

The Hyland logo consists of a square with a vertical gradient from green at the top to blue at the bottom. The word "Hyland" is written in white, serif font, centered within the square.

Hyland®

Service Organization Controls 3 Report

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

for the period May 1, 2020 through October 31, 2020





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.

### *Scope:*

We have examined management's assertion, contained within the accompanying Management Assertion Regarding the Effectiveness of Its Controls Over the Hyland Cloud Platform Based on the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy (Assertion), that Hyland Software, Inc.'s controls over the Hyland Cloud Platform (System) were effective throughout the period May 1, 2020 to October 31, 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality, privacy (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Hyland Software, Inc. (Hyland) uses Amazon Web Service (AWS) to provide physical hosting and data replication services for a subset of in-scope solutions. The Description of the boundaries of the System (Attachment A) indicates that Hyland's controls can provide reasonable assurance that certain service commitments and system requirements, based on the applicable trust services criteria, can be achieved only if AWS's controls, assumed in the design of Hyland's controls, are suitably designed and operating effectively along with related controls at the service organization. The Description presents Hyland's system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS. Our examination did not extend to the services provided by AWS and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period May 1, 2020 to October 31, 2020.

### *Management's Responsibilities*

Hyland Software, Inc.'s management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Hyland Cloud Platform (System) and describing the boundaries of the System
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of their system
- identifying, designing, implementing, operating, and monitoring effective controls over the Hyland Cloud Platform (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement

### *Our Responsibilities*

Our responsibility is to express an opinion on the Assertion, 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 Software Inc.'s relevant security, availability, confidentiality, and privacy 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 to provide a reasonable basis for our opinion.

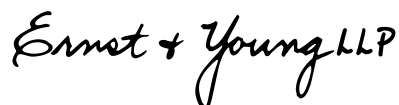
Our examination was not conducted for the purpose of evaluating Hyland Software Inc.'s cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

*Inherent limitations:*

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Hyland Software, Inc.'s principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. 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.

*Opinion:*

In our opinion, Hyland's controls over the system were effective throughout the period May 1, 2020 to October 31, 2020, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria, if the subservice organization applied the controls assumed in the design of Hyland's controls throughout the period May 1, 2020 to October 31, 2020.



Ernst & Young LLP  
December 23, 2020

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

December 23, 2020

We, as management of, Hyland Software, Inc. (Hyland) are responsible for:

- Identifying the Hyland Cloud Platform (System) and describing the boundaries of the System, which are presented in the Hyland Cloud Background section below
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in the section below
- Identifying, designing, implementing, operating, and monitoring effective controls over the Hyland Cloud Platform (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion
- Performing annual due diligence procedures for third-party sub-service providers and based on the procedures performed, noting deviations that prevents Hyland from achieving its specified service commitments

Hyland uses Amazon Web Service (AWS) (subservice organization) to provide physical hosting and data replication services for a subset of in-scope solutions. The Description includes only the controls of Hyland and excludes controls of AWS, however it does present the types of controls Hyland assumes have been implemented, suitably designed, and operating effectively at AWS (Attachment A). The Description also indicates that certain trust services criteria specified therein can be met only if AWS's controls assumed in the design of Hyland's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of AWS.

We assert that the controls over the system were effective throughout the period May 1, 2020 to October 31, 2020, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality, and privacy set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Hyland Software, Inc.

## Hyland Cloud Platform Background

Established in 1991, Hyland Software, Inc. (Hyland) is the developer of Enterprise Content Management (ECM) solutions design to help organizations streamline their document and content management processes and share information among employees, partners, and customers. In 2017, Hyland acquired Perceptive Software product lines. Hyland is based in Westlake, Ohio.

Hyland's core ECM solution 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 SaaS (Software as a Service) solutions, which include the OnBase, OnBase Accelerated Financial Reporting Management (AFRM), ShareBase, Guardian, and Perceptive hosted products and modules. Primarily, 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). 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). In addition to co-location deployment, Hyland deploys third-party cloud environments for customers purchasing select media streaming and ECM solutions. In this case, the third-party provides the physical network and infrastructure services that are used to deploy third-party cloud environments within the Platform. Hyland is responsible for selecting and administering the architecture, configuration, and other services required to support these hosting solutions.

### Services covered by this report

The Hyland Cloud Platform is composed 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 including those 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.

Hosting services may be provided to customers through an internet-enabled network and infrastructure that is owned by a third-party cloud provider. Hyland manages the servers, OS services, storage, and network access. Hyland is ultimately responsible for the architecture and deployment of the cloud environment used to deploy the Platform. Solutions can be deployed in domestic and international regions within the third-party cloud environment. Hyland has no direct access to the physical infrastructure of the third-party cloud provider and enforces these requirements via contractual agreements with the third party.

### 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, confidentiality, and privacy 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.
- ▶ Metadata 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.

### Risk Assessment

The process of identifying, assessing and managing risks is a critical component of the internal control system. The GCS GRC Team performs an annual risk assessment to identify, assess, and manage a variety of risks that impact Hyland's business. The risk assessment scope includes internal, external, third-party relationships such as vendors, contractors, and customers. During the assessment, threats to Information Security (which includes, but is not limited to, issues concerning availability, security, confidentiality, privacy, and data loss) are identified by the business owners and confirmed through interviews with subject matter specialists, and the risk from those threats is assigned a risk ranking. The results of the risk assessment are reviewed and approved by the GCS VP.

### 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.

### **Third-Party Cloud Provider**

Two of Hyland's production data centers are hosted at AWS facilities in Dublin, Ireland (AWIE) and Ashburn, VA (AWVA). This sub-service provider is responsible for physical hosting and data replication services (AWS). The system description includes only the controls of Hyland and excludes controls of AWS. The system description also indicates that certain trust services criteria specified therein can be met only if AWS's controls assumed in the design of Hyland's controls are suitably designed and operating effectively along with the related controls at the Service Organization. Hyland performs annual due diligence procedures for third-party sub-service provider including the review of available SOC reports and based on the procedures performed, nothing has been identified that prevents Hyland from achieving its specified service commitments.



## Attachment A

► Services Provided and Expected Controls

Hyland uses AWS to provide physical hosting and data replication services. The affected criteria are included below along with the expected minimum controls in place at AWS.

Criteria	Controls Expected to be in Place at AWS
<p><b>CC6.4:</b> 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.</p>	<p><b>Note: These controls apply only to AWS:</b></p> <p>Physical access to the computer rooms, which house the entity’s IT resources, servers, and related hardware, is restricted to authorized individuals through a badge access system or equivalent and monitored by video surveillance.</p> <p>Requests for physical access privileges require management approval.</p> <p>Documented procedures exist for the identification and escalation of potential physical security breaches.</p> <p>Visitors must be signed in by an authorized workforce member before gaining entry and must be escorted at all times.</p>
<p><b>CC9.1:</b> The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.</p>	<p><b>Note: These controls apply only to AWS:</b></p> <p>A data replication process is in place to back up customer data stored within the production environment.</p>
<p><b>A1.2:</b> The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.</p>	<p>Access to modify the data replication configuration is limited to authorized individuals.</p>
<p><b>P4.2:</b> The entity retains personal information consistent with the entity’s objectives related to privacy.</p>	

► Details regarding management’s monitoring control over the sub-service providers

Due diligence procedures are in place upon engagement, and at least annually, for third-party service providers according to the Global Cloud Services Policy Suite. The annual third-party vendor review includes obtaining and evaluating applicable SOC 2 report(s), an evaluation of financial stability, ability to meet contractual obligations, compliance and service obligations and expectations, and business continuity plans.