GENERAL CONTROLS SUPPORTING THE CLOUD HOSTING SERVICES

SOC 3 Audit Report

Independent Service Auditor's Report on Controls Placed in Operation Relevant to the Trust Services Categories of Security and Availability

For the Period January 1, 2021 to December 31, 2021

INDEPENDENT SERVICE AUDITOR'S REPORT

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

The Moore Group, CPA
SOC Audit Specialists

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Hyve Managed Hosting Corp Inc.,

Scope

We have examined Hyve Managed Hosting Corp Inc.'s (HYVE) accompanying management's assertion found in Section 2 titled "Assertions by the Service Organization's Management" (assertion) that the general controls supporting the cloud hosting services and systems (system) were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that HYVE's principal service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security and availability* (*AICPA, Trust Services Criteria)*.

HYVE uses a third party data center (subservice organization) to house its critical production computer servers, applications and networking equipment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HYVE, to achieve HYVE's service commitments and system requirements based on the applicable trust services criteria. The description presents HYVE's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of HYVE'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 HYVE, to achieve HYVE's service commitments and system requirements based on the applicable trust services criteria. The description presents HYVE's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of HYVE'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

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

Service Auditor's Responsibilities

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

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risk that controls were not effective to achieve HYVE's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve HYVE's service commitments and system requirements based on the applicable trust services criteria.

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within HYVE's cloud hosting services were effective throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that HYVE's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of HYVE's controls were effective throughout that period.

The Moore Group CPA, LLC

Nashua, NH
January 26, 2022

SECTION 2

ASSERTIONS BY THE SERVICE ORGANIZATION'S MANAGEMENT

MANAGEMENT ASSERTION OF HYVE MANAGED HOSTING CORP

January 26, 2022

We are responsible for designing, implementing, operating, and maintaining effective controls within Hyve Managed Hosting Corp Inc.'s (HYVE) cloud hosting services and systems (system) throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that HYVE's service commitments and system requirements relevant to security and availability (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented in Section 3 titled "Description of the Service Organization's System Provided by HYVE Management" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that HYVE's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security and availability* (AICPA, *Trust Services Criteria)*. HYVE's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements related to the applicable trust services criteria presented in Section 3.

HYVE uses a third party data center (subservice organization) to house its critical production computer servers, applications and networking equipment. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HYVE, to achieve HYVE's service commitments and system requirements based on the applicable trust services criteria. The description presents HYVE's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of HYVE's controls. The description does not disclose the actual controls at the subservice organization.

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

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

We assert that the controls within the system were effective throughout the period January 1, 2021 to December 31, 2021 to provide reasonable assurance that HYVE's service commitments and system requirements were achieved based on the applicable trust services criteria.

SECTION 3

DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM PROVIDED BY HYVE MANAGEMENT

DESCRIPTION OF CONTROLS PLACED IN OPERATION

OVERVIEW OF OPERATIONS

Company Background

Hyve Managed Hosting (HYVE) was incorporated in May of 2017 with the aim of bringing a new breed of managed hosting and “extra mile” support to the USA. Building on the solid reputation of its parent UK based company Hyve Ltd, HYVE is delivering custom hosting solutions to US and multinational customers.

Jake Madders and Jon Lucas started the UK parent company back in 2001 after they realized they could deliver a much better service and end user experience for any early adopters of cloud hosting services. Growing the company each year, moving to the US was the next logical step.

Hyve’s ethics of putting the customer first and delivering unparalleled customer support and fully managed hosting remains a focus for the team.

Hyve Managed Hosting delivers Private, Public and Hybrid clouds that are designed by highly experienced technical architects who will build a solution that is fit for now and the future.

Scope of SOC Audit

The scope of this SOC audit includes an assessment of the general organizational and information technology controls supporting the cloud hosting services and systems of HYVE. The scope does not include an assessment of any banking, fraud protection, cash receipts/payments, accounting, or other internal or external financial responsibilities of HYVE.

Description of Services Provided

Hyve Managed Cloud is HYVE’s core hosting offering. Created by cloud experts with over 15 years industry experience, Hyve Managed Cloud is hosted on HYVE’s own infrastructure, providing full control. Unlike a public cloud solution, Hyve Managed Cloud is only used by HYVE verified customers for added security.

Cloud Hosting

- Managed Cloud – HYVE’s US-based fully managed, multi-tenant cloud delivers high-performance, reliability and scalability that outperforms the competition.
- Hybrid Cloud - HYVE’s Hybrid Cloud can use a combination of on-premise, private cloud and managed cloud services, working together in tandem. Hybrid Cloud provides businesses with the security and control of a private cloud and the flexibility and cost savings of public cloud.
- Private Cloud - HYVE’s private cloud runs on hardware dedicated to the client’s organization**.** No shared resources means that clients have the ultimate in security**.** HYVE’s private cloud keeps sensitive information locked down, giving clients peace of mind that their data is secure. Clients get full control of every aspect of their server.

Principal Service Commitments and System Requirements

HYVE makes service commitments to its customers and has established system requirements as part of the cloud hosting services. Some of these commitments are principal to the performance of the service and relate to the applicable trust services criteria. HYVE 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 HYVE's service commitments and system requirements are achieved.

Service commitments to customers are documented and communicated in HYVE's policies and procedures, system design documentation, customer agreements, or other written company materials provided to user entities as well as in the description of the service offering provided online. Service commitments include, but are not limited to, the following:

- Security: HYVE has made commitments related to a secure information technology control environment and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, and other relevant security controls.

- Availability: HYVE has made commitments related to providing reliable and consistent uptime and connectivity for the IT systems used in the services offered by HYVE. These commitments include, but are not limited to, design, development or acquisition, implementation, monitoring, and maintaining environmental protection of systems, software, data back-up processes, and recovery infrastructure to meet availability commitments.

HYVE has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in its system policies and procedures, system design documentation, and customer agreements. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of various HYVE services.

Components of the System

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the description of services and the components of infrastructure, software, people, procedures, and data.

The components of the system used to provide the services are as follows:

Infrastructure

Subservice Organization - HYVE utilizes the services and controls of a third-party data center, Equinix, for hosting critical production web application servers, development servers and the necessary networking equipment. The Equinix data center had a SOC 1 Type II and SOC 2 Type II audits completed for the review period of November 1, 2020 to October 31, 2021. The scope of this audit does not include the controls of Equinix.

The cloud environment infrastructure has redundancy at all levels. Redundant layers at the edge (routers and firewalls), redundant at the core (switching), redundancy within the hosts, and redundant backend storage.

Third-party enterprise monitoring applications are used to monitor system downtime and operations issues to help ensure that system downtime and performance does not exceed predefined levels. This includes monitoring of both critical network and server hardware, as well as processes and services. The enterprise monitoring application is configured to send alert notifications to operations personnel when predefined metrics are exceeded on monitored network devices. Alerts are communicated via SMS text or email to appropriate support personnel.

Servers and workstations utilize anti-virus endpoint protection, which is kept properly updated and conducts routine scans.

Windows Server operating system patches for critical production systems are updated manually to ensure adequate testing and that no production interference will result. Workstation operating system patches are updated automatically to ensure critical vulnerabilities are patched as soon as possible. A central service, Windows Update Services, automatically pushes updates on a periodic basis for routine patching, and immediately for critical vulnerabilities.

Software

A combination of custom developed and commercial applications is utilized to support the cloud hosting services provided to user organizations. The applications run on Windows Server Operating Systems, VMWare, and HP Enterprise blade servers and SAN's with commercial databases to support the applications.

People

HYVE is led by its Co-Owners/Directors, Jake Madders and Jon Lucas, and executives in the departmental areas of Technology, Operations, and Sales. HYVE's organization structure provides the overall framework for planning, directing, and controlling operations. Personnel and business functions are separated into departments according to job responsibilities. The structure provides defined responsibilities and lines of authority for reporting and communication. The assignment of roles and responsibilities within the various departments provides effective segregation of duties.

In the Control Environment section of this report, additional information is described related to organizational controls implemented at HYVE. These organizational controls are intended to serve as the internal foundation for providing services to its customers.

Procedures

HYVE has implemented processes and procedures to support the operations and controls over the services and systems provided to its customers. Specific examples of the relevant procedures include, but are not limited to, the following:

- Policies and procedures are in place to guide personnel regarding assessing risks on a periodic basis.
- Security policies are in place to guide personnel regarding physical and information security practices.

- Policies and procedures are in place for identifying the system security requirements of authorized users.
- Third-party enterprise monitoring applications are used to monitor system downtime and operations issues to help ensure that system downtime and performance does not exceed predefined levels.
- An Incident Response plan is in place to ensure appropriate response to outages or security incidents in an organized and timely manner.
- Policies and procedures are in place to guide personnel regarding addressing how complaints and requests relating to security issues are resolved.
- Policies and procedures are in place to assign responsibility and accountability for system changes and maintenance.
- Policies and procedures are in place to guide personnel regarding identifying and mitigating security breaches and other incidents.
- Management utilizes intrusion detection systems (IDS) to detect unauthorized intrusion into the production environment. The IDS subscription is kept current.
- HYVE IT personnel utilize security issue monitoring services to keep abreast of recent critical issues, attacks and vulnerabilities that must be addressed immediately.
- Firewall systems are in place to screen data flow between external parties and the HYVE production network.
- Policies and procedures are in place to add new users, modify the access levels of existing users, and remove users who no longer need access.
- Production server users are required to authenticate via a unique user ID and password before being granted access to the production environment.
- Application users are required to authenticate via an authorized unique user ID and password before being granted access to the production environment. Multifactor authentication is enabled.
- Each customer is assigned a designated administrator during the onboarding process with authority to create or modify user access to the hosted user application for their organization.
- Physical security policies and procedures are in place to guide personnel regarding restricting access to the facility.
- Management periodically performs internal security assessments, including reviews of server logs and other critical items.
- Policies and procedures are in place to ensure that design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.
- Policies and procedures are in place to ensure that change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.

Data

Access to data is limited to authorized personnel in accordance with HYVE's system security policies. HYVE is also responsible for the overall availability of data, including system backups, monitoring of data processing, and file transmissions as well as identifying and resolving problems.

Backups are performed to provide the capability to restore data and software in the event of system failure or corruption. Documented procedures are in place to guide HYVE personnel in the backup and restoration process.

For backup of critical customer data, an initial seed image is taken of virtual machines and then a nightly incremental backup is performed to dedicated backup storage.

Databases containing critical customer data are replicated to a set of standby servers at geographically dispersed data center utilizing Microsoft SQL Server publications and subscriptions or High Availability Groups over secure site-to-site VPN tunnels.

Encryption is utilized to protect data in transit, including TLS encryption over HTTPS connections utilized for secure communications between HYVE and customer end users. Certain IT engineer's access production network equipment and data stored at the third-party data center remotely, via secure VPN tunnels protected by TLS and IPsec encryption and/or secure SSH sessions.

Controls in place specific to the data responsibilities of HYVE include, but are not limited to, the following:

- Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Firewall systems are in place to screen data flow between external parties and the HYVE production network.
- A secure VPN (Virtual Private Network) connection is used for remote external access to the internal network by authorized HYVE employees.
- Site-to-site VPN tunnels are locked down to specific locations via an access control list. IPsec network layer encryption is utilized.
- Policies and procedures are in place to guide personnel regarding sharing information with third parties.
- Communication sessions between HYVE's servers/applications and external parties are secured using various encryption methods when applicable.
- File transfer sessions that utilize production server applications are secured through the use of the following encryption methods:
    - TLS encryption over FTPS connections
    - SSH encryption over SFTP connections.
- Transaction processing performed on web-based applications is secured through the use of the Transport Layer Security (TLS) encryption protocol over HTTPS connections.
    - This includes the use of the website file upload page.
    - Traffic directed to HTTP connections for this are redirected to HTTPS connections.

Disaster Recovery

HYVE maintains a current Disaster Recovery Plan and Business Continuity plan. Disaster and business continuity emergency situations are ultimately managed through proper planning (crisis management, recovery and continuity) and response. Identified risks have been mitigated through prevention, minimization or rapid recovery resources and planning. HYVE's disaster recovery and business continuity program helps to ensure that disruptive incidents are responded to quickly and effectively.

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 HYVE's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of HYVE's ethical and behavioral standards, how they are communicated, and how they are reinforced in daily practice.

These standards 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, and by personal example.

Specific control activities that HYVE has implemented in this area are described below.

- HYVE maintains an employee handbook which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.
- Policies and procedures require that new employees sign an employee handbook acknowledgment form indicating that they have been given access to it and understand their responsibilities. The signed form is kept in the employee personnel file.
- Employees must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Criminal records data base check*s* are performed for *all* positions as a component of the hiring process. Only completely clear returns are accepted.
- *Contract employees (1099)* must sign a confidentiality and non-disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.
- Management maintains a commercial general liability insurance policy which includes technology/professional errors and omissions coverage and/or employee dishonesty.

Commitment to Competence

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

Specific control activities that HYVE 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 job descriptions.
- Candidates' abilities to meet job requirements are evaluated as part of the hiring, performance review, and transfer evaluation processes.

- Roles and responsibilities for company personnel to interact with and monitor the activities of external third-party information technology vendors are defined in written job descriptions and communicated to personnel.
- Management has developed a training and development program for employees. This includes initial training/orientation with peers and supervisors in the period immediately after hire.
- Management encourages employees to complete and continue formal education and technical certification programs. (formally or informally)
- Certain approved professional development expenses incurred by the employees are paid by HYVE. (training certs, classes, etc.)
- Employees undergo an annual performance review. A formal evaluation is prepared and is maintained in the employee's HR file.
- Employees undergo a 90 day review after hire. A formal evaluation is prepared and is maintained in the employee's HR file.
- HYVE utilizes an independent CPA firm to prepare tax returns.

Board of Directors' Participation

HYVE's control consciousness is influenced significantly by its Board of Directors participation. The Board of Directors oversees management activities and meets at least quarterly to discuss strategic, operational, and compliance issues.

Management's Philosophy and Operating Style

HYVE's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward the cloud hosting services, information processing, accounting functions and personnel. Management is periodically briefed on regulatory and industry changes affecting services provided. Management meetings are held on a periodic basis to discuss and monitor operational issues.

Specific control activities that HYVE has implemented in this area are described below.

- Each employee undergoes Security Awareness training annually.
- Management holds annual discussions with each employee related to their individual responsibilities for Information Security including data and systems security.
- Management regularly attends trade shows, utilizes trade and regulatory publications, journals, online news feeds and government sites, and belongs to industry associations to stay current on regulatory compliance or operational trends affecting the services provided.
- Operational meetings are held on a regular basis to discuss internal control responsibilities *(data and system security)* of individuals and performance measurement.
- HYVE utilizes an independent CPA firm to prepare tax returns.

Organization Structure and Assignment of Authority and Responsibility

HYVE's organization structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. HYVE's management believes that establishing a relevant organization structure includes considering key areas of authority and responsibility and appropriate lines of reporting. HYVE has developed an organization structure suited to its needs. This organization structure is based, in part, on its size and the nature of its activities.

HYVE'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 that all 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 HYVE has implemented in this area are described below.

- Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel.

Human Resource Policies and Practices

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

Specific control activities that HYVE has implemented in this area are described below.

- Management utilizes a new hire process to ensure that specific elements of the hiring process are consistently executed.
- A formal process is in place to ensure HR informs IT when employee access to company IT resources needs to be added or removed.
- Criminal records data base checks are performed for *all* positions as a component of the hiring process. Only completely clear returns are accepted.
- HYVE maintains an employee handbook which contains organizational policy statements, behavioral standards, codes of conduct and disciplinary policies to which all employees are required to adhere.
- Management has developed a training and development program for employees. This includes initial training/orientation with peers and supervisors in the period immediately after hire.
- Employees undergo an annual performance review. A formal evaluation is prepared and is maintained in the employee's HR file.
- Employees undergo a 90 day review after hire. A formal evaluation is prepared and is maintained in the employee's HR file.
- Management utilizes a termination checklist to ensure that specific elements of the termination process are consistently executed. A copy of the checklist is kept in the employee file.

END OF REPORT