

One company
Unlimited possibilities

Hyland®

Hyland
creator of OnBase®

Service Organization Controls 3 Report

**Report on Hyland Software, Inc.'s Hyland Cloud
Platform, relevant to Security, Availability, and Confidentiality**

for the period May 1, 2017 through October 31, 2017





Ernst & Young LLP
Suite 1800
950 Main Avenue
Cleveland, OH 44113-7214

Tel: +1 216 861 5000
Fax: +1 216 583 2013
ey.com

Report of Independent Accountants

To the Board of Directors
Hyland Software, Inc.

Approach:

We have examined management's assertion that Hyland Software, Inc. (Hyland) maintained effective controls to provide reasonable assurance that:

- the Hyland Cloud Platform was protected against unauthorized access, use, or modification to achieve Hyland Software, Inc.'s commitments and system requirements
- the Hyland Cloud Platform was available for operation and use to achieve Hyland Software Inc.'s commitments and system requirements
- the Hyland Cloud Platform system information is collected, used, disclosed, and retained to achieve Hyland Software Inc.'s commitments and system requirements

during the period May 1, 2017 through October 31, 2017 based on the criteria for security, availability, confidentiality in the American Institute of Certified Public Accountants' TSP Section 100A, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Hyland's management. Our responsibility is to express an opinion 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 management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Hyland's relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Hyland's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

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 inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability, and confidentiality are achieved.



Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, projections of any evaluation of effectiveness to future periods are 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, Hyland's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, and confidentiality.

Ernst & Young LLP

Ernst & Young LLP
December 21, 2017

Management Assertion Regarding the Effectiveness of Its Controls Over the Hyland Cloud Platform Based on the Trust Services Principles and Criteria for Security, Availability, and Confidentiality

December 21, 2017

We, as management of, Hyland Software, Inc. (Hyland) are responsible for designing, implementing and maintaining effective controls over the Hyland Cloud Platform (System) to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in Security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

We have performed an evaluation of the effectiveness of the controls over the system throughout the period May 1, 2017 to October 31, 2017, to achieve the commitments and system requirements related to the operation of the System using the criteria for the security, availability, confidentiality (Control Criteria) set forth in the AICPA's TSP section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Based on this evaluation, we assert that the controls were effective throughout the period May 1, 2017 to October 31, 2017 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Hyland's commitments and system requirements
- the System was available for operation and use, to achieve Hyland's commitments and system requirements
- the System information is collected, used, disclosed, and retained to achieve Hyland's commitments and system requirements based on the Control Criteria.

Our attached description of the boundaries of the Hyland Cloud Platform identifies the aspects of the Hyland Cloud Platform covered by our assertion.

Global Cloud Services Management
Hyland Software, Inc.

Hyland Cloud Platform Background

Established in 1991, Hyland Software, Inc. (Hyland) is the developer of OnBase, an Enterprise Content Management (ECM) solution designed to help organizations streamline their document and content management processes and share information among employees, partners, and customers. Hyland is based in Westlake, Ohio.

The OnBase ECM software electronically captures and manages everything from paper reports to web content. It is used by customers in industries ranging from financial services and government to manufacturing and health care. In addition to its core solutions, Hyland also offers specific add-on modules for functions such as business process automation, digital imaging and capturing, records management, and enterprise file synchronization and sharing. Customers utilize these solutions to fulfill a variety of business needs, including information consumption, streamlining business needs with a high degree of reliability and integrity.

Hyland leverages the Hyland Cloud Platform to deliver hosted OnBase ECM solutions. These hosted solutions reside on servers that are owned and managed by Hyland. The Hyland Cloud is co-located within N+1 redundant data centers that are owned and operated by third-party Internet Service Providers (ISPs), AT&T, BlueBridge Networks, and KIO Networks. These ISPs provide internet connectivity, physical security components, power, threat and environmental systems monitoring and services to the hosting environment. Customers securely access their hosted solution from the Internet using encrypted network protocols including secure sockets layer (SSL), transport layer security (TLS), and/or secure file transfer (SFTP).

Services covered by this report

The Hyland Cloud Platform is comprised of components such as network devices, servers and software that are physically installed and operating within its defined system which is limited to components such as network drives, servers, and software that are physically installed and operating within Hyland's internet-enabled network infrastructure, and its process boundaries, which are limited to those that are executed by a Hyland employee within Hyland's Global Cloud Services (GCS) department, an authorized third-party, or processes that are executed within their established system boundaries.

For the purposes of this report, the Hyland Cloud Platform's system boundary does not include any instances of a hosted solution that is used for non-production workloads. This includes systems that are used exclusively for pilot, demo, testing, or development purposes.

Components of the Hyland Cloud Platform Providing the Defined Services

Infrastructure

Hosting services are provided to customers through an internet-enabled network infrastructure that is owned and operated by Hyland. The system components associated with this network infrastructure are physically located within data centers that are owned and operated by third-party ISPs. These ISPs provide internet connectivity, physical security components, power, threat and environmental systems monitoring and services to the hosting environment.

Hyland installs servers within each data center on an as-needed basis. Hyland owns and operates these servers. This includes, but is not limited to, web, application, file and database servers. A variety of peripheral devices are also used. This may include, but is not limited to, network appliances, disk drives, and keyboard video monitor switches which are also owned and operated by Hyland.

People

Hyland's organizational structure provides a framework for planning, executing, and controlling business operations. Executive and senior leadership play important roles in establishing the Company's tone and core values. The

organizational structure assigns roles and responsibilities to provide for adequate staffing, security, efficiency of operations, and segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel.

Primary responsibility for the delivery of Platform hosting services, including administration, has been assigned to Hyland's Global Cloud Services (GCS) department. Employees are screened and qualified before a job position is offered. Hyland maintains written job descriptions/plans specifying the responsibilities and corresponding academic and professional requirements for key job positions to determine that current and prospective employees have the qualifications and skill level necessary to perform the job successfully. All employees are informed of their security-related responsibilities before access to the Hyland Cloud Platform is provisioned. Policy and security-related training is provided on an annual basis.

Policies and Procedures

All Hyland employees are expected to adhere to company-wide, departmental, and, when applicable, position-specific policies and procedures that define how hosting services should be delivered. These requirements are documented within Hyland's GCS Information Security policies which includes the GCS Process Manual. Policy documents are provided upon hiring and then can be accessed by appropriate personnel. The GCS Information Security policies align with the guidance described in the ISO 27001 Annex A and includes controls (e.g., Risk Management, Access Controls, Supplier Relationships). These controls are designed to safeguard the security, availability and confidentiality of all system components including Customer Data. Policies are reviewed and, if necessary, updated annually by the GCS Vice President and Leadership Team.

Data

Data, as defined herein, constitutes the following:

- ▶ Files owned by a customer that are stored within customer-designated disk groups. Disk groups are configured to write electronic documents to a primary network attached storage device or file server.
- ▶ Files owned by a customer that have been transferred to the Hyland Cloud Platform SFTP (Secure File Transfer Protocol) systems.
- ▶ Meta-data owned by a customer that is stored within the solution's database. The database is configured to store data files and transaction log files to redundant array of inexpensive disks (RAID).

Hyland Cloud Platform customers retain control and ownership of their own data. Customers are responsible for the development, content, operation, maintenance, and use of their content. The Hyland Cloud Platform is designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software.

Availability and Incident Handling

The Hyland Cloud Platform is architected in a manner to maintain availability of its services through defined programs, processes, and procedures.

Hyland employees monitor the network using both automated and traditional means. Predefined events (e.g., ping failures, full drive, missing application heartbeats) generate alerts that are delivered to Hyland personnel on a 24/7 basis.

Customers are instructed to contact the Hyland Technical Support Team and report any suspected availability incidents. The Hyland Technical Support Team will interview the user and gather information to assess the event as to whether it is a malfunction or a possible service failure.

If it is determined that the event represents a potential service failure, Hyland employees follow documented escalation procedures. All availability incidents are investigated promptly and thoroughly by individuals who are qualified to perform this task. All availability incidents are documented and reviewed within de-escalation procedures conducted by the GCS Leadership Team.

Once normal business operations have been restored after a service failure, Hyland will deliver a summary report to the applicable impacted customers. Information contained within this report will include, but is not limited to, when the incident occurred, when normal business operations were restored, the root cause of the incident, the technical effect of the incident, an accounting of actions taken to restore service, and a description of any outstanding remediation plans that have been approved by the GCS Leadership Team.

The Hyland Cloud Platform is architected in a manner to maintain availability of its services through defined programs, processes, and procedures. The disaster recovery plan encompasses the processes and procedures by which Hyland identifies, responds to, and recovers from a major event or incident within the environment. This program builds upon the traditional approach of addressing contingency management, incorporating elements of business continuity and disaster recovery plans while expanding to consider critical elements of proactive risk mitigation strategies. Contingency plans and incident response procedures are maintained to reflect emerging continuity risks and lessons learned. Plans are tested and updated through the course of business and the disaster recovery plan is annually reviewed and approved by senior leadership.

Hyland has identified critical system components required to maintain the availability of the system and recover services in the event of an outage. These components are replicated across multiple co-location data centers; backups are maintained and monitored to ensure successful replication.

Service usage is continuously monitored, protecting infrastructure needs and supporting availability commitments and requirements. Additionally, GCS maintains a capacity planning model to assess infrastructure usage and demands.

Co-location Vendors

Hyland owns and operates an internet-enabled network infrastructure. The Hyland Cloud Platform components associated with this network infrastructure are physically located within data centers that are owned and operated by Internet Service Providers (ISPs). These ISPs provide internet connectivity, physical security components, power, and environmental systems and services. GCS installs servers within the co-location data centers on an as-needed basis to this internet-enabled network infrastructure. GCS owns and operates these servers. This includes, but is not limited to, web, application, file, and database servers and other peripheral devices as required to configure and manage customer solutions.