ENCYCLOPAEDIA BRITANNICA®, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE BRITANNICA® EDUCATION ONLINE SERVICES SYSTEM

FOR THE PERIOD OF FEBRUARY 1, 2023, TO JANUARY 31, 2024

Attestation and Compliance Services

INDEPENDENT SERVICE AUDITOR'S REPORT

To Encyclopaedia Britannica®, Inc.:

Scope

We have examined Encyclopaedia Britannica®, Inc.'s ("Encyclopaedia Britannica") accompanying assertion titled "Assertion of Encyclopaedia Britannica Service Organization Management" ("assertion") that the controls within the Britannica® Education Online Services system ("Online Services system") were effective throughout the period February 1, 2023, to January 31, 2024, to provide reasonable assurance that Encyclopaedia Britannica's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Encyclopaedia Britannica uses a subservice organization for cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Encyclopaedia Britannica, to achieve Encyclopaedia Britannica's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system 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.

Service Organization's Responsibilities

Encyclopaedia Britannica 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 Encyclopaedia Britannica's service commitments and system requirements were achieved. Encyclopaedia Britannica has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Encyclopaedia Britannica 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 systems 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 management's assertion is fairly stated, in all material respects. 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 risks that controls were not effective to achieve Encyclopaedia Britannica'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 Encyclopaedia Britannica'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.

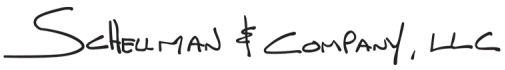
Inherent Limitations

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 Encyclopaedia Britannica's 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 Encyclopaedia Britannica's Online Services system were effective throughout the period February 1, 2023, through January 31, 2024, to provide reasonable assurance that Encyclopaedia Britannica's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



Chicago, Illinois
March 5, 2024

ASSERTION OF ENCYCLOPAEDIA BRITANNICA SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Encyclopaedia Britannica®, Inc.'s ("Encyclopaedia Britannica") Britannica® Education Online Services system ("Online Services system") throughout the period February 1, 2023, to January 31, 2024, to provide reasonable assurance that Encyclopaedia Britannica's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below 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 February 1, 2023, to January 31, 2024, to provide reasonable assurance that Encyclopaedia Britannica's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Encyclopaedia Britannica's objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 February 1, 2023, to January 31, 2024, to provide reasonable assurance that Encyclopaedia Britannica's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE ONLINE SERVICES SYSTEM

Company Background

Founded in 1768, Encyclopaedia Britannica®, Inc. (Encyclopaedia Britannica) has published a general reference encyclopedia in the English language for more than 250 years. Today, Encyclopaedia Britannica's institutional division (Britannica® Education) is focused on developing online learning resources for Kindergarten (K) – 12 classrooms, higher and further education institutions, including colleges and universities, and libraries. Britannica Education also supports schools and libraries with dedicated education consultants for K – 12 educator training and professional development services.

Encyclopaedia Britannica employs approximately 200 people, reporting to its headquarters in Chicago, Illinois, and is privately held by Encyclopaedia Britannica Holding S.A.

Description of Services Provided

The Britannica Education Online Services system (Online Services system) consists of a suite of database solutions, third-party access authentication services, and access control services for K – 12 schools, higher and further education institutions, including colleges and universities, and libraries, including the following:

Proprietary Database Solutions:

- Britannica Online School Edition™ – Digital encyclopedia for K – 12 schools.
- Britannica Online Library Edition™ – Digital encyclopedia for libraries.
- Britannica Online Academic Edition™ – Digital encyclopedia for higher and further education institutions.
- ImageQuest® – Database of three-and-a-half million rights-cleared images for K – 12 schools, higher and further education institutions, and libraries.
- Britannica Escolar™ – Digital, Spanish-language encyclopedia for grades K – 8.
- Britannica Moderna™ – Digital, Spanish-language encyclopedia for grades 9+ and higher and further education institutions.
- Britannica Original Sources™ – Database containing thousands of primary source documents across 12 subject areas.
- Britannica Online Japan™ – Digital, Japanese-language encyclopedia for K – 12 schools, higher and further education institutions, and libraries.
- Britannica Fundamentals!™ – Digital, early learning platform with literacy and math games, read-aloud books, drawing tools, and science exploration interactives for grades K – 2.
- Britannica Collective™ – Digital reading platform with a collection of nonfiction e-books for K-12 schools.
- Britannica LaunchPacks® – Digital platform that enables educators to build their social studies and science curricula using multimodal building blocks.
- LumieLabs® – Digital video creation and storytelling tool for K – 12 schools.
- Expedition: Learn!™ – Supplemental, digital curriculum resource that builds literacy while developing content-area knowledge in science and social studies for grades 3 – 8.
- Britannica Usage Statistics (Stats)™ – Britannica's product usage statistics reporting portal.

Third-Party Database, Access Authentication Services:

- Merriam-Webster's® Unabridged Dictionary – Encyclopaedia Britannica authenticated access to Merriam-Webster, Incorporated's subscription-based digital dictionary and comprehensive source of information on the English language.

- Encyclopaedia Universalis™ – Encyclopaedia Britannica authenticated access to Encyclopaedia Universalis' subscription-based digital, French-language encyclopedia for grades 9+ schools, higher and further education institutions, and libraries.
- Universalis Junior™ – Encyclopaedia Britannica authenticated access to Encyclopaedia Universalis' subscription-based digital, French-language encyclopedia for K – 8 schools.

Access Control Services:

- Learning Tools Interoperability® (LTI®) – An authentication method that uses the LTI standard published by IMS Global Learning Consortium.
- Shibboleth™ – An open-source authentication method that allows users to securely sign into Britannica's products without maintaining usernames and passwords.

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 services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

Encyclopaedia Britannica designs its processes and procedures related to the system to meet its objectives for the Online Services system. Those objectives are based on the service commitments that the organization makes to user entities, the laws and regulations that govern the provisioning of the Online Services system, and the financial, operational, and compliance requirements that the organization has established for the services. The Online Services system is subject to the relevant regulatory, industry, and data security requirements in which Encyclopaedia Britannica operates.

The security, availability, and confidentiality commitments to user entities are documented and communicated in the service agreement and security addendums. Specifically, these commitments include, but are not limited to, the following:

<u>Security</u>

- Protect customer data against unauthorized access, use, disclosure, modification, and destruction with the use of role-based, least privileged access.
- Require employees to complete security awareness training upon hire and annually thereafter.

<u>Availability</u>

- Perform data backups on a periodic basis to support system recovery.
- Maintain system availability within the production environment 99.5% of the time.
- Perform ongoing maintenance of the in-scope production systems.

<u>Confidentiality</u>

- Retain and/or dispose of confidential information in accordance with guidelines and contractual requirements.
- Encrypt confidential information at rest and in transit.

Encyclopaedia Britannica establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. This includes using encryption technologies to protect system user data both at rest and in transit, implementing background screening for certain personnel, performing periodic vulnerability scans and penetration tests, authenticating personnel using

strict password enforcement mechanisms, revoking access to personnel upon termination, and ongoing monitoring to ensure the achievement of the related objectives.

Such requirements are communicated in Encyclopaedia Britannica's policies and procedures, system design documentation, and service agreements and security addendums. Information security policies define an organization-wide approach to how systems and data are protected. These include policies pertaining to how Encyclopaedia Britannica's systems are designed, developed, and operated, its internal business systems and networks are managed, and its employees are hired, trained, and supervised. 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 the Online Services system.

In accordance with the assertion and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

The infrastructure and software supporting the Online Services system is maintained at third-party data center facilities operated by Amazon Web Services, Inc. (AWS) in the following regions: United States (US) East (N. Virginia), US West (N. California), Asia Pacific (Singapore), and South America (Sao Paulo) regions. Encyclopaedia Britannica operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure (i.e., physical infrastructure, geographical regions, availability zones, edge locations, operating, managing, and controlling the components from the host operating system, virtualization layer, and storage), and Encyclopaedia Britannica is responsible for the security of the platform deployed in AWS (i.e., customer data, applications, identity access management, operating system, network, virtual firewall, and network traffic). The Online Services system is housed on servers running Amazon Linux operating systems, utilizing PostgreSQL and Oracle databases. Additionally, the Amazon Simple Storage Service (S3) is utilized to support the system.

The in-scope infrastructure consists of multiple systems as shown in the table below:

Primary Infrastructure			
Production System	**Business Function Description**	**Platform**	**Physical Location**
Active Directory	Used to manage network user accounts and authentication requirements.	Active Directory on Google Cloud	USA
Identity and Access Management (IAM)	Used to manage access to cloud infrastructure and resources, including the creation and management of users and groups, and use of permissions to allow and deny their access to resources.	Amazon IAM	US East (N. Virginia), US West (N. California), Asia Pacific (Singapore), and South America (Sao Paulo)
Servers	Used for application delivery and to run code.	Amazon Linux / Elastic Compute Cloud (EC2)	
Databases	Used to store, retrieve, and manage data input into the system.	PostgreSQL / Oracle	
Storage System	Used to store and retrieve file data, including files uploaded by customers.	Amazon S3	
Firewall System	Protects the network perimeter and production environment and limits inbound and outbound access.	Amazon EC2 Security Groups / CloudFlare	

Primary Infrastructure			
Production System	**Business Function Description**	**Platform**	**Physical Location**
Encyclopaedia Britannica Solutions	Portfolio of applications delivered as a Software-as-a-Service (SaaS) to assist clients with research and knowledge-gathering activities.	Amazon Linux / EC2	US East (N. Virginia), US West (N. California), Asia Pacific (Singapore), and South America (Sao Paulo)

Encyclopaedia Britannica uses additional tools/utilities to support the in-scope systems. The ancillary systems listed below are purchased products and may support some facets of the delivery of services described. These utilities are covered within the scope of the report to the extent they support achieving the objectives and were not subject to information technology general controls (ITGC) testing.

Ancillary and Supporting Systems	
Software/Utility	**Business Function Description**
Jira	Used for tracking application issues and their resolution.
Confluence	Dynamic team workspace and collaboration tool.
GitHub	Software development platform for source code and development projects.
Spiceworks	Used for Helpdesk requests for IT services and tracking incidents from detection to response and resolution.
osTicket	Used for submitting requests to deploy application, update database, upgrade system software, and otherwise process data.
CircleCI	Continuous integration (CI) tool used to support DevOps practices.
Netlify	Development platform that includes build, deploy, and serverless backend services for web applications.
Salesforce	Customer relationship management (CRM) tool used for centralizing sales, customer service, marketing, and analytics initiatives.

People

The personnel supporting the Online Services System include, but are not limited to, the following:

- Executive Committee – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
- Human resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisition, employee retention, compensation, employee benefits, performance management, employee relations, training, and development).
- System operations (SysOps) / IT – responsible for operating, deploying, updating, and monitoring the Online Services system as well as performing security maturity assessments.
- Software development – responsible for coding, building, testing, and debugging the Online Services system as well as the design and update of new and existing services.
- Legal – responsible for managing employee and contractor engagement, customer contracts, security assessment requests (including vendors), and other legal and regulatory compliance requirements.

- Sales, product management, and customer service – responsible for product demonstrations to customers and sales-related activities as well as troubleshooting customer issues.

Procedures

Access Authentication and Authorization

Access to system information, including confidential data, is protected by authentication and authorization mechanisms. The ability to administer the in-scope systems is restricted to user accounts accessible by authorized personnel. Predefined user groups are utilized to assign role-based access privileges and segregate access to data within the in-scope systems. IT personnel are responsible for assigning and maintaining access rights to the in-scope systems.

The in-scope systems are configured to authenticate users with a user account and enforce a combination of minimum password requirements including minimum length, complexity, age, lockout, and history as well as multi-factor authentication (MFA). Encrypted virtual private networks (VPNs) are utilized for remote access for the security and integrity of the data passing over the public network. To authenticate to the in-scope systems, engineers and developers are required to first authenticate to the Google Cloud active directory. Once authenticated, users leverage centralized authentication via AWS IAM to subsequently authenticate to the production servers, databases, storage system, firewall, and web applications.

Access Requests and Access Revocation

To ensure that access to confidential data is restricted to appropriate personnel, a formal provisioning and deprovisioning process has been established for managing user accounts and controlling access to Encyclopaedia Britannica's resources within the production environment. Upon a candidate's acceptance of a written offer from the corresponding manager, the manager notifies HR in writing to confirm their approval of the same and authorize HR to initiate Encyclopaedia Britannica's new-employee access provisioning process by submitting an access request ticket within the ticketing system. IT personnel subsequently create new user accounts, granting access according to the principle of least privilege.

Upon notification from HR of an employee termination, a termination ticket is created within the ticketing system and notification of the termination is communicated to the appropriate departments via the ticketing system (i.e., system owners, IT, etc.). Upon receipt of the termination notification, the notified departments work together with IT to ensure the terminated employee's access is revoked as of their termination date.

A meeting is held on a bi-weekly basis to review privileged user access to verify that accounts are revoked for terminated employees, administrative access privileges are assigned to authorized personnel, and system access levels are commensurate with current job responsibilities. When a user is identified who no longer requires access to the in-scope systems, their access is subsequently revoked.

Device and Network Security

Firewall systems, consisting of a perimeter firewall and AWS security groups, are in place to block unauthorized inbound network traffic from the Internet and configured to deny any type of network connection that is not explicitly authorized by a rule. To protect data while in transit, the Online Services system's customer sessions are transmitted utilizing HTTPS and the TLS encryption protocol. TLS encryption is utilized for web communication sessions as part of the default installation to ensure a secure transmission over the Internet. Additionally, encrypted VPNs are utilized for remote access for the security and integrity of the data passing over the public network.

Customer data is stored in an encrypted format and access privileges to the cryptographic keys stored within the key management system are restricted to authorized personnel. Additionally, Encyclopaedia Britannica utilizes full disk encryption on employee workstations.

Change Management

Documented change management and software development lifecycle (SDLC) policies and procedures are in place to guide personnel in the authorization, testing, approval, and implementation of changes into the production environment. The goals of the policies include, but are not limited to, the following:

- Ensure delivery of quality systems which meet or exceed customer expectations.
- Provide a framework for developing quality systems using an identifiable, measurable, and repeatable process.
- Establish a project management structure to ensure that each project is effectively managed through the lifecycle.

Encyclopaedia Britannica has defined the following SDLC phases, which describe the work products and documents created, reviewed, refined, and approved within each phase:

Phase	Definition
Initiation	The change process kicks off when management determines that it is necessary to enhance a business process through the application of information technology. The purpose of the initiation phase is to: • Identify and validate an opportunity to solve a business need • Identify significant assumptions and constraints on solutions to that need • Recommend the exploration of alternative concepts and methods to satisfy the need
Project Viability	Product management and business personnel jointly determine whether the project should move forward. If approved, the aforementioned personnel produce a project plan with timelines and budget estimates for development.
Requirements Analysis	Product management personnel define the functional user requirements to a level of detail sufficient for system design to proceed based on the high-level requirements identified in the previous phases.
Design	SysOps and development personnel design the system with elements to satisfy the functional requirements identified in the previous phase, which include, but are not limited to, the following: • Identifying potential risks and defining mitigating design features • Performing a security risk assessment • Allocating processes to resources
Development & Testing	Development personnel translate the functional requirements into system components and request SysOps personnel to push the updates into a testing environment to test for error, bug, and various compliance checks. Quality Assurance (QA) personnel then test the system in several testing environments before deploying it to the production environment.
Acceptance & Implementation	SysOps personnel deploy the tested updates into production and QA personnel perform post-implementation testing until the system is operating in accordance with the defined user requirements.
Operations & Maintenance	SysOps personnel monitor the system for continued performance in accordance with user requirements.

Change management meetings are held on a weekly basis involving members of the development, QA, SysOps, and executive technology leadership teams to discuss ongoing and upcoming changes and releases.

Encyclopaedia Britannica utilizes a ticketing system to document and track the various stages and lifecycle of changes from request through implementation. Changes made to in-scope systems are authorized, tested when applicable, and approved prior to implementation. Upon authorization, development personnel begin development in the software development platform that enables development personnel to check-out different versions of the code for editing as well as rollback capabilities to ensure they can revert the software back to the last known good

state should a change impair the system. Additionally, the software development platform is configured to require automated smoke testing that ensures pull requests meet predefined requirements.

The software development platform additionally utilizes branch protection rules to enforce multiple, independent approvals of code changes for merge requests from two distinct user groups. By default, branch protection rules disable forced pushes to the matching branches and prevent the matching branches from being deleted. These rules further protect subsequent branches, and ultimately the master production branch, from forced pushes and deletion. Write access to the software development platform is restricted to authorized personnel. Once a given change has been through each stage of the lifecycle, the VP of engineering and senior systems engineer evaluate the change before the change is migrated to the production environment.

Encyclopaedia Britannica utilizes an automated continuous integration and continuous deployment (CI/CD) pipeline to minimize errors and help ensure the integrity of changes. CI processes automatically build, test, and integrate code changes within a shared repository, while CD processes automatically deploy changes to consumers directly by relying upon rigorous testing tools and a mature testing culture. Additionally, the CI/CD pipeline offers code resilience through test coverage, observability tooling, and feature flags, as well as code security through permission checks and a virtual paper trail for investigating and resolving failures and non-compliance events. Upon receiving approval, authorized personnel migrate the change to production. To ensure that changes made within the test environments do not affect changes in the production environment, the production environment is logically segmented from the development and test environments.

Encyclopaedia Britannica operates within a DevOps model where certain development personnel require elevated access to the production environment. As such, a change monitoring platform is utilized to monitor for suspicious events and is configured to notify IT personnel via e-mail for investigation and resolution in the event unexpected/unscheduled changes are identified, including for changes that were developed or deployed by personnel outside of the dedicated teams or for changes deployed outside of normal working hours. Additionally, the change monitoring platform notifies various IT personnel in real time whenever a change is migrated to the production environment.

Data Backup and Disaster Recovery

An automated backup system is utilized to backup production databases on a daily basis. The automated backup system is configured to notify IT personnel on a daily basis regarding the success or failure of backup jobs. IT personnel review the daily backup reports, investigate the cause for any failed backup jobs, and track the resolution of noted errors.

An automated replication system is used to replicate backups on a continuous basis across multiple availability zones and regions. Additionally, database backup restoration procedures are tested on a semi-annual basis to test the recovery plan procedures.

A disaster recovery plan is in place to address the framework in which a business disruption would be managed to minimize the loss of vital resources throughout the organization. The purpose of Encyclopaedia Britannica's disaster recovery plan is to define the baseline disaster recovery plan to be developed and implemented to describe the process to recover IT systems, applications, and data from any type of disaster that causes a major outage, as well as to guide personnel in procedures to protect against disruptions caused by an unexpected event. The disaster recovery plan is additionally tested on a semi-annual basis to help ensure the recoverability of operations in the event of a disaster.

Incident Response

Documented incident response and escalation procedures are in place to guide personnel in evaluating security events, understanding, containing, remediating, and communicating security incidents, and in the identification, development, and implementation of activities to recover from identified security incidents. The procedures are communicated to employees via Encyclopaedia Britannica's intranet.

Encyclopaedia Britannica defines an incident as an event that violates Encyclopaedia Britannica's policies related to information security, network security, and office security, and threatens the security, confidentiality, or availability of information resources. Furthermore, Encyclopaedia Britannica classifies incidents according to the following severity levels:

Severity	Description	Examples
Low	Incident where the impact is minimal.	• E-mail spam • Isolated virus infections
Medium	Incident where the impact is significant.	• Delayed or limited ability to provide services or meet Encyclopaedia Britannica's mission • Delayed delivery of critical e-mail or data transfers
High	Incident where the impact is severe.	• Disruption to the services and/or performance of Encyclopaedia Britannica's mission-critical functions • Information resources have been compromised • A virus or worm has become widespread
Critical	Incident where the impact is catastrophic.	• Shutdown of Encyclopaedia Britannica's systems • Information resources have been compromised and published publicly • Safety systems are unavailable

An incident response team (IRT) is in place to determine the scope and risk of, respond to, communicate the results of, and reduce the likelihood of reoccurrence for incidents. Additionally, the IRT is required to complete training on an annual basis to prepare to respond to an actual incident, should one occur, by following the defined incident response workflow:

- Detect and respond – IT personnel utilize security tools to detect suspected events and analyze the events to determine whether they are incidents.
- Analyze and confirm – The CTO performs static and dynamic analyses of the malicious code, reviews system boundary protections, and determines the breadth and depth of the attack.
- Escalate – The IRT escalates the confirmed incident to departments and personnel according to the incident severity from Low (IT department) to Critical (CTO, CFO, and CEO, as needed).
- Contain – The CTO and IRT together perform containment activities that include, but are not limited to, shutting down compromised systems and logically isolating the cause of the incident.
- Preserve evidence – The IRT provides forensic consultants with access to internal systems to evaluate how the incident occurred, the types of resources involved, and the organizations impacted.
- Recover – The CTO and IRT restore internal systems to normal operations from backups or by rebuilding systems from an Encyclopaedia Britannica-approved baseline.
- Report and communicate – The IRT works with the legal team and Executive Committee to determine necessary communication to employees, those impacted by the incident, the public, and law enforcement or regulatory bodies as needed.
- Post-incident activities – The IRT reviews the aforementioned incident response activities and answers questions such as which parts of the process worked as intended, was the IRT prepared for the incident, and what corrective actions can be implemented to prevent future incidents.

Once an event is identified, Encyclopaedia Britannica leverages a ticketing system to document security incidents, responses, and resolution. Included within incident tickets are the incident status, priority, and description. Additionally, management meetings are held as needed but at least annually to discuss potential security events and actions to prevent or address them as well as corrective measures to help ensure that incidents are resolved.

Finally, the IRT is required to complete data breach response training on an annual basis to confirm their understanding regarding evaluating security events and review lessons learned from previous incidents.

System Monitoring

IT personnel actively monitor the production systems for issues in order to ensure system availability. Enterprise monitoring tools are utilized to monitor system traffic and are configured to alert IT personnel via e-mail when certain predefined events occur, such as downtime and errors. Additionally, security monitoring tools are utilized to monitor system logs and events to detect anomalies indicative of malicious acts, natural disasters, and errors. Upon receiving alerts, IT personnel determine whether any additional action should be taken.

IT personnel and third-party vendors perform vulnerability scans daily and penetration tests annually, respectively, to identify new vulnerabilities and susceptibilities to new vulnerabilities. Issues that are identified are communicated to relevant parties, tracked, and monitored through resolution.

Data

The Online Services system is dependent on the use of a variety of data within the system to improve workflows for customers. The types of data that might be collected, managed, processed, and stored include, but are not limited to, curriculum and usage statistics. Student, teacher, and customer information such as name, address, billing, location, e-mail, and log-in credentials is managed via the web applications. As students and teachers complete online learnings, they can save their progress in training modules within the web applications. Refer to the Description of Services Provided section above for more information on data used within the system.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Examples**	**Classification**
Information that, if made public, will not harm Encyclopaedia Britannica in any way.	• Materials published at britannicaeducation.com, including learning curriculum and webinars	Public
Unauthorized access may cause minor damage and/or inconvenience to Encyclopaedia Britannica.	• Business contact information, such as IP address • Information pertaining to Encyclopaedia Britannica's security program	Internal
Unauthorized access to information may cause considerable damage to the business and/or Encyclopaedia Britannica's reputation.	• Student, teacher, and other customer contact information • Customer usage statistics within the system	Confidential
Unauthorized access to information may cause catastrophic damage to the business and/or Encyclopaedia Britannica's reputation.	• Customer credit card and checking account information	Restricted

Significant Changes During the Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

Subservice Organizations

The cloud hosting services provided by AWS were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone or in combination with controls at Encyclopaedia Britannica, and the types of controls expected to be implemented at AWS to meet those criteria.

Control Activities Expected to be Implemented by AWS	Applicable Trust Services Criteria
AWS is responsible for implementing controls to manage logical access to the underlying network and virtualization management software for its cloud hosting services where production systems reside.	CC6.1 – CC6.3 CC6.6 – CC6.7
AWS is responsible for implementing controls to restrict physical access to facilities and protected information assets.	CC6.4
AWS is responsible for implementing controls to render data unreadable, when directed by Encyclopaedia Britannica, prior to the decommissioning of physical assets.	CC6.5
AWS is responsible for implementing controls to protect against environmental vulnerabilities and changing environmental conditions.	A1.2

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the Online Services system.