting of a video conference or on sight meeting so that each user is set up in the iFOLIO platform.
- Sales & Marketing: The software sales team works to connect, engage, and convert with new clients. They use an omni channel approach incorporating social media, zoom demonstrations, conference sponsorships and more to reach as many prospects as possible.
- Legal: iFOLIO has in-house counsel responsible for all HR issues, tax preparation and data privacy.

Data

iFOLIO uses Hypertext Transfer Protocol Secure (https) + Transport Layer Security (TLS) to encrypt the transported data. Security is achieved by data transfer encryption, multilevel access control, users' actions audit, automated logs monitoring with multiple triggers altering iFOLIO about any suspicious activity.

iFOLIO ensures for responsible account management with the following:

- Audit logs that record user's events and track changes during sessions
- Role based access control (RBAC) that can assign permissions to authorized users and restrict control for unauthorized users to edit templates or view information
- Single Sign On (SSO) allowing the user to log in once and access services without re-entering authentication factors
- Single Log Out (SLO) so that a single action of signing out terminates access to all active user sessions to secure the account.

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 iFOLIO policies and procedures that define how services are delivered. These are located on the Company's intranet and can be accessed by any iFOLIO team member.

Physical Security

iFOLIO facility is protected by external locked doors and is monitored by security cameras to detect potential security threats. The facility has a designated reception area which is attended by either a receptionist or a security guard 24 hours per day. Access to the reception area is unlocked from 8am to 5pm on business days and is locked at all other times. Upon arrival, a visitor will make their way to the reception area, where the guard or receptionist will confirm that they are an expected guest/visitor by requesting their full name and respective organization. Upon confirmation, the guest is allotted a guest access card used to access the elevators. Access beyond the reception area is controlled through the access card system.

Visitors check in with the receptionist or security guard stationed in the reception area. Visitors must present a valid, government-issued photo ID. The visitor's name, employer, and purpose for visit are recorded in a visitor log and his or her visit must be approved by an iFOLIO employee who is authorized to sign non-employees into the facility. The visitor is issued a temporary ID badge to be worn throughout his or her visit. This temporary badge does not permit users access through any secured doors within the facility.

Upon exit, the badge/name tag is collected and the hr/min/sec timestamp for visitor exit is captured. Visitor logs are stored for at least 90 days via securely stored paper or digital records. Visitors that are unescorted do not have the ability to logically access restricted areas unless pre-authorization has been given by the approving manager. Visitors receive a temporary badge or name tag - badge/name tag is marked in a way that identifies them as a visitor. Any non-escorted or unauthorized visitors should be reported to the security team immediately.

A team manager must review, audit, and document user accounts and associated privileges of at least high-risk and critical vendors at least quarterly to ensure that access is restricted appropriately.

Logical Access

This Information Security Policy addresses the basic information security policy topics which maintain the security and confidentiality of iFOLIO applications, systems, infrastructure, and data. At least annually, iFOLIO updates this policy and implements different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to iFOLIO including compliance with applicable laws and regulations.

This policy applies to iFOLIO assets utilized by personnel acting on behalf of iFOLIO or accessing its applications, infrastructure, systems, or data. All personnel are required to read, accept, and follow iFOLIO policies and plans upon starting and at least annually.

iFOLIO adheres to the principle of least privilege access, specifying that team members are given access to only the information and resources necessary to perform their job functions as determined by management or a designee. Requests for escalation of or changes to privilege and access are documented and require approval by an authorized manager. System access is revoked upon termination or resignation.

Audits of access and privileges to sensitive iFOLIO applications, infrastructure, systems, and data are performed and reviewed by authorized personnel on a quarterly basis.

Unique accounts and passwords are required for all users. Passwords are kept confidential and not shared with multiple users. Where possible, all user and system accounts have a minimum of eight characters including alpha (upper and lower case), one numeric and one non-alphanumeric character. Accounts use unique passwords not used elsewhere.

If a password is suspected to be compromised, the password is rotated immediately, and the security team is immediately notified.

Passwords are only stored using an iFOLIO approved password manager. iFOLIO does not hard code passwords or embed credentials in static code.

iFOLIO maintains a Configuration and Asset Management Policy designed to track and set standard configurations to protect iFOLIO devices, networks, systems, and data. In compliance with such policy, iFOLIO provides team members laptops or other devices to perform their job duties effectively.

iFOLIO inventories and tracks assets that are used to view or store confidential information. The asset inventory will include systems connected to the network and network devices themselves. Examples of items to be inventoried could be laptops, desktops, and servers.

Assets such as smaller peripheral devices, video cards, keyboards, or mice may not be tracked. Assets that store data are tracked either as part of a computing device or as a part of network-attached storage.

Prior to the acquisition of any unapproved hardware, software, or other equipment and during transitions to new systems or following a failure or disaster, information security, capacity planning, and other relevant business considerations are addressed. iFOLIO management approves any new assets that may be used to access iFOLIO data, systems, network, or applications.

Confidential data is also considered an asset and are tracked accordingly. Confidential data is stored in accordance with security policies and the location of all covered data regardless of classification or encryption status must be maintained.

- iFOLIO maintains an inventory of servers, desktops, laptops, and other devices used to store, create, modify, delete, or transmit confidential information.
- Assets are mapped to the device’s serial number or another identifier.
- Assets no longer in use or deemed no longer usable are removed from the inventory.
- iFOLIO performs annual asset management system checks for various classes of asset records.
- iFOLIO devices issued to team members are returned upon termination or resignation of such team members.

The CFO or designee are held accountable for the accuracy of the inventory and audit the asset list at least annually. The review is retained as evidence of completion.

Production systems handling confidential data include documented baseline configurations, when available. iFOLIO management is responsible for creating and implementing documented standard configurations for all applicable assets including third-party cloud products and employee devices.

Each applicable asset and system in the iFOLIO environment are hardened to the minimum standards defined by iFOLIO management.

Hardening standards are in line with industry standards and provide sufficient logical and physical security for the asset(s) being configured.

Users of iFOLIO systems and applications are provided with unique credentials (IDs, keys, etc.) that can be used to trace activities to the individual responsible for that account. Shared user accounts shall only be utilized in circumstances where there is a clear business benefit and when user functions do not need to be traced. Shared account passwords are only stored in an iFOLIO approved password manager.

Unique accounts and passwords are required for all users. Passwords are kept confidential and not shared with multiple users. Where possible, all user and system accounts have a minimum of eight characters including alpha (upper and lower case) and one numeric character. All accounts use unique passwords not used elsewhere.

If a password is suspected to be compromised, the password is rotated immediately, and the security team is immediately notified. Passwords are only to be stored using an iFOLIO approved password manager. iFOLIO does not hard code passwords or embed credentials in static code.

When available, multi-factor authentication is used. Multi-factor authentication is used for access to Company email/ticket, version control tool and cloud infrastructure.

In order to onboard new personnel, the following steps are taken and documented:

- iFOLIO devices provided to the new hire are inventoried in accordance with iFOLIO policy.
- A new hire email or ticket is sent to the appropriate team to inform them of new personnel.
- IT/Engineering and the new personnel's manager documents a checklist of accounts and permission levels needed for that hire.
- The applicable team sets up each user with the appropriate access.
- Onboarding processes are appropriately documented via ticketing or other document management tools.

In order to offboard an employee or contractor, the following steps are taken:

- An offboarding email or ticket is sent to IT/Engineering when personnel have been terminated or resigned informing them of the team members' last day.
- IT/Engineering goes through and documents the appropriate revocation checklist to revoke access to iFOLIO systems and applications within 24 hours of the last day with the company or sooner if necessary.
- iFOLIO devices provided are collected and accounted for in accordance with iFOLIO policy.
- Offboarding processes are appropriately documented via communication emails between IT and the appropriate manager.

Requests for changes to access level(s) such as in the case of a change in job duties, are documented and approved by the appropriate manager.

A documented request is sent to the appropriate department when an employee or contractor role changes to evaluate whether access privileges are changed, or when accounts are no longer required, and user access rights are reviewed and reallocated as necessary prior to changes being made. Such changes are tracked via email communication.

A team manager reviews, audits, and documents user accounts and associated privileges of at least high-risk and critical vendors quarterly to ensure that access is restricted appropriately.

Computer Operations – Backups

Vital data that would be affected by disruption are maintained and controlled by the data's applicable teams.

In the event of a facility disruption, critical records located in such a facility may be destroyed or inaccessible. The number of critical records, which would have to be reconstructed, will depend on when the last transfer of critical records to the cloud storage location occurred.

- Database backups are typically performed weekly.
- Backups are typically retained for at least 30 days.
- The maximum allowable retention period is determined based on regulatory and contractual requirements.
- Backups are tested, at least annually, to ensure that backups are sufficient and reliable in accordance with this plan.
- Backup systems and media protect the availability of stored data.

iFOLIO utilizes and relies on mission critical third-party cloud services. In the event of a significant business disaster, iFOLIO will execute their business continuity plan and quickly work to attempt establishing alternate arrangements if a mission critical vendor can no longer provide the needed services or goods.

Mission critical third-party vendors include: AWS, Bitbucket and G-Suite

This plan depends on the likelihood that:

- Remote work can continue to take place in the event of a disaster; and
- Mission critical vendor services, and essential iFOLIO services, systems, and data can still be made available or alternative solutions can be implemented (including backups and services provided by such third-party vendors).

Computer Operations – Availability

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.

IFOLIO monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements. IFOLIO 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 space, power, and cooling
- Disk storage
- Network bandwidth
- Processing bandwidth

IFOLIO has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and IFOLIO system owners review proposed operating system patches to determine whether the patches are applied. Customers and IFOLIO systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. IFOLIO staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control
iFOLIO maintains documented Systems Development Life Cycle (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. All change requests are documented end-to-end via the iFOLIO change management and ticketing tools.

The iFOLIO product management team evaluates which change requests and features are implemented based on their alignment with the business plan and the overall level of effort required. Change requests are prioritized in terms of benefits, urgency, effort required, security impacts, and other potential impacts on the organization's operations.

A ticket is created to track a change request at the onset. If the change is part of an existing ticket the original ticket may be used and modified appropriately.

Planning and evaluating the change. This stage may include design, scheduling, and implementation of a communications plan, testing plan, and roll-back plan. During planning, wireframes, mockups, and functional requirements are created and reviewed among the applicable team members. The team may set priority levels of the service and may determine any risk that the proposed change introduces to the system.

The scope and impact of the change, specific use cases, user interface and user experience (UI/UX) and other optimizations typically occur to enhance the performance and security of the change across all platforms. The changes are tested in the iFOLIO staging environment before release to production. Test setups and scenarios are built for operational, performance, and security testing. Automated test scripts are developed, used, and updated as changes occur.

The appropriate teams work to create documentation such as release notes, help articles, and blog posts applicable to the changes. Existing documentation is updated to ensure that team members and customers have the most up-to-date and accurate information. Customer-facing documentation is provided to iFOLIO customers as required.

iFOLIO uses code reviews to maintain the quality of iFOLIO code and products. Code reviewers verify: design, functionality, complexity, tests, security, naming, comments, style, documentation, and code sourcing.

Secure coding practices are incorporated into the development lifecycle and security architecture of iFOLIO. Engineers at iFOLIO are responsible for defining security requirements early in the software development life cycle and then evaluating for compliance with those requirements. Engineers at iFOLIO are responsible for reviewing the OWASP top 10 web application security risks.

Once the new release is ready and the appropriate documentation is in place, the new release may be pushed to the production environment after the appropriate review and approval by the appropriate product owner. Automation test suites are used across all production environments.

Access to push changes to production at iFOLIO is restricted to a limited set of authorized team members and the engineers responsible for coding the changes are not responsible for pushing the changes to production, unless approved by management. Implemented changes are communicated to applicable team members and externally as appropriate.

iFOLIO continuously measures the success of new releases and identifies areas that can be enhanced further in the future.

The appropriate team conducts a post-implementation review to determine how the change is impacting iFOLIO and their customers, either positively or negatively. Discuss and document lessons learned with product management and other appropriate team members.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

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. In the event that a primary system fails, the redundant hardware is configured to take its place.

Vulnerabilities are monitored on a real-time basis in accordance with IFOLIO policy. These technologies are customized to monitor the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated. If a vulnerability is identified, the Company will follow the documented incident management policy and procedures. Tools requiring installation in the IFOLIO system are implemented through the Change Management process.

Authorized employees may access the system from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system

Boundaries of the System

The scope of this report includes the Digital Engagement Platform System.

This report does not include the data center hosting services provided by Amazon Web Services.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

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 iFOLIO’s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of iFOLIO’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.
- Contractors are required to enter into an agreement which delineates their responsibilities.

Commitment to Competence

iFOLIO'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 particular 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.

Management's Philosophy and Operating Style

iFOLIO's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

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 as a whole.

Organizational Structure and Assignment of Authority and Responsibility

iFOLIO'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.

iFOLIO'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.

Human Resources Policies and Practices

iFOLIO'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. iFOLIO'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 on their first day of employment.
- 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.

Risk Assessment Process

This Risk Assessment Policy guides iFOLIO in performing risk assessments to account for threats, vulnerabilities, likelihood, and impact to iFOLIO assets, team members, customers, vendors, suppliers, and partners based upon the iFOLIO services considering security, availability, and confidentiality needs.

From time to time, iFOLIO updates this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to iFOLIO including applicable laws and regulations.

This policy applies to all iFOLIO assets utilized by personnel acting on behalf of iFOLIO or accessing its applications, infrastructure, systems, or data. All personnel are required to read, accept, and follow all iFOLIO policies and plans.

This process has identified risks resulting from the nature of the services provided by iFOLIO, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk – changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance – legal and regulatory changes

iFOLIO conducts assessments of risk, which include the likelihood and impact of harm from the unauthorized access, use, disclosure, disruption, modification and/or destruction of iFOLIO systems, applications, infrastructure, and the data processed, stored, or transmitted by such.

The risk assessment process is coordinated by the CFO, identification of threats and vulnerabilities is performed by asset owners, and assessment of consequences and likelihood is performed by the risk owner.

A risk assessment may include a review of:

- Internal controls including policies, procedures, and implemented security safeguards
- Human resource practices related to hiring, termination, and discipline procedures
- Facility controls
- Exposure to theft
- Systems and applications used to collect, store, process or transmit confidential data

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of iFOLIO's Platform to Secure the Digital Engagement Platform System; as well as the nature of the components of the system result in risks that the criteria will not be met. iFOLIO 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 are unique. As part of the design and operation of the system, iFOLIO management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication is an integral component of IFOLIO's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At IFOLIO, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Management lead company-wide meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate IFOLIO personnel via e-mail messages.

Specific information systems used to support IFOLIO's Digital Engagement Platform System are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. IFOLIO's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

IFOLIO's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in IFOLIO's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of IFOLIO's personnel.

Reporting Deficiencies

An internal 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. 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.

Changes to the System as of the Review Date

No significant changes have occurred to the services provided to user entities as of the review date.

Incidents as of the Review Date

No significant incidents have occurred to the services provided to user entities as of the review date.

Criteria Not Applicable to the System

Within the Common Criteria/Security CC6.5 is not applicable to the Digital Engagement Platform System as the data within a users' iFOLIO is based on information entered by the user. The user has the ability to add, modify and or remove the data; however, iFOLIO does not add, modify or remove a users' data on their behalf.

Subservice Organizations

This report does not include the cloud hosting services provided by Amazon Web Services.

Subservice Description of Services

AWS provides infrastructure cloud hosting services for iFOLIO's systems.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization – AWS		
Category	Criteria	Control
Common Criteria/Security	CC6.4, CC6.5	AWSCA-4.12: KMS-Specific – Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
		AWSCA-4.13: KMS-Specific – Access attempts to recover key materials are reviewed by authorized operators on a cadence defined in team processes.
		AWSCA-5.1: Physical access to data centers is approved by an authorized individual.
		AWSCA-5.2: Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		AWSCA-5.3: Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		AWSCA-5.4: Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		AWSCA-5.5: Physical access points to server locations are managed by electronic access control devices.
		AWSCA-5.6: Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

iFOLIO 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, iFOLIO performs monitoring of the subservice organization controls, including the following procedures:

- Holding discussions with vendors and subservice organization at least annually.
- Reviewing attestation reports over services provided by vendors and subservice organization.
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization.

COMPLEMENTARY USER ENTITY CONTROLS

iFOLIO’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 of the Trust Services Criteria related to iFOLIO’s services to be solely achieved by iFOLIO control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of iFOLIO’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 iFOLIO.
2. User entities are responsible for notifying iFOLIO of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of iFOLIO 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 iFOLIO services.
6. User entities are responsible for providing iFOLIO with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying iFOLIO of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security Category)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	iFolio has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance. In addition, personnel acknowledge the Code of Conduct promptly on hire. iFolio evaluates the performance of internal personnel through a formal, annual performance evaluation. Background checks are performed for new hires prior to the new hire's start date as permitted by local laws. Hiring managers screen new hires or internal transfers to assess their qualifications, experience, and competency to fulfill the job role and responsibilities. Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors taking into consideration segregation of duties as necessary at various levels of the organization and requirements relevant to security.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The board of directors or equivalent entity function includes senior management and external advisors, who are independent from the Company's operations. Senior management and BOD meet at least annually to review business objectives, company initiatives, resource needs, and risk management activities.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes the organizational chart for personnel. Management publishes the Acceptable Use policy to internal personnel. In addition, internal personnel acknowledge these procedures within 60 days of hire.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Management publishes the Data Classification Policy to internal personnel. In addition, internal personnel acknowledge these procedures within 60 days of hire. Management publishes the Information Security Policy to internal personnel. In addition, internal personnel acknowledge these procedures within 60 days of hire. Hiring managers screen new hires or internal transfers to assess their qualifications, experience, and competency to fulfill the job role and responsibilities. Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors taking into consideration segregation of duties as necessary at various levels of the organization and requirements relevant to security.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Background checks are performed for new hires prior to the new hire's start date as permitted by local laws. Hiring managers screen new hires or internal transfers to assess their qualifications, experience, and competency to fulfill the job role and responsibilities. iFolio has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance. In addition, personnel acknowledge the Code of Conduct promptly on hire. iFolio evaluates the performance of internal personnel through a formal, annual performance evaluation. Internal personnel complete annual training programs for information security to educate them of their obligations and responsibilities related to security and confidentiality. Management publishes the Acceptable Use policy to internal personnel. In addition, internal

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Environment		
CC1.0	**Criteria**	**Control Activity Specified by the Service Organization**
		personnel acknowledge these procedures within 60 days of hire. Management publishes the Data Classification Policy to internal personnel. In addition, internal personnel acknowledge these procedures within 60 days of hire. Management publishes the Information Security Policy to internal personnel. In addition, internal personnel acknowledge these procedures within 60 days of hire. Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors taking into consideration segregation of duties as necessary at various levels of the organization and requirements relevant to security.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	iFolio evaluates the performance of internal personnel through a formal, annual performance evaluation. Management maintains a formal organizational chart to clearly identify positions of authority and the lines of communication, and publishes the organizational chart for personnel. Violations of iFolio policies are subject to disciplinary action and such disciplinary action is clearly documented in one or more policies.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	iFolio has a continuous monitoring solution for internal controls used in the achievement of Company's service commitments and system requirements. The Chief Financial Officer performs a formal risk assessment, which includes the identification of relevant internal and external threats related to security, confidentiality, fraud, and an analysis of risks associated with those threats. Vulnerability monitoring is performed real-time on production infrastructure systems. iFolio remediates identified deficiencies, if any, on a timely basis.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	iFolio has a confidential reporting channel available to internal personnel and external users to report security and other identified concerns. Security commitments and expectations are communicated to external users via the Company's website. iFolio publishes its Privacy Policy to both external users and internal personnel. This policy details the Company's privacy commitments. iFolio's Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution. iFolio has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance. In addition, personnel acknowledge the Code of Conduct promptly on hire. Senior management and BOD meet at least annually to review business objectives, company initiatives, resource needs, and risk management activities. Internal personnel complete annual training programs for information security to educate them of their obligations and responsibilities related to security and confidentiality.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Information and Communication		
CC2.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Management publishes the Acceptable Use policy to internal personnel. In addition, internal personnel acknowledge these procedures within 60 days of hire. Management publishes the Data Classification Policy to internal personnel. In addition, internal personnel acknowledge these procedures within 60 days of hire. Management publishes the Information Security Policy to internal personnel. In addition, internal personnel acknowledge these procedures within 60 days of hire. iFolio's management is responsible for the design, implementation, and management of the organization’s security policies and procedures. The policies and procedures are reviewed at least annually.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	iFolio has a confidential reporting channel available to internal personnel and external users to report security and other identified concerns. Security commitments and expectations are communicated to external users via the Company's website. iFolio publishes its Terms of Service to both internal personnel and external users. These Terms of Service detail the Company's confidentiality commitments. iFolio communicates critical information to customers and other external parties, as applicable via the website and or direct communication. iFolio publishes its Privacy Policy to both external users and internal personnel. This policy details the Company's privacy commitments.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	iFolio's Management performs a formal review of the Risk Assessment and Vendor Management Policy at least annually. Risk tolerance and strategies are defined in the policy. The Chief Financial Officer performs a formal risk assessment, which includes the identification of relevant internal and external threats related to security, confidentiality, fraud, and an analysis of risks associated with those threats.
CC3.2	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.	iFolio maintains and reviews a list of the Company's system components (including confidential information) and owners. The Chief Financial Officer performs a formal risk assessment, which includes the identification of relevant internal and external threats related to security, confidentiality, fraud, and an analysis of risks associated with those threats. The Chief Financial Officer maintains and reviews a risk register, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy. iFolio's Vendor Risk Management Policy defines a framework for the onboarding and management of the vendor relationship lifecycle. The Chief Financial Officer assess new vendors according to the Vendor Risk Management Policy prior to engaging with the vendor. The relationship owner collects and reviews the SOC reports (or equivalent) of its subservice organizations on an annual basis.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The Chief Financial Officer performs a formal risk assessment, which includes the identification of relevant internal and external threats related to security, confidentiality, fraud, and an analysis of risks associated with those threats. Management uses information technology tools including security systems, fraud detection and monitoring systems, and incident tracking systems to identify and manage fraud risk.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Assessment		
CC3.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The Chief Financial Officer performs a formal risk assessment, which includes the identification of relevant internal and external threats related to security, confidentiality, fraud, and an analysis of risks associated with those threats. Management uses information technology tools including security systems, fraud detection and monitoring systems, and incident tracking systems to identify and manage fraud risk.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Monitoring Activities		
CC4.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	System owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities. iFolio has a continuous monitoring solution for internal controls used in the achievement of Company's service commitments and system requirements. Vulnerability monitoring is performed real-time on production infrastructure systems. iFolio remediates identified deficiencies, if any, on a timely basis.
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.	System owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities. Senior management and BOD meet at least annually to review business objectives, company initiatives, resource needs, and risk management activities. iFolio has a continuous monitoring solution for internal controls used in the achievement of Company's service commitments and system requirements. Vulnerability monitoring is performed real-time on production infrastructure systems. iFolio remediates identified deficiencies, if any, on a timely basis.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	iFolio maintains and reviews a list of the Company's system components (including confidential information) and owners. The Chief Financial Officer performs a formal risk assessment, which includes the identification of relevant internal and external threats related to security, confidentiality, fraud, and an analysis of risks associated with those threats. The Chief Financial Officer maintains and reviews a risk register, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	iFolio's Change Management Policy governs the system development life cycle (including emergency changes), documented policies for tracking, testing, and approving changes. Management publishes the Data Classification Policy to internal personnel. In addition, internal personnel acknowledge these procedures within 60 days of hire. iFolio's Policies outline roles and responsibilities for personnel with responsibility for the Security of the system. iFolio's Data Classification Policy and Acceptable Use Policy details the security and handling protocols for sensitive data.
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.	iFolio has established a Code of Conduct outlining ethical expectations, behavior standards, and ramifications of noncompliance. In addition, personnel acknowledge the Code of Conduct promptly on hire. Management publishes the Acceptable Use policy to internal personnel. In addition, internal personnel acknowledge these procedures within 60 days of hire. Management publishes the Data Classification Policy to internal personnel. In addition, internal

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Control Activities		
CC5.0	**Criteria**	**Control Activity Specified by the Service Organization**
		personnel acknowledge these procedures within 60 days of hire. Management publishes the Information Security Policy to internal personnel. In addition, internal personnel acknowledge these procedures within 60 days of hire. iFolio's management is responsible for the design, implementation, and management of the organization’s security policies and procedures. The policies and procedures are reviewed at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	iFolio maintains and reviews a list of the Company's system components (including confidential information) and owners. Users are assigned unique IDs to access sensitive information. User access to systems and applications with customer data requires a form of two-factor authentication, where available. iFolio has formal policies for password requirements, including complexity and length and the use of authentication mechanisms, when available. Production infrastructure is restricted to authorized users with a unique account, SSH key or access key. Administrative access to production servers, databases, and internal administrative tools is restricted based on the principal of least privilege access. Users are provisioned access, as approved to systems based on principal of least privilege access. Upon termination or when internal personnel no longer require access, infrastructure and application access is removed, as applicable. Service data is encrypted at rest, through the use of AWS encryption settings. iFolio's Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls and is reviewed at least annually. System owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.
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.	Users are provisioned access, as approved to systems based on principal of least privilege access. Upon termination or when internal personnel no longer require access, infrastructure and application access is removed, as applicable.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		System owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.
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.	Administrative access to production servers, databases, and internal administrative tools is restricted based on the principal of least privilege access. Users are provisioned access, as approved to systems based on principal of least privilege access. Upon termination or when internal personnel no longer require access, infrastructure and application access is removed, as applicable. System owners conduct at least annual user access reviews of production servers, databases, and applications to validate internal user access is commensurate with job responsibilities.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criteria is the responsibility of the subservice organization. Please refer to the "Subservice Organization" section above for controls managed by the subservice organization.
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.	This criteria is the responsibility of the subservice organization. Please refer to the "Subservice Organization" section above for controls managed by the subservice organization.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Users are assigned unique IDs to access sensitive information. User access to systems and applications with customer data requires a form of two-factor authentication, where available. iFolio has formal policies for password requirements, including complexity and length and the use of authentication mechanisms, when available. Production infrastructure is restricted to authorized users with a unique account, SSH key or access key.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Logical and Physical Access Controls		
CC6.0	**Criteria**	**Control Activity Specified by the Service Organization**
		Administrative access to production servers, databases, and internal administrative tools is restricted based on the principal of least privilege access. Service data is encrypted at rest, through the use of AWS encryption settings. Encryption is used to protect the transmission of data in transit. Configurations ensure available networking ports and protocols are restricted as necessary. iFolio's Encryption and Key Management Policy supports the secure encryption and decryption of app secrets, and governs the use of cryptographic controls and is reviewed at least annually. Anti-malware software is installed on workstations to detect and prevent the transmission of data or files that contain malware recognized by the anti-malware software.
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.	Administrative access to production servers, databases, and internal administrative tools is restricted based on the principal of least privilege access. Service data is encrypted at rest, through the use of AWS encryption settings. Encryption is used to protect the transmission of data in transit. iFolio encrypts hard drives for portable endpoints with full disk encryption.
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.	iFolio's Configuration and Asset Management Policy governs configurations for new sensitive systems. iFolio's Change Management Policy governs the system development life cycle (including emergency changes), documented policies for tracking, testing, and approving changes. Anti-malware software is installed on workstations to detect and prevent the transmission of data or files that contain malware recognized by the anti-malware software.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	iFolio's Configuration and Asset Management Policy governs configurations for new sensitive systems. iFolio's Vulnerability Management Program outlines the procedures to identify, assess, and remediate identified vulnerabilities. Vulnerability monitoring is performed real-time on production infrastructure systems. iFolio remediates identified deficiencies, if any, on a timely basis.
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.	Company endpoints are managed via MDM or equivalent. Management had implemented tools to provide monitoring of network traffic to the production environment. iFolio uses logging and monitoring software to collect data from servers, detect potential security threats and unusual system activity and monitor system performance. iFolio uses alerting software to notify impacted teams of potential security and availability events. Anti-malware software is installed on workstations to detect and prevent the transmission of data or files that contain malware recognized by the anti-malware software.
CC7.3	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.	iFolio publishes its Privacy Policy to both external users and internal personnel. This policy details the Company's privacy commitments. iFolio's Incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution. iFolio's Security Response Team tracks and ensures resolution of identified incidents according to the Incident Response Plan.
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.	iFolio's Security Response Team tracks and ensures resolution of identified incidents according to the Incident Response Plan.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
System Operations		
CC7.0	**Criteria**	**Control Activity Specified by the Service Organization**
		iFolio performs a 'lessons learned' exercise after each significant incident to determine the root cause and shares this document with the appropriate team to make any required changes.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	iFolio's Security Response Team tracks and ensures resolution of identified incidents according to the Incident Response Plan. iFolio performs a 'lessons learned' exercise after each significant incident to determine the root cause and shares this document with the appropriate team to make any required changes.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Change Management		
CC8.0	**Criteria**	**Control Activity Specified by the Service Organization**
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.	iFolio's Change Management Policy governs the system development life cycle (including emergency changes), documented policies for tracking, testing, and approving changes. System changes are tested prior to being deployed into production. Code merge requests are required to be independently peer reviewed prior to integrating the code change into the master branch and system users who make changes are unable to deploy their own changes without independent approval. The production and staging environments are segregated to ensure testing and or changes in the lower environments does not impact the production system. Production data/client data is not used in the development and staging environments. iFolio's Configuration and Asset Management Policy governs configurations for new sensitive systems. Descriptions of the Company's services are available to both internal personnel and external users, on the Company's product page.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
Risk Mitigation		
CC9.0	**Criteria**	**Control Activity Specified by the Service Organization**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	iFolio's incident Response Plan outlines the process of identifying, prioritizing, communicating, assigning and tracking confirmed incidents through to resolution. iFolio has a current insurance policy to help minimize the financial impact of business loss events. The Chief Financial Officer performs a formal risk assessment, which includes the identification of relevant internal and external threats related to security, confidentiality, fraud, and an analysis of risks associated with those threats. The Chief Financial Officer maintains and reviews a risk register, which records the risk mitigation strategies for identified risks, and the development or modification of controls consistent with the risk mitigation strategy. Full backups are performed on a weekly basis and retained in accordance with the Backup Policy. iFolio maintains a business continuity and disaster recovery plan. iFolio tests its Business Continuity and Disaster Recovery Plan on an annual basis. When necessary, Management makes changes to the Business Continuity and Disaster Recovery Plan based on the test results.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	iFolio's management is responsible for the design, implementation, and management of the organization’s security policies and procedures. The policies and procedures are reviewed at least annually. The relationship owner collects and reviews the SOC reports (or equivalent) of its subservice organizations on an annual basis.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

Hancock Askew & Co., LLP's examination of the controls of iFOLIO was limited to the Trust Services Criteria, related criteria and control activities specified by the management of iFOLIO and did not encompass all aspects of iFOLIO's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria;
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization;
- Determine whether the criteria are relevant to the user entity's assertions; and
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria.