Pearson Clinical Assessments Information Security Program

PEARSON ASSESSMENTS
Information Security Office
2020.12.01 v1.8

Table of Contents

Information Security Program

Overview

Information Technology (IT) systems are trusted only when the data and information they contain are kept confidential and secure. And this can only happen when a comprehensive information security program governs its design, development, and delivery of the services they provide. Pearson takes the privacy and security of customer and company information seriously. To protect sensitive assessment data, such as test items and student confidential information, Pearson employs recognized industry standard security measures to safeguard the confidentiality, integrity, and availability of customer data and the services we provide.

Our information security policies and standards are based on the ISO/IEC 27001 information systems security framework, and we continue to work toward also aligning our program with the NIST catalogue of security controls. This evolving alignment with NIST reflects our ongoing commitment to ensure our information security program remains current and appropriate to address the evolving threats to information security and data privacy.

In support of this, Pearson's technology teams are encouraged to continually improve their skills and gain professional recognition for their mastery of them. To this end, the teams that support and maintain the systems that provide services to our customers collectively hold numerous professional certifications in the areas of AWS Architecture, AWS DevOps, AWS Development, Splunk Log Management, Jenkins Deployment, Java Development, Data Science Analytics, Information Security, Information Privacy, Project Management, and Agile Scrum Mastery, just to name a few. Because of our teams' well-established experience and credibility as technology professionals, our more senior level staff regularly sit on discussion panels and speak at local, regional, and national conferences.

System Security and Resiliency

In accordance with security best practices, multiple layers of security exist in the computing environment to reduce the risk of unauthorized exposure of customer data. These protections include not only preventive controls designed to stop security incidents from happening, but also detective controls to inform us in the unlikely event a security control failure occurs. Along with the resilient and reliable design of our assessment platform, Pearson leads the industry in its ability to protect against and mitigate the effects of distributed denial of service (DDoS) attacks.

Staff Training Requirements

When employees and staff augmentation resources begin working for Pearson, they must sign an acknowledgement of their obligation to adhere to the Pearson Global Information Security Policies and follow the company's implementation guidelines and standards. On an annual basis, members of the Pearson workforce must complete information security training that is designed to ensure they not only maintain awareness of their responsibility to protect customer and company information, but also to help ensure they are educated regarding changes in the ever-evolving information risk universe.

Need to Know and Least Privilege

Pearson provides access to systems based on *need to know* and in accordance with the *principle of least privilege.* If a workforce member does not have a business need for access, they do not get it. And where access is authorized, user accounts are assigned the minimum level of privilege necessary for their role.

These principles also extend into the assessment services we provide. Customer staff who have been assigned to administration roles in service solutions have the ability to place staff into specific roles, with privileges appropriate to them. In this way, administration of the assessment platform can conform to role-based access needs of each customer.

Entitlement Review

A review of users and the permissions assigned to them is performed periodically, as well as when staff change positions and employment statuses change. This helps to ensure on-going adherence to our commitment to grant access based on *need to know* and according to the *principle of least privilege*.

Data Classification

Pearson's Global Information Security Policies and Standards define a four-tier data classification level (DCL) scheme. DCL4, the highest classification tier, denotes data subject to data privacy regulation and requires the most stringent information security controls. Given the nature of the services we provide to customers, practically all of our systems are designed with the baseline assumption that the data it maintains and processes is DCL4.

Governance, Risk, and Compliance

Pearson's executive management is committed to ensuring the customer and company data we hold is not only secure and confidential, but also meets applicable regulatory requirements. This requires ensuring appropriate governance over matters of information security risk and privacy compliance. To this end, Pearson Assessments has an established cadence for evaluating the risk landscape for ongoing compliance to internal and external security and privacy requirements. This includes an internal risk assessment process that evaluates the threat landscape and determines where new controls need to be put in place, as well as existing controls strengthened.

Audits

Annually, certain systems within our assessment platform undergo an external Service Organization Control 2 (SOC2) audit, adhering to the Association of Independent Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No.18 (SSAE 18), the most recent version, which became effective May 1, 2017.

Whether performed internally by trained and experienced staff or externally by an independent third-party audit firm, if gaps or weaknesses in our security and privacy controls are identified, they are reported to the Pearson Assessments Information Security Office (AISO), who then works with business, legal compliance, and technical management to identify and implement appropriate remediation solutions.

Remediation

Remediation efforts focus on reducing risk to an acceptable level or eliminating it altogether. These projects are typically assigned a technical project manager (TPM), who works with the appropriate subject matter experts (SME) and stakeholders to develop a remediation plan, determine roles and responsibilities, establish target dates and milestones, and provide ongoing oversight throughout the life of the project. Relevant documentation is created and published internally by members of the project team, ensuring effective communication and appropriate visibility of remediation efforts and changes.

Corporate Governance

Pearson's Global Corporate Information Security Office (CISO) defines, publishes, and socializes information security ISO-aligned policies and standards. The CISO has further defined organizational roles to carry out the information security mandate within each line of business (LOB). Through roles focused on the various aspects of

information security, the policies and standards propagate to the individual business units that make up that region's component of the LOB in which they operate. The Pearson Assessments LOB maintains a dedicated information security office team to support not only the adoption of Pearson's Global Information Security Policy, but also to ensure customers' specific information security requirements are met.

Security Incident Management & Response

Executive management supports a defined security incident management team with direct responsibilities for the management and response to security Incidents. Only authorized, trained personnel within this group are given responsibility for incident management and response.

Responsibilities and procedures are established and documented for the Incident Management Team. These include procedures for:

- monitoring, detecting, and reporting security events.
- assessment, classification, and decision on security events.
- response, escalation, recovery, and communication.
- for timely collection, protection and preservation of relevant system and application logs, and all other evidence pertaining to the incident in compliance with technical forensic needs and applicable legal requirements.

Security Incidents are categorized based upon the incident severity. Procedures exist and provide guidance on the proper handling of any potential incident, regardless of severity level. The severity levels range from Critical events with business disruption on a massive scale, to Low-severity events that are isolated to a small number of individuals, systems, or processes.

All communication on security Incidents, both internal and external are strictly controlled and only initiated by authorized staff, which is done in consultation with Pearson Legal and Pearson Corporate Affairs.

Regulatory Compliance

As with any company that operates in multiple countries, compliance to the laws of each jurisdiction play a central role in the definition of its policies, standards, and guidelines. Pearson takes this responsibility seriously, ensuring the security and privacy of customer data conforms not only to the contractual obligations of its customers, but also to the compliance requirements of the jurisdictions in which they operate.

To this end, Pearson Assessments maintains trained, qualified professionals whose responsibilities include staying abreast of applicable regulatory requirements. By the very nature of the services we provide, the privacy of student data sits at the top of our information security program's list of high-value, critical information assets. As

such, everything we do carries a measure of consideration for ensuring we meet the obligations of Federal, State and Provincial data privacy laws

Data Residency

Pearson respects the data privacy laws of the jurisdictions in which we do business. We recognize that data residency has become an important consideration when selecting a service provider who will handle confidential and sensitive information—particularly personal identity information. To this end, all of the data collected, stored, processed, maintained, and transmitted by Pearson Assessments' systems reside within the jurisdictions outlined in the governing customer contract. If the data is allowed to only reside and be transmitted within a certain country or jurisdiction, Pearson will work with our customers to identify an appropriate solution to meet data residency requirements. Our use of Amazon Web Services affords us the flexibility to limit where data is stored and the destinations to which it is transmitted.

Cyber-Attack and Exfiltration Defence

Pearson employs a number of different methods to mitigate the risk of unauthorized access to our systems:

- All data transmitted externally is encrypted.
- All item content payloads are encrypted end-to-end using AES encryption.
- All student/patient responses are encrypted using AES encryption, and use a key that is different from the key used to encrypt content payloads.
- Account and password controls meet accepted industry standards for length, complexity, re-use, expiration, and log-on retry lockout.
- Accounts are only given the least set of privileges needed to perform authorized activities.
- Anomaly detection built into the application allows Pearson engineers to detect unexpected or potentially harmful application behaviour in near-real-time.

Antivirus and Malware Controls

All workstations and servers on the internal Pearson network make use of installed antivirus and malware detection software. Malware definition updates occur automatically, ensuring all workstations in the Pearson network can detect and quarantine known malicious software. Additionally, the annual information security training mentioned above, includes modules to educate our workforce to such things as social engineering and phishing.

Windows servers, because of the virtually ubiquitous use across the globe and its foundational similarity to its desktop OS counterpart, employ anti-virus/anti-malware software—particularly for any servers that are directly accessible from the Internet.

The operating system that is most prevalent in the design and architecture of the systems providing our assessment services are variants of Linux (*e.g.,* Amazon Linux, CentOS, Ubuntu), which have been risk assessed in conjunction with system architecture.

The risk assessment determined that stability and performance of the Linux variants were at greater risk when anti-malware tools were deployed. For this reason, a defence-in-depth design that precludes direct Internet access to the servers in the cloud environment has been implemented, thus dramatically reducing the risk of malware infection compared to the risk of destabilizing and/or degrading the environment. We continually monitor the risk landscape for changes in technology and cyberattack vectors that would impact this risk decision.

Wireless Network Security

Pearson's wireless network requires users to be members of Pearson's Active Directory trusted domain to ensure only authorized users can connect to the internal network. All transmissions over the wireless network make use of strong encryption. Further, since our assessment platforms exist 100% in the cloud, the Pearson wireless network does not have a direct connection to them.

System Maintenance

As with all information technology solutions, patches, updates, and fixes to unexpected events need to be deployed from time to time. Pearson establishes regular maintenance windows and coordinates with customers as needed to ensure minimal interruption to assessment services. Our goal is to make sure customers know in advance about any update or system downtime that may be necessary.

Vulnerability Management & Patching

Patches are released periodically by the manufacturers of Pearson's underlying system components, devices, platforms, and applications. Each patch undergoes an assessment to determine applicability, risk, and whether or not mitigating controls already exist.

If the assessment determines a patch to be necessary, it is applied in a test environment where it is regression tested to verify the patch works and does not negatively impact the assessment platform. Once regression testing completes, user acceptance testing (UAT) is performed to confirm the platform is fully operational. If the patch passes UAT, then we send notification, as applicable, to affected customers and release the patch into the production environment through a standardized change control process.

Change Management

Our change management processes are designed to reduce the risk of service interruption and degraded performance, as well as to ensure all changes made to production system are authorized. Rigorous adherence to change controls throughout the system development lifecycle (SDLC) works to ensure successful implementation on the first attempt.

The process includes:

- acknowledgement and record of changes
- assessment of the impact to the costs, benefits, and risks of proposed changes
- management approval
- management and coordination of implementation
- closure review

Web Components and Transmission

Pearson employs HTTPS, an encrypted method of passing data over the Internet via web-based systems. Transport Layer Security (TLS) works with HTTPS to ensure the data is encrypted as it passes from our servers to the clients. Web-based services and application layer interface (API) calls use industry standard representational state transfer (REST) architecture to appropriately constrain and control data as it passes between components and across connections.

File Transmission

Pearson's assessment platforms provide for the ability to transfer student data to customer-authorized destinations via multiple methods, based on the needs of the customer. Such methods of file transfer include:

- Synchronous:
  - Pearson's cloud-based solution leverages customers' ability to establish connections directly to the cloud storage repositories where extracts of the data can be placed. Customers are issued authentication and access credentials, as well as instructions describing how to use this solution.
  - Secure FTP can be used, as well, enabling customers to pull data from SFTP servers over an SSH connection using commonly available SFTP client software.
- Asynchronous:
  - Based on the needs of customers, Pearson is often able to meet specific data transfer requirements through a collaborative effort to define and implement a suitable solution.

System Logging

Pearson's assessment platforms possess extensive logging and monitoring capabilities. Some logs directly feed real-time monitoring systems and dashboards, while other logs facilitate troubleshooting and forensic analysis. Examples of logged events include, but are not limited to:

- User provisioning and access level assignment
- Logon and logoff success and failure events, along with date and time
- Database access
- Transmission of data and files
- System errors, aborts, and other events to enable detection of anomalous behaviours

System Monitoring

Although we constantly monitor for anomalous system behaviour, special care is taken during student testing cycles to provide the highest possible levels of availability and performance. Our monitors watch for anomalous activity throughout the entire system, not just at the application or network layers. If suspicious activity shows up on our systems, our system triggers alerts to our technical staff for investigation and handling.

In addition to overall, system-wide monitoring for suspicious and anomalous system activity, we also make sure our systems remain at current patch levels. We use a suite of tools to scan for vulnerabilities at the network, operating system, platform, and application layers.

Service Delivery Analytics

Our assessment solutions include extensive logging features, which enable detailed performance and test activity analytics, particularly as it regards such things as the type of browser, IP addresses, operating system type, and usage statistics. Pearson maintains a dedicated system status dashboard for each program detailing real-time status for all key technology services involved in the given assessment delivery chain. Industry standard web analytic services collect statistics to provide a comprehensive view into technology and platform usage.

Dependable, Scalable, and Resilient Architecture

Overview

A successful testing experience for each student requires technology that is not only secure, but also dependable, scalable, and resilient. Pearson's assessment platforms meet these requirements through the use of cloud-based hosting infrastructure, system isolation, and elastic compute power. We augment this with careful 24x7 tracking of system performance metrics.

We deliver consistent testing and assessment performance, even when subject to widely fluctuating demands on our environment, where the load can swing rapidly from periods of low demand to high. Our technology and architecture allow us to rapidly adjust to sharp changes in system demand, increasing capacity at the time demand occurs, instead of waiting to perform scale-up operations during off-hours. Because of this, students and teaching staff can focus on learning and teaching, instead of on the technology that enables them.

Cloud-based Architecture

Hosting our solutions in a virtual private cloud (VPC) affords our customers with the quality, security and scalability they expect. We have designed our platforms to be cloud-native and dynamically scalable.

Security Features

Advanced security measures, such as at-rest and in-transit data encryption, IP-based and identity-aware network filtering, web application firewall capability, industry standard network access controls and authentication processes, increased flexibility to provide data access to authorized users...in short, customer confidential and personal identity information, along with test items, student/patient responses, and other data considered sensitive or subject to regulatory compliance are protected with the most up to date technologies available. This is in addition to ensuring the data is encrypted from end to end.

Scalability

Virtually unlimited scalability gives Pearson the ability to quickly meet the resource demands during peak testing volumes, which ensures consistent performance for students and teachers when they need it most.

Resiliency

Redundancy and fault-tolerance form the foundation of all our assessment platform components. If one component of the system experiences problems, the platform shifts traffic to other servers in configured availability zones. Availability zones can be equated to datacentres, which are geographically separated from one another. This geographic separation is often referred to in the industry as the “air gap.” This sustains not just high availability through automatic load balancing, but also high resiliency against disaster events. And, equally important, ensures a consistent performance experience. This approach allows us to provide secure, high quality services even under the most demanding workloads and threat conditions.

Auto-scaling

In addition to the use of availability zones, we build auto-scaling capabilities into each customer critical system we provide. Based on real-time load and incoming monitoring data, compute capacity dynamically increases to handle whatever the processing load demands. When auto-scaling kicks in, new servers get spun up and undergo a series of automated quality checks before coming fully online to serve customer traffic. In this way, the infrastructure dynamically scales to give our customers stable, reliable service.

Network Control

Pearson’s approach to standing up and provisioning our systems in the cloud affords us the ability to maintain full control of incoming and outgoing data access traffic on a per-system basis. Instead of relying only on a centralized firewall perimeter, as is typical in brick-and-mortar datacentres, our cloud-based architecture gives us increased cybersecurity protection through more granular control over what traffic is allowed in and out of the cloud. The VPCs that host our systems are isolated from other public cloud services, as well as from the public Internet. Because of these isolation and network segmentation options, customer data gains an inherently higher level of protection and isolation.

Accessibility

VPCs are, by definition, hosted in an Internet-accessible cloud environment, which negates the need for private extranet links to be created between Pearson and its customers. This allows us and our customers to avoid the costs associated with specialized network services and connections.

Open Source Tech Stack

We use an open source technology stack, which dramatically reduces software costs compared to our competition. It gives Pearson the ability to use the most robust, affordable, and customizable solutions available in the technology market today.

Disaster Recovery and Resiliency

Disaster declaration is governed by the decisions of the Disaster Response and Recovery Team, which is formed at the outset of any system-wide or company-wide event that disrupts service and thereby threatens the confidentiality, integrity, or availability of valuable information assets. Pearson's Disaster Recovery and Incident Management policies provide high-level guidance regarding the classification of events and defines four severity categories, as follows:

- Critical – Level 1 Events that have the potential to disrupt business on a massive scale, or have material legal, strategic, operational or financial implications. All suspected or known personal data breaches must be classified as Critical – Level 1.
- High – Level 2 Events that have the potential to disrupt business on a large scale, or have significant legal, contractual, or financial implications.
- Moderate – Level 3 Events likely to cause service disruptions to isolated groupings of systems or processes and have limited legal, strategic, operational or financial implications.
- Low – Level 4 Events isolated to a small number of individuals, computers or processes that are unlikely to have any meaningful impact to the organization.

With regard Disaster Resiliency, Pearson replicates all data, systems, and components across multiple availability zones to maintain physically redundant and geographically-dispersed replicas of the production environment. This dramatically reduces the risk of experiencing service-impacting events associated with such events as fire, flood, earthquake, and other similar events. The use of VPCs, elastic computing, and the services offered our cloud provider, allows for physical and logical redundancy that is unmatched in the industry. The disaster recovery procedures, inclusive of automated services and manual actions, exist in disaster recovery runbooks. This documentation is version-controlled and kept up to date by trained Pearson staff.

Data Backup

In traditional backup methods, a full backup of the data is taken only when system loads are low, such as during the night on weekends. During the week, the traditional method typically only backups the data that changed each day, thereby requiring longer and more complex restore processes.

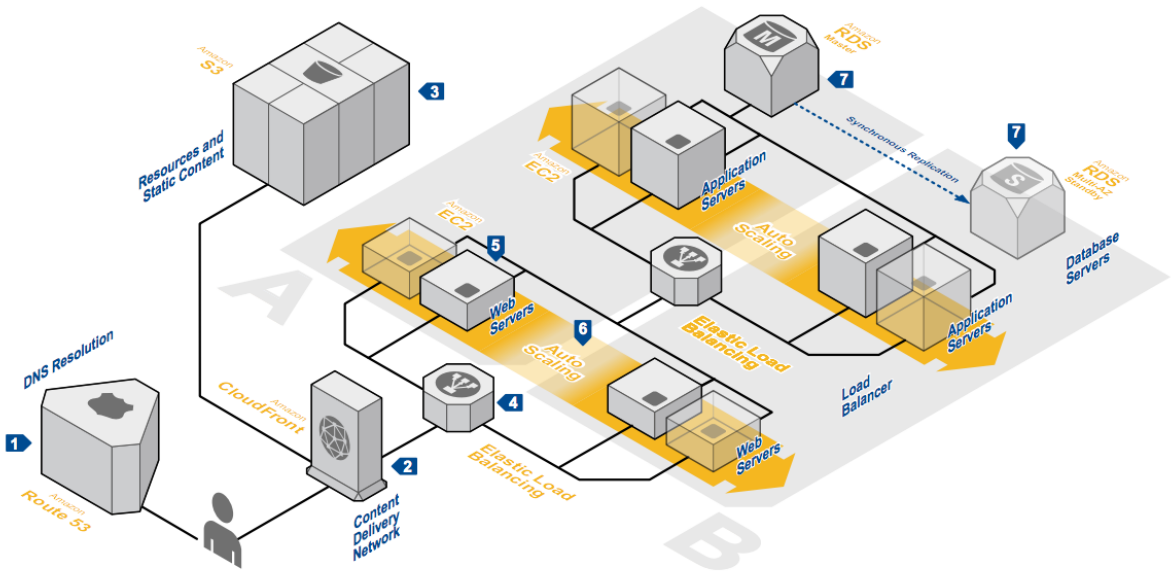
Pearson's backup method replicates data securely on a near-real-time basis, which means we maintain a full backup of customer data at all times, enabling a more robust ability to recover or restore data to the point in time closest to the event that is possible.

Automated systems monitor production data replication services, and any failure or delay in backup or replication operations will generate an alert to Pearson's on-call staff. In this way, we are able to provide high assurance to our customers that their data remains safe, backed up, and secure.

Pearson's data backup operations use Transport Layer Security (TLS) encryption when transmitting the data both internally and externally. And the backed up data at rest (called "snapshots") enjoys the protection afforded by the Advanced Encryption Standard (AES) encryption algorithm, the industry's strongest encryption, and does so at 256-bit strength. These snapshots are taken at intervals defined based on risk and will vary among systems, but at a minimum occur daily.

Logical Architecture Diagram

The diagram below depicts a typical network architecture for our cloud-based solutions.



Reference: Amazon Web Services
(http://media.amazonwebservices.com/architecturecenter/AWS_ac_ra_web_01.pdf)