Honors College Thesis
Submitted in partial fulfillment of the requirements for
graduation from the Honors College

"Best Practices for Managing Privacy and Security of Cloud-Based Student Data in Primary and Secondary Education"

Ashley Peralta

Dr. Kees Leune

Professor Mark Grabowski

Professor Sung Kim

May 9, 2024

Table of Contents

ABSTRACT

The adoption of cloud computing is increasing rapidly and plays a vital role in educational institutions. Schools have started implementing various cloud services for their community to aid in better performance of academic and efficiency tasks. This thesis aims to highlight how cloud computing, specifically cloud services, has created a new environment of technology for students, educators, and faculty as they learn how to handle the accessibility of the cloud. The research presents background about the cloud, privacy and security, data, and positive and challenging effects on educational institutions. I created a Third–Party Review implementation for primary and secondary education by reviewing higher education cloud service contracts. Successful adoption of cloud computing services is based on proper privacy and security implementations and guidelines agreed upon by educational institutions and their cloud service providers.

Keywords: *cloud computing, privacy, security, educational institutions, cloud services, third-party reviews*

Introduction

Technology has advanced throughout the years. We see different aspects of technology everywhere we go and, more importantly, everything we do. Medical records, bank information, sensitive educational data, and applications rely on technology services to operate successfully and securely. Due to its faster and more convenient operations, more industries are leaning towards cloud adoption as it provides benefits for accessible services over the Internet [1].

Cloud computing is a convenient model for data access that cloud providers use to offer cloud services to all types of users [2]. Cloud computing hides the complexity and details of the infrastructure from clients and applications. Cloud computing has certain advantages that attract potential users to gear towards computing. Clients want the flexibility and the option to pay for what they are using, with the scalability provisions to either increase or decrease the scale of managing their data access. Cloud computing offers greater data security in that you do not have to constantly check and maintain security protocols as it is done for you [3]. Cloud computing systems have recovery measures to ensure faster and more efficient data recovery if there is a breach or data loss. What is interesting and different about cloud computing is that cloud providers are the ones who maintain the systems, as opposed to an organization maintaining their systems and software using an in-house infrastructure. The best way to describe cloud computing is that instead of having files and services on a local storage device, we will use the Internet to access everything we need [3,5,8].

While cloud computing is rising, there is also an emphasized use of in-house infrastructure. Clients use in-house infrastructure to perform many activities within their companies, have more control over the operation, and reduce any mistrust and misunderstanding from third-party services. With in-house infrastructures, companies can have customized solutions based on what the company is currently looking for. On the other hand, cloud

computing offers scalability, which adds to having multiple virtual servers across a network, especially when dealing with heavy workloads [8]. With a device that connects to the Internet, the data in the server becomes more accessible – with proper authorization. As the demand for resources increases, companies must consider upgrading to newer features. With cloud services, through the functionalities of a cloud computing infrastructure, the flexibility to add and remove resources becomes more accessible. Cloud services offer a multitude of advantages for users and companies. Cloud services facilitate users' data by storing them in servers and providing access through the Internet. With any implementation, the advantages also come with some disadvantages. Users enjoy the luxury of remote data access, but concerns about cloud use exist.

Industries and companies are adopting cloud services, but it is important to understand how the cloud and its services work to know where our data resides. Cloud service providers store a wide variety of data on behalf of their users. Data is the information from clients created and processed inside the cloud. Clients upload and use data such as files, documents, and applications daily. Clients gain efficiency within their industries and companies while the provider ensures everything is held up to privacy standards. A strong relationship between the cloud service provider and the client is fundamental in ensuring that the clients are not being misled about where their confidential data is. The cloud provider should share all the concerns and regulations with the client to gain their trust. The client should ask for transparency and be informed about the provider's services before they migrate their data to the cloud by a third party. Through trust and transparency, the clients will keep returning for continuous services if providers keep up their end of the agreement.

Internet users trust that their data is secure enough to not worry about infrastructure issues. Providers need to relieve uncertainty, which is why privacy and security are two critical

components of cloud services. Privacy is the right to control your information when it is being viewed and used, while security concerns the confidentiality, integrity, and availability of unauthorized disclosure of information [4]. The security and privacy of client data break when a malicious use of a resource exists within the provider. Data breaches, unauthorized access, and malware attacks are examples of the plethora of concerns within cloud services. Security is a major concern because users and organizations entrust third-party providers with confidential information. That is why understanding data privacy and security is essential to address how cloud services manage these concerns.

Amidst the COVID-19 pandemic, many educational institutions had to transition to cloud services to accommodate remote learning for students. There were instances where schools did not have the opportunity to do a full due diligence of a service provider as they needed to implement quick solutions to ensure classroom learning continuity [68]. Before agreeing to a contract, it may have been difficult for the IT team to thoroughly review a vendor and consider important factors such as their specific needs and requirements, data security, and compliance [67]. Now that contracts may be up for renewal, institutions' IT teams can take further steps to verify that the vendor has adequate protection of the services to address and prevent the loss of data confidentiality. Additionally, with a robust and guided reviewing procedure, there is an opportunity to address gaps and identify recommendations to safeguard user information in an educational setting. The research conducted for this thesis focuses on implementing a Third-Party Review Procedure for primary and secondary institutions to develop recommendations for best practices for managing the privacy and security of cloud-based services.

1. Research Question

This thesis set out to answer the following question: “What are the best practices for managing privacy and security of cloud-based student data in primary and secondary education?”

The question can be further divided into sub-questions as follows:

- What is the cloud?
- What are the components of the cloud?
- What are cloud services?
- What is privacy? What is security?
- What is data?
- How can there be threats to data? What are those threats?
- What is the relationship between the client of the data and the cloud provider?
- How can this relationship be explicitly extended to cloud services in educational institutions?
- What steps are higher education institutions taking to ensure that certain criteria are met before agreeing to a service?
- How can these steps and possible procedures be implemented in primary and secondary education?

2. Methodology

This research involves preparing and comprehensively understanding the meaning of cloud computing through a literature review. The review was based on peer-reviewed articles, books, and journal reports. The literature review provides greater research on the advantages and

disadvantages of cloud services, the importance of data protection within various industries and companies, and sample recommendations and approaches.

The following section explains the cloud and its different components, encompassing services and resources for data. Section 4 lays out the concept of privacy and security, recognizing that different privacy frameworks exist across the United States and the European Union. A perspective of other regions will help understand how they structure their priorities for maintaining privacy and security. These frameworks and laws thoroughly explain the standards and compliance that cloud organizations, companies, and industries must uphold when dealing with the security of use. Section 5 outlines what is considered 'data' from the perspective of adopting cloud computing. This section also mentions the potential risks and threats that client data faces and preventive measures.

Section 6 will address how cloud computing and its services have provided benefits and challenges in educational systems. The goal of Section 7 is to assess how cloud service providers comply with adequate privacy and security standards. I will review cloud security frameworks, assessments, and questionnaires such as the Higher Education Cloud Vendor Assessment Toolkit, Vendor Security Alliance Questionnaire, and Consensus Assessments Initiative Questionnaire. The tools will help institutions collect information about the provider to ensure it aligns with the institution's requirements, privacy compliance, and regulations before a contract is signed. Section 8 goes into further research, focusing on previously approved contracts from an institution to clearly understand their Third-Party Review procedure. I analyzed three different service vendors and documented how each vendor compared to the others regarding purpose, compliance, and reporting process. Furthermore, after reviewing how a higher education institution performs its TPR procedure, I am creating a possible implementation of the TPR

procedure for primary and secondary education to use as general guidance when thinking about implementing a third-party service for the institution. In the end, the same TPR procedure will serve as recommendations that primary and secondary institutions can utilize to ensure they manage the privacy and security of student and even faculty data.

Background

3. What is the Cloud?

Cloud services offer a multitude of advantages for users and companies. Cloud services facilitate user's data by storing the data in a server that can be accessed over the Internet. Small businesses, all the way to big companies, have started to implement this management method. Cloud computing involves deployment models, which focus on how services are managed and available to users. Figure 01 - displays the four types of cloud deployment models. The four types are public, private, hybrid, and community [2,3].

3.1 Deployment Models

The public cloud is owned by the deliverer of the cloud services and grants permission to any user to access the systems and the services [2]. Due to its shared environment nature, the public cloud model is vulnerable to security concerns, such as vulnerabilities and cyber attacks. The public cloud offers scalability and self-service provisioning to keep up with the demands of the users [10]. With a public cloud model, a user will have access to what they need and at their desired scale from any device over the Internet. As mentioned, scalability is just one advantage of using a public cloud model for cloud services, such as faster time to market and reliability [11]. There are a vast number of public cloud services that are commonly used, including Google Cloud, Amazon Web Services, and Microsoft Azure.

The private cloud model is used by a single organization, compromising multiple consumers [2]. The private cloud has greater flexibility of control over cloud resources. Compared to the public cloud, the private cloud has the advantage of data security and privacy as the information is only accessible to authorized users. Data security and privacy are maintained through company firewalls and internal hosting so third-party providers do not gain access to valuable data [3, 13].

The hybrid cloud blends two or more distinct cloud infrastructures (private, community, or public) [2]. A hybrid cloud approach facilitates the mobility of workloads and ensures that applications function consistently across various environments. This approach enables a unified computing platform to extend and interact with multiple cloud services.

Lastly, the community cloud integrates multiple organizations. It allows organizations to communicate, share, and collaborate without relying on public clouds [2]. The community cloud is flexible because it can be designed and managed by different authorized members of the organization.

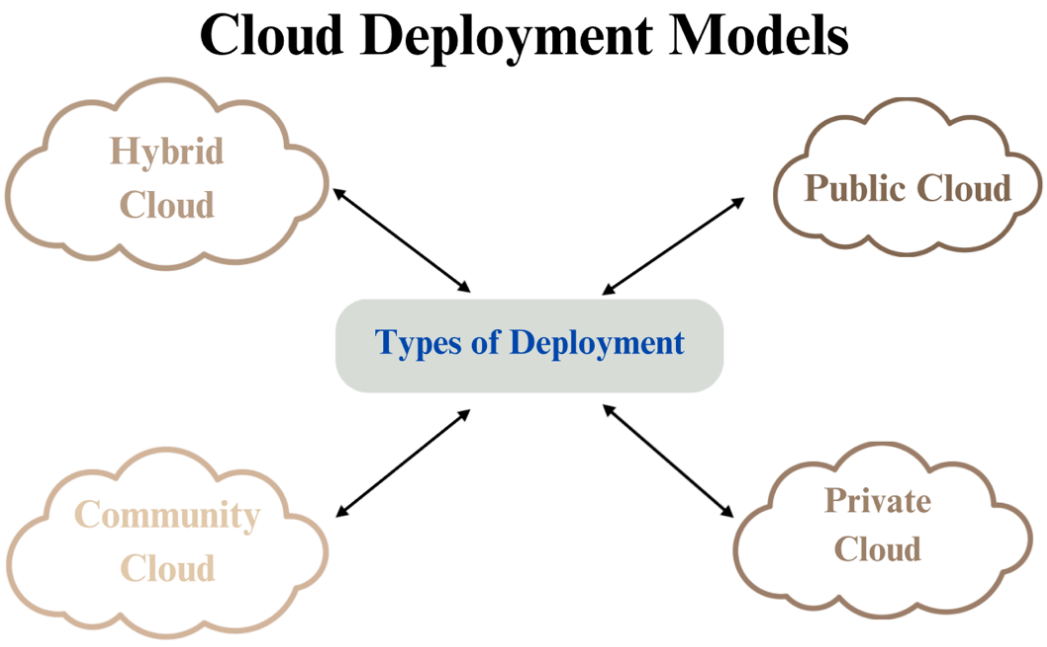


Figure 01 – Four Types of Cloud Deployment Models

3.2 Cloud Service Models

Cloud computing is composed of three cloud service models that facilitate client activities: Software-as-a-Service (SaaS), Platform-as-a-service (PaaS), and Infrastructure-as-a-Service (IaaS), which is demonstrated in Figure 02. A third-party provider distributes the data for Software-as-a-Service so clients can access it through web browsers on any device. The client does not manage what's inside the infrastructure but is limited to configuration settings. SaaS providers examples include Google Workspace, Slack, Zoom, and Adobe Creative Cloud – to name a few. In Platform-as-a-Service, a service provider facilitates services to users through software programs that can solve specific tasks. Once again, the client has the total control to execute the application and its settings. Some PaaS providers include Google App Engine and Oracle Cloud Platform. Lastly, in Infrastructure-as-a-service, the service providers offer the capability for the client to use machines and storage to improve operating systems and applications such as firewalls [3].

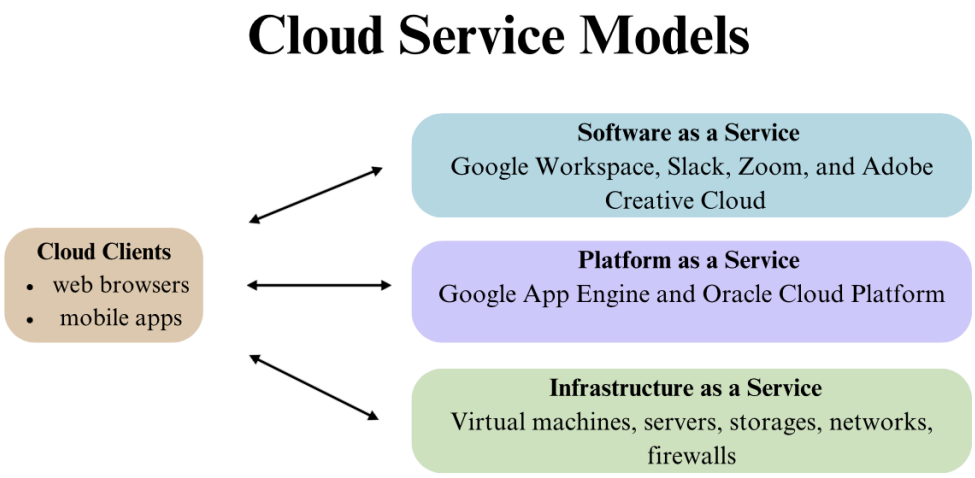


Figure 02 – The three different cloud service models and their examples.

4. Privacy and Security

Privacy is the right to control how your information is viewed and used. Through major laws and policies, privacy is visible worldwide, and gives citizens and users the guarantee that their freedom and information are protected from interference. In the cloud, privacy means that when users visit sensitive data, the cloud services can prevent potential adversaries from inferring the user's behavior by the user's visit model [3].

In the United States, the Privacy Act of 1974 governs the practices surrounding data use [16]. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the individual's written consent, according to the U.S. Office of Special Counsel. The law provides individuals with the right to request their records; the right to request a change to their records that are not accurate, relevant, timely, or complete; and the right to be protected against unwarranted invasion of their privacy resulting from the collection, maintenance, use, and disclosure of their personal information [16]. While this law does not have authority over a private enterprise, like a vendor, it is important to highlight how federal agencies also have limitations on how our personal information is handled.

Data protection is a main priority in the European Union (EU). They want to protect their citizens' personal data from the organizations and services they are using. They have implemented and adopted the General Data Protection Regulation (GDPR). GDPR is a privacy and security law that imposes obligations on organizations that target or collect data related to people in the EU [14]. GDPR gives individuals more control over their data collection, use, and protection online. There are many components of GDPR, starting with the extra-territorial scope of the law. Because this law aims to protect EU people's data, any organization that processes and stores data related to EU residents must abide by these regulations [15]. The GDPR aims to continue to strive for individuals to have control over personal information and how it will be

managed through the organization. This emphasizes the goal of protecting privacy and data. The components and principles build a foundation for trust in getting a safer and more transparent platform for EU individuals to store and maintain their accurate data.

A second EU framework also provides guidelines and laws for more data privacy solutions. The Organization for Economic Cooperation and Development (OECD) is an international organization that builds policies to alleviate challenges and aims for a better living [17]. OECD established a privacy framework and provided an analysis and advice on privacy to ensure trust and a safe digital environment. The guidelines set by the OECD apply to personal data, whether in the public or private sector, which, because of how they are processed or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties [18].

Privacy comes in different frameworks and is a crucial factor in security. Organizations establish these frameworks to create a firm method of complying with privacy laws and regulations that are put in place. These frameworks benefit both organizations and customers as they help lower the chance for risks and mitigate solutions for data security. Security concerns the confidentiality, integrity, and availability of unauthorized disclosure of information [4]. It encompasses an organization or institution's systems, resources, data, and information. The security role entails examining the systems' weaknesses, creating procedures and measures to increase privacy capacity, and assessing data authentications. Security is a concept that deals with creating a safe and efficient technology environment. You can have security without privacy, but you cannot have privacy without security [21]. This statement is specifically true when managing cloud-based data.

By affirming adequate security measures and providing transparency about security protocols, cloud service providers can help clients feel more confident about choosing their services and constantly know what to expect about managing their data.

The concept of security can be divided into different areas. To start, we need to consider the CIA triad, which refers to the three components of Information Security.

4.1 CIA Triad

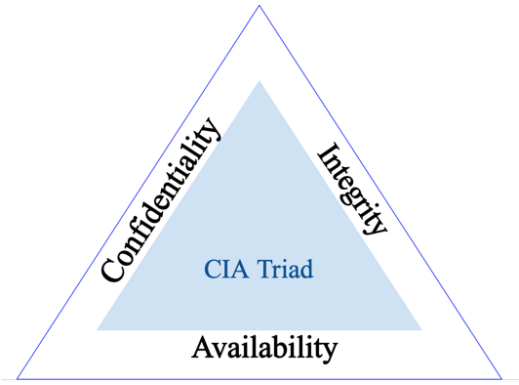


Figure 03: CIA Triad

Figure 03 is a diagram of the CIA Triad that compasses three components: confidentiality, integrity, and availability. Confidentiality involves protecting information from unauthorized access and disclosure [19]. A breach in confidentiality may include a hacking attack that can tamper with information such as students' records, medical records, and personal data. Integrity ensures that information remains accurate, unaltered, and trustworthy. It involves protecting data from unauthorized modification, whether intentional or accidental [19]. Data integrity can be at risk if threats such as security errors, malware, and cyber-attacks are present at the system's core. Lastly, availability refers to information and systems being accessible and usable when needed by authorized users. A system demonstrates availability through a functional computer system and security controls. Organizations use authentication and authorization to

make information available to those who need it and who can be trusted with it. Authentication proves that a user is the person they claim to be. Authorization is the act of determining whether a particular user has the right to carry out a certain activity, such as reading a file or running a program. Users must be authenticated before carrying out the activity they are authorized to perform. Security is strong when the means of authentication cannot later be refuted—the user cannot later deny that they performed the activity [19].

There are different privacy and security regulations that are critical for protecting students' private and confidential information when storing and transferring it using cloud services.

4.2 Family Educational Rights and Privacy Act of 1974

Student educational records are protected by law through the Family Educational Rights and Privacy Act of 1974 (FERPA). This federal law applies to educational agencies and institutions that receive federal funds under an applicable U.S. Department of Education program, focusing on protecting students' privacy [9]. FERPA governs the disclosure of educational records by school agencies and institutions and will apply regardless of the circumstances where the records are maintained, including those shared in the cloud [26]. Records regarding each student generated by the local schools are educational records under FERPA. Therefore, disclosures by the local schools to third-party cloud service providers must meet FERPA's requirements [26]. Focusing on PreK-12 students, FERPA provides parents the right to inspect and review their child's education records; the right to seek to amend information in the records they believe to be inaccurate, misleading, or an invasion of privacy; the right to annual notification of information concerning their rights; and the right to consent before the disclosure of non-directory and personally identifiable information in their child's education records. It is important to note that these rights are later transferred to students when entering a

higher education institution. Students are the ones who will maintain the right to their educational records moving forward. An example of this would be that professors are not allowed to discuss a student's progress with a parent in a higher education setting without obtaining approval from the student [23]. Overall, the rights stated under FERPA, whether PreK-12 or higher education, ensure that students' privacy regarding access, control, and authentication is thoroughly maintained.

4.3 Children's Online Privacy Protection Act of 1998

While FERPA is the foundational federal law on privacy that applies to *all* academic institutions, there are other important laws that deal with students' privacy. Children's Online Privacy Protection Act (COPPA) is one of them [26]. This United States federal law regulates the online or web-based information collected from children and may apply to various cloud services. COPPA defines "personal information" to include (1) a first and last name; (2) an address; (3) an e-mail address; (4) a telephone number; (5) a Social Security number; or (6) any other identifier that the Federal Trade Commission may determine permits the physical or online contacting of a specific individual. If a website is directed at children or the operator knowingly collects personal information from children under 13, COPPA requires that the website obtain parental notice and consent.

4.4 Protection of Pupil Rights Amendment

The third law, the Protection of Pupil Rights Amendment (PPRA), is a federal law that regulates the disclosure of certain student information collected for surveys and evaluations and might apply to various cloud computing activities of educational institutions [27]. Similar to FERPA, PPRA applies to the programs and activities of a State educational agency, local education agency, and other recipients of funds under any program funded by the U.S.

Department of Education [26, 27]. PPRA's scope applies to all education institutions, ranging from PreK-12 students. Specific rights are afforded under the PPRA for parents and transferred to the student when they turn 18 years old or become an emancipated minor [27]. First, all material used in connection with any required survey, analysis, or evaluation of students funded in whole or in part by the U.S. Department of Education, including instructional materials, must be made available for parents to inspect prior to use. Second, schools and contractors must acquire parental consent before a minor student is required to participate in related inquiries. In addition, the PPRA empowers a parent the opportunity to opt a student out of (1) surveys involving protected personal information; (2) non-emergency, invasive physical exams; or (3) activities involving the collection, disclosure, or use of personal information obtained from students for marketing, sale, or other distribution of the information to third parties.

4.5 California Consumer Privacy Act of 2018

The California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them [66]. This data privacy law was designed to enhance California residents' privacy rights and consumer protection. The CCPA grants specific rights, including (1) the right to know about the personal information a business collects about them and how it will be used and shared, (2) the right to delete personal information collected from them, (3) the right to opt-out of the sale or sharing of their personal information, and (4) the right to equal service and price for exercising their CCPA rights. This data privacy law obligates businesses to be transparent about their data practices and hold them accountable for how they handle consumers' personal information. Prioritizing privacy and giving consumers the right to equal service regardless of their exercising their rights helps build trust and confidence. The consumer will feel comfortable trusting the business because

businesses cannot deny goods or services, charge a different price, or provide a different level or quality of service just because the consumer exercised their rights under CCPA. Consumers also have the right to delete and opt-out, which may help mitigate the risk of unauthorized use of personal information.

Another aspect of the California Consumer Privacy Act includes provisions addressing collecting and protecting children's information. Businesses can only sell the personal information of a child that they know to be under the age of 16 if they get affirmative authorization ("opt-in") [66]. However, if there are children under 13 using the service, the authorization must come from the child's parent or guardian. By providing an opt-in mechanism, businesses consider that minors may be using their services and acknowledge that consumers have the right to decide whether or not they opt in or out of selling and sharing personal data.

The CCPA is a state law that sets strict provisions to ensure that consumer data, including children's personal information, is handled with secure measures to continue using services. It is becoming a sample model for other states to start considering similar privacy legislation. By implementing strong data protection regulations in our digital era, the CCPA creates an initiative for more privacy-focused client services.

4.6 Protection Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI-DSS) is an information security standard designed to reduce payment card fraud by increasing security controls around cardholder data [48]. The main goal is to protect cardholder data and sensitive authentication data wherever it is processed, stored, or transmitted. Both the merchants and service providers must comply with the overall PCI-DSS enforced by the Council. The Council is a global forum that brings together payments industry stakeholders. Each payment industry is responsible for

implementing and enforcing its own specific requirements for compliance validation and reporting. Merchants accept debit or card payments for services, while service providers are directly involved in processing card data. There are specific requirements instilled by PCI-DSS that entities should follow, including building and maintaining secure networks and systems, regularly monitoring and testing networks, and maintaining a policy that addresses information security for all personnel. Adhering to these standards helps organizations mitigate the risk of fraud through breaches, maintain a client, and provide a trust relationship when handling payment card data. Furthermore, There are three ongoing steps for adhering to the PCI-DSS [48]:

- Assess: Identify all locations of cardholder data, take an inventory of your IT assets and business processes for payment card processing, and analyze them for vulnerabilities that could expose cardholder data.
- Repair: Fix identified vulnerabilities, securely remove an unnecessary cardholder data storage, and implement secure business processes.
- Report: Document assessment and remediation details and submit compliance reports to acquiring bank and card brands you do business with.

These three steps provide an organized approach for organizations to maintain PCI-DSS compliance and help them mitigate risks, protect cardholder information, and, most importantly, uphold the client-vendor trust relationship throughout the process.

5. Data and Its Risks

Cloud service providers store and process a wide variety of data on behalf of their users. When accessing a service or a third party, users provide their personal identifiable information, contact information, and payment information. Depending on the work industry or home activities, data is being collected and stored in our cloud. Data usage would include uploading

files and pictures and interacting with them by sharing or backing up stored data. Data is everywhere—our data range from creating simple documents to private patient medical records. Data will be moving between users and the cloud and in the cloud between several physical servers.

My research will focus on the data collection and management within educational institutions from PreK–12. However, a greater repository of big data is stored with cloud service providers, which will be briefly discussed before going into the scope of education.

5.1 Electronic Health Records

Electronic Health Records (EHR) have gradually been adopting cloud-based computing services. EHR is defined as documentation containing information about the patient's clinical evolution during their health assistance process [7]. The main advantage is the ability for authorized medical staff to share patient records with other clinical centers, facilitating seamless collaboration and improving communication across the Internet. Cloud services enable healthcare providers to fully view a patient's medical history, diagnostic tests, and treatment plans, regardless of the specific healthcare facility where the data originated. However, it is essential to prioritize and have up-to-date security and privacy measures to ensure the confidentiality and integrity of patient data as they are being shared across clinical centers. One of the most important privacy policies to secure patient health information that doctors, nurses, and health professionals must abide by is the US Health Insurance Portability and Accountability Act (HIPAA), which protects patient privacy by limiting what information medical professionals can share about patients with family, friends, and the public [23].

5.2 Financial Institutions

Big data is also visible in banks, storing a wide range of data covering areas of business operations, customer data, and regulations. Customer data consists of a big part of banking interactions, so it is essential for financial institutions to safeguard sensitive data. The Gramm-Leach-Bliley Act (GLBA) establishes rules governing the duties of a financial institution to provide particular notices and limitations on its disclosure of non-public personal information [25]. Such responsibilities include providing notice of its privacy policies and practices regardless of whether a financial institution shares non-public personal information, providing the opportunity to opt out of the disclosure to a nonaffiliated third party, and establishing re-disclosure and reuse limitations from information obtained from a nonaffiliated financial institution. GLBA helps safeguard sensitive customer information by promoting transparency by providing customers with privacy notices and limiting disclosures to a nonaffiliated third party.

Furthermore, as financial institutions deal with large amounts of customer information and ensure privacy with GLBA, cloud computing can facilitate business operations. Through cloud computing, service providers offer models that eliminate the cost and hassle of purchasing additional data centers. Because of this, the banking business data can be stored, analyzed, processed, and mined quickly [24]. Having faster data processing will ensure that banks get quicker results for their business decisions and client satisfaction. Faster processing is useful as customers require banking services daily. Personal information, including customer names, addresses, contact details, social security numbers, account numbers, and documents, are constantly getting processed and stored in the cloud. Whether customers are first-timers or depositing money, those are considered transactional records that contain vital private information. Overall, cloud service providers contribute to the agility of banking systems, as they

allow for a quick and efficient adaptation to changing conditions and adhere to the customer's privacy and security. Cloud providers often implement robust security measures, including encryption and access controls, to safeguard sensitive information. The cloud's scalability, efficiency, and security features empower banks to navigate the complexities of managing vast amounts of customer data while delivering seamless and secure financial services.

5.3 Educational Institutions

At educational institutions, students, teachers, and faculty use the Internet for multiple activities throughout the school day. Classrooms are using the Internet to access SaaS cloud services. Google Workspace and Microsoft Office are resources where users can interact and share corresponding files. The most evident benefit of institutions using cloud services is the accessibility to course materials. Teachers can upload assignments, exams, and additional materials, and students can access everything they need with a device and Internet connection. Aside from teachers and students, faculty from different departments handle confidential data - student records, grades, and administrative data. However, not everyone has access to the students' information. As previously mentioned, this type of information is protected by law through FERPA [9]. Educational institutions must establish and uphold policies that control access to student records and ensure the confidentiality of sensitive data. These policies typically include guidelines for who can access student information, under what circumstances, and the procedures for obtaining consent. It is crucial for educational institutions to balance the benefits of technology with the responsibility of ensuring security, accessibility, and equal opportunities for all students. In terms of cloud service providers, the institution needs to thoroughly review if the provider complies with educational privacy laws and where HIPAA regulations apply. The

institution's reviewer will feel confident that the service should be implemented if they know how the provider explicitly states and handles their user's data exposure.

Many institutions collect data from their clients in multiple ways, so storing, analyzing, and ensuring security and privacy becomes a concern. The increase in data manipulation, misuse, deletion, and similar threats affects individual users and negatively impacts all sectors and critical infrastructures [22]. Cloud-based data are constantly exposed to threats and risks, especially as they are stored away for data collection and retrieval. While data is processed through the providers, there are events where the confidentiality, integrity, and availability of the data are compromised – this is where privacy and security challenges arise. The following subsection will examine the possible data threats and risks associated with cloud service providers.

5.4 Data Risks

Security risks are visible throughout different organizations. They trust that their data is safely stored and safeguarded through encryption methods as they utilize the services they paid for. Data are exposed to risks, primarily when critical processes such as data collection, preprocessing, and analysis are performed [22]. That is why a concern is data location. How can clients and users know their data is safe and protected if they do not know where it is stored or located or who stores it? Many cloud computing services store data in multiple physical locations, and most of the time, the location of an organization's data is unavailable or not disclosed to the service consumer [29]. Data leakage can also occur because, without an accurate location of where the data is being transferred, stored, audited, or processed, it is likely to reach a malicious attacker.

Insider Access creates a security risk because the clients within the organization pose a threat. In some cases, it will be the employees. An insider attack will occur in many ways. The first is when employees access services from a cloud service provider without the sufficient knowledge of the risks [30]. The second would be intentionally causing harm to the organization's networks, systems, and more. The threats may involve fraud, espionage, sabotage of information resources, and theft of confidential information. Insider access risk increases when the range of users' access to the organization's networks is widened. A malicious user can launch a Denial-of-Service attack where, if successful, the system cannot satisfy any request from other legitimate users due to resources being unavailable [8]. Ransomware attacks can occur by denying access to a user's data, usually by encrypting the data with a key that the hacker knows until the ransom is paid.

Data breach incidents may occur due to human error, which includes phishing and weak authentication practices. Phishing refers to the practice where attackers send emails or messages to deceive users into revealing personal information and sensitive information [40]. Weak authentication practices can cause system vulnerabilities and opportunities for malicious attackers. Weak login credentials are the easiest way to target users because of predictable usernames and passwords. Attackers are more likely to try easy-to-guess passwords to gain access to the system. To prevent such attacks, services and organizations can create specific password requirements to enforce that the contents stored in the account are secure and that access is restricted. Another method to help with login credentials is setting up Multi-factor Authentication, which adds an extra layer of login security to prevent unauthorized users, even when passwords have been stolen. Human error can come from human negligence because users

leave their devices unlocked before leaving the area, leak sensitive information, and do not abide by the confidentiality and security regulations in place.

A third party would most likely use a data center for storage; however, there are some risks associated with outside storage. Third-party data storage comes with the issue of control because clients do not have full control and do not know the location of the storage server and security services [40]. With data storage, there is the threat of data loss and leakage. Data loss is the deletion, alteration, and theft of data without a backup of the original content [40]. Data loss and leakage can happen due to multiple reasons. The first one is the result of a successful data breach attack. The second one can be caused by a disruption at the vendor site. If a disruption happens and the vendor is unprepared, backups and operations can fail. If the standards and steps for backing up data are not contingent on current processes in the organization, there is uncertainty about the data's security. However, if their Business Continuity Plan and Incident Response Plan are established and up to date, the disruption will cause their Disaster Recovery Plan to activate so the vendor's Information Security Department can work accordingly to the problem and initiate relocation to an alternate site if necessary [45]. Each vendor's Information Department will have assessed different scenarios and strategies to mitigate the downtime of business operations. More information about vendors and their Incident Response Plan and Disaster Recovery Plan will be discussed in the Third-Party Review Procedures section.

6. Cloud Services in Educational Institutions

Educational institutions are gradually adopting cloud computing infrastructure. Technology provides faster delivery and storage of collected data for educational purposes, such as teaching and learning. Furthermore, we can analyze, share, manage, and communicate huge amounts of information. This helps students receive vast resources to engage and collaborate

with others during the academic journey, regardless of the devices or internet browsers they are using.

In PreK-12 schools and universities, administration, teachers, and students can upload and prepare their own documents and share them across networks and platforms. Figure 04 demonstrates the areas where different school members can use a cloud service to complete their tasks. For schoolwork, students can work on team projects, homework assignments, and presentations. Outside of the classroom environment, students can check their grades and view their attendance status; with authorized access, parents can do the same. Parents can interact with the teachers via remote access and provide accurate, up-to-date information about their children when they ask. Teachers can create their school-year curriculum and have it saved and accessible whenever they need it – with proper Internet connections. Teachers can create lesson plans and prepare presentations, videos, and student handouts. All their teaching materials are stored within the SaaS applications to which their institutions are subscribed to. School administrators use the services provided by the cloud to keep track of parents, students, and faculty personal identifiable information (PII) to have a profile built and their relevance to the school. PII includes sensitive personal information such as full name, ID numbers, and medical records. School administrators handle financial information for tuition or student affairs payments. Handling finances means that they are in possession of others' credit card and billing information. If necessary, the administration can interact with other institutions when dealing with school transfers and share student records with potential colleges and universities.

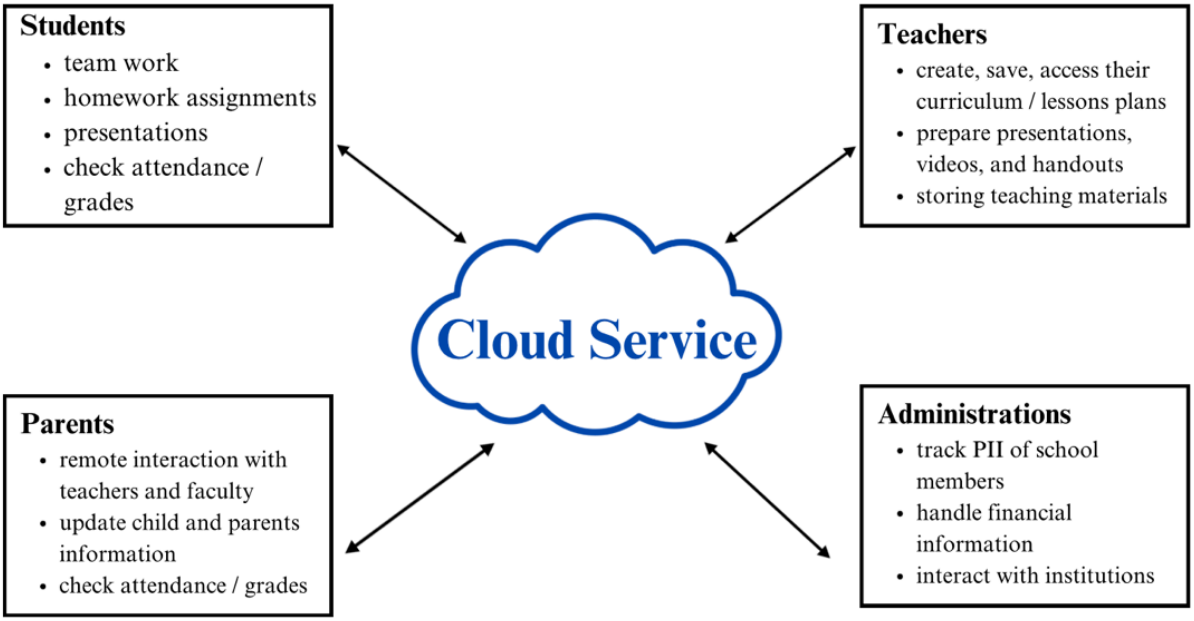


Figure. 04 – Different Areas in Educational Institutions Using Cloud Services

The benefit of educational institutions adopting cloud computing services is that they only receive services for what they are looking for. Some institutions may want resources and services more than others. That is why, when adopted, cloud service providers can use a cloud computing infrastructure to customize their resources to meet each site's different needs and challenges. With customization comes benefits. We can see the positive effects and concerns no matter how services are used.

6.1 Positive Effects on Educational Institutions

1. *Virtualization*: In-house infrastructures sometimes have slower processing times but depend on adequate maintenance practices. With the cloud, processing time is quicker to access websites and apps on school devices. There is also the advantage of accessing materials and resources if they are remote learners. The virtualization of their cloud

environment offers a new way of getting and utilizing computing resources remotely or in person, regardless of location [28].

2. *Elasticity with Cloud Storage*: With elastic cloud storage, the providers will allow education institutions to meet the exact storage requirements within minutes. Cloud elasticity provides the resources needed for each task. They are increasing the speed and performance of the service [28, 31].
3. *Quick Service and Data Availability:* Users can access stored data on their devices independent of the location. Students and Educators can log into their desired service when they need to access documents or upload files or new reports. While administrators have access, they should not log into the school database and email outside school hours.
4. *Individualized Learning:* Students can access and share a wide range of resources and projects. Teachers and students can engage in online learning when applicable. While absent, students can still access their work and documents, so they are not behind in school.
5. *Minimum maintenance*: There is an absence of software and hardware setup installation. The malfunctions and faults will be reduced to a minimum level. Therefore, there will be no need for technical support staff or maintenance problems [31]. It will be up to the cloud service provider to adhere to their maintenance standards and ensure the institutions are notified of any changes made to the system.
6. *Competitive advantage:* Using cloud computing services in education creates a competitive advantage through access and use of advanced software and applications that allow us to analyze and process big data. Students, teachers, and researchers can access

the newest and most advanced methodologies in education and scientific research, while other institutions can achieve these results.

6.2 Challenges Facing Cloud Computing Services in Educational Institutions

1. *Security*: We have established that security is the biggest concern of clients when using cloud services or its resources. Schools deal with sensitive student and staff information such as full name, address, medical information, and biometrics. Before adopting cloud computing infrastructure and/or purchasing a service, they must ensure that the service adheres to all student privacy laws and relevant regulations.
2. *Unsolicited advertising:* This advertising can be from spamming or pop-ups when navigating certain websites. Without restrictions, adware can continue to make its way through devices, ultimately collecting personal and specific information and continuing the chain of forwarding. When dealing with information from students 13 and under, their privacy must be protected when using the application or service that offers advertisements. Using cloud services that comply with COPPA regulations, children can remain secure with proper data collection and marketing restrictions.
3. *Malicious Insider:* Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring inherent risk [29, 30]. In the context of educational institutions, an insider can be a current or former employee who knows how to use the organization's systems, interface, and database. An insider may use a device to inject malware code into cloud storage. If done successfully, the code grants access to information, and its criticality depends on how the code was designed and what security measures were in place by the provider.

4. *Data location*: A common compliance issue is that many cloud computing services store data redundancy in multiple physical locations, and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer [29]. Depending on the data flow, it becomes difficult to figure out what international and domestic regimes are in play.
5. *Bandwidth*: Before implementing a cloud service, organizations must evaluate the communication bandwidth requirements and assess the services with respect to the large amount of data transmission. If the Internet bandwidth is insufficient, it will be challenging to deliver educational services, mainly because the services are deployed by the public cloud [28]. It is possible that some PreK-12 institutions do not have enough bandwidth; this will be a challenge when a vast portion of the school is on devices. There will be slower performances that can hinder learning and affect online testing periods.

6.3 Cloud-Based Services in Educational Institutions

Cloud-based services such as Google and Microsoft provide resources and computers for institutions to promote the adoption of this new infrastructure. The following section is a brief overview of two examples of cloud services that are used in educational institutions and their security implementations.

6.3.1 Google Workspace for Education

Google provides Google Workspace, composed of Mail, Calendar, Docs, Slides, Sheets, and Drive without cost and advertisements. Google enables seamless collaboration to make it easier for everyone in the school to collaborate. It gives teachers easy-to-use tools to help simplify tasks and save time – boosting productivity in the classroom. There is access to flexible communication through email, chat, and video. Students and educators can organize tasks by

building to-do lists, creating task reminders, and scheduling meetings. Aside from productivity and learning resources, Google Workspace provides trusted security to safeguard against digital threats with multilayered security [32].

An important aspect of adopting cloud computing and its services is knowing they follow the rules and regulations to meet privacy and security standards. Google uses it in compliance with numerous requirements and industry standards, including FERPA, COPPA, and GDPR. With Google Workspace, institutions own their data, and admins have full control and visibility in managing their tools for students and educators [33]. Owning their data eliminated the concern of an outsider storing the data. The users are always aware of where their data is and that it will not be transferred or scanned for advertising purposes. The Google Cloud Whitepaper 2021 issue states that, for the most part, they are the ones that conduct all their data processing activities but will engage third-party suppliers for customer and technical support [34]. This complete outline demonstrates the security measures that Google has implemented to allow for safe collaboration and productivity with every minute of learning.

6.3.2 Microsoft Office 365 Education

Like Google, Microsoft has established "Office 365 Education," which provides a global forum to pursue educational initiatives with familiar applications accessible everywhere. Microsoft brings powerful tools for the classroom, where file updates in real-time continue to build a seamless and user-friendly curriculum [35]. Their application, OneNote, helps organize class materials and easily collaborate with students and colleagues, all in one place – a digital notebook.

Microsoft aims to establish a simple, secure, efficient technology environment that maximizes learning. There are cybersecurity tools that can be implemented in Office 365

Education to ensure security, privacy, and compliance. One of them is Microsoft Intune for Education, a cloud-based endpoint management solution. It manages user access and simplifies app and device management across many devices, helping educators and students stay productive on classroom devices and secure data. The advantages of Intune for Education include configuring and assigning the apps students use in the classroom, controlling how students and teachers access and share classroom information, and including only the settings to manage specific school devices [36].

By configuring and assigning the apps, students can only use certain apps they have access to. Restricted access helps prevent unauthorized usage of apps or software that can hinder the security of their devices and data. Controlling access and sharing ensures that sensitive and confidential information about students and teachers is protected from unauthorized users, ultimately reducing the risk of data breaches and disclosures. Enabling only the necessary settings for the school devices creates strict limits that will help minimize unnecessary workflow management. Instead, IT departments can focus solely on managing and controlling the essential configurations. Unnecessary data collection and sharing are avoided, ensuring that data is protected in compliance with privacy regulations.

Experiment

7. Cloud Service Providers Assessment

This section of the thesis will focus on conducting an assessment review to understand the frameworks and questionnaires completed by cloud service providers. There was an analysis and review of necessary privacy and security standards that need to be considered when agreeing to a contract between the provider and the institutions. In this review, the vendor is the cloud

service provider, and the client is the institution. The completed frameworks and questionnaires are given to the client so they can review them during their Third-Party Review procedure. I developed cloud privacy and security standards and will be used to create a PreK-12 vendor assessment questionnaire.

7.1 Review of Three Risk Assessment Frameworks

The first step is using multiple security toolkits and questionnaire frameworks to create standards and requirements for the implementation to audit how the vendor (cloud service provider) complies with the proper implementation and execution of security controls.

I reviewed three essential toolkits and frameworks. They are explained in the following subsections:

7.1.1 Higher Education Cloud Vendor Assessment Toolkit

The Higher Education Information Security Council created the Higher Education Cloud Vendor Assessment Toolkit (HECVAT). HECVAT is a self-assessment that attempts to standardize higher education information security and data protection requirements around cloud service providers. This framework measures vendor risk and confirms that information, data, and cybersecurity policies are in place to protect the institution's PII [37]. According to EDUCAUSE, HECVAT:

- Helps higher education institutions ensure vendor services are appropriately assessed for security and privacy needs, including some unique to higher education.
- Allows a consistent, easily adopted methodology for campuses wishing to reduce costs through vendor services without increasing risks.

- Reduces the burden that service providers face in responding to requests for security assessments from higher education institutions.

HECVAT is broken down into sections to address different areas where vendors and their products are present in the institutions. HECVAT sections center on documentation, data governance and privacy, and Business Continuity Planning. Documentation is a good section for the assessment because we get an overview of what procedures and policies are in place and how they are managed and updated when necessary. Governance and Privacy relates to how vendors will handle and protect sensitive data and comply with privacy regulations such as FEPRA. The Business Continuity Planning section includes questions about the strategies and activities maintained in their plan to execute the proposed business recovery when necessary.

The HECVAT has two versions: HECVAT-Full and HECVAT-Lite. Vendors use both versions, but some factors must be considered before completing the assessment. The HECVAT-Full version thoroughly assesses the cloud service provider's privacy and security practices. It incorporates all the sections available in the assessment, including company overview and documentation, IT accessibility and third-party assessment, security and compliance measures, and incident handling and quality assurance. It is more suitable for in-depth evaluations when dealing with high-risk or critical data-sharing engagements [37].

On the other hand, HECVAT-Lite is a streamlined version that speeds up the assessment. This version only focuses on specific sections such as documentation and data governance, security and authentication, business continuity and disaster recovery, and system management. The HECVAT-Lite is designed for vendors who need a rapid evaluation and are dealing with lower-risk services [53]. The choice between the two versions depends on the specific needs and priorities of the institution who is conducting the assessment.

7.1.2 Vendor Security Alliance

The Vendor Security Alliance (VSA) questionnaire focuses deeply on vendor security. The VSA is a coalition of companies focused on measuring and reducing vendor risk, with the goal of making the internet safer for everyone. Through access to the different areas of security and risks, organizations can understand the vendor's information security policies based on their answers. VSA-Full is the questionnaire with the following approaches taken [46]:

- *Data-Risk Based: The risk is proportionate to the sensitivity of the data they are accessing (and the volume of data).* This means that the risk level is associated with the sensitivity of the data and the volume of the data that the vendor has access to. Not all vendors can access all data types, so the controls and approaches will be determined based on their data risk.
- *Integrated Security: This is achieved by thinking about security from the start.* This approach involves considering all the different aspects of how the service will function. We can take the correct steps to minimize a break and protect against security threats by considering other factors.
- *Service Oriented: Rather than audit the company, we focus on just the services being delivered.* The VSA questionnaire focuses only on the services the institution will be using, so they have a clear scope of the relevant security policies and controls for review.

All these approaches are incorporated into different sections of the questionnaire. The Data Protection & Access Control section asks questions about data access, handling, and third-party data processing. These questions are important to review so we know the extent of the data's sensitivity and what protections will be provided. This is where the Compliance section

comes into play. Before agreeing with the vendor, the institution must assess how audits and regulations are maintained.

7.1.3 Consensus Assessments Initiative Questionnaire (CAIQ)

The CAIQ is a survey for cloud consumers and auditors to assess a Cloud Service Provider's security capabilities. It is currently in its fourth version and combined with the Cloud Controls Matrix (CCM). The Cloud Security Alliance's CCM is a cybersecurity control framework for cloud computing composed of 197 control objectives that cover key aspects of cloud technology that align with CSA best practices.

CAIQ v4 helps organizations conduct self-assessments to test their compliance against the CCM v4 using 'yes' and 'no' questions that can determine if the CCM controls are met. The 17 security domains in CCM aim to support the internal cloud service provider governance, risk, and compliance activities and provide a helpful baseline for transparency [47]. These domains cover various security components, such as audit management and application security, business continuity to data security, and risk management. CCM addresses cryptography, supply chain transparency, threat and vulnerability management, and endpoint security. Each domain offers specific control specifications tailored to mitigate risks and ensure robust security measures across various aspects of cloud environments.

7.2 Privacy and Security Standards

When creating, signing, and entering an agreement with a cloud service provider, there are specific requirements and standards that the educational institution needs to ensure the vendor meets.

7.2.1 Data Collection and Ownership

A primary requirement is acknowledging what data is being collected and how the data will be handled during the timeframe that the contract is active. The agreement must address how the institution will own its data and can retrieve it when necessary. Cloud service providers do not have the rights or licenses to use the data for their own purposes or interests aside from contractual obligations. The organization's ownership rights over the data must be clearly stated in the service contract to enable a basis for trust and privacy of data [29].

7.2.2 Transparency

Another main requirement is having complete transparency and accountability for security from cloud providers. An aspect of transparency is clear communication with the client about the security policies, protocols, and practices to which the provider adheres. There should be regular updates about incidents that have occurred and improvements that are made. These updates inform the client of current data breaches, vulnerabilities, and remediations. For accountability, the vendor is responsible for protecting client data and maintaining the CIA Triad up to par. Section 4 can be referenced to review how to implement robust measures regarding confidentiality, integrity, and availability upkeeping. Through transparency and accountability, institutions can know exactly where their data is stored and how it is processed in the cloud.

7.2.3 Compliance

Compliance is another aspect of an agreement. Compliance refers to an organization's responsibility to operate according to established laws, regulations, standards, and specifications [29]. Clients should have the right to audit and access the contract and the reports a third party conducted. The client must ensure that the vendor addresses all the requirements and complies

with educational laws and regulations associated with the service. Another regulation would include compliance with HIPAA, followed by the PCI-DSS standard if applicable.

7.2.4 Notification of Breach

Immediately notifying about data breaches is an excellent aspect of transparency. Furthermore, the cloud provider must outline the data breach procedures. For vendor assessments that cloud service providers complete, there is a section about how the vendor will respond and react if there is any breach. As a vendor, an important step is to comply with applicable breach notification laws. In New York State, The NYS Information Security Breach and Notification Act states that entities and persons or businesses conducting business who own or license computerized data, including private information, must disclose any data breach to New York residents whose private information was exposed [44]. This means that no matter the type of organization, the vendor must notify the client's central point of contact. In the case of Federal Student Aid, the Student Aid Internet Gateway Enrollment Agreement (SAIG) is an example of how Title IV participating institutions "[m]ust ensure that all Federal Student Aid applicant information is protected from access by or disclosure to unauthorized personnel" [45]. Institutions are responsible for protecting sensitive student information and PII from unauthorized disclosure. Aside from disclosure protection, the SAIG Agreement includes a provision that the institution must immediately notify Federal Student Aid about an actual or potential breach. If the breach is notified immediately, it can be identified, contained, and mitigated so that it does not affect multiple institutions. A provision about immediate notification establishes a clear understanding of what needs to be done to minimize a breach properly and ensures excellent communication with clients using such services.

It is recommended that a central point of contact be responsible for receiving initial breach information, the investigation information, and communication messages as they are coming. Most importantly, the point of contact on the vendor's side can evaluate and investigate the threat and quickly activate their recovery plan [43]. The client needs to be informed about the scope of the breach, the type of incident that occurred, and what information was compromised. After the client is informed, the next step for the vendor would be to address the data breach issue and provide accurate documentation, if possible, about how they will perform data recovery.

7.2.5 Termination of Contract

Providers need to specify the process of contract termination in different scenarios. Questions such as "How will the contract be terminated if one of the two parties fails to comply with the regulation set by the agreement?" and "What are the terms for termination?" are important because it builds on the client-vendor trust relationship. Institutions must trust that their cloud data will be returned or permanently deleted. Deletion of client data is a crucial component that should be outlined in the agreement. There should be a detailed explanation of how the vendor will handle the disposal of the client data, mainly since public cloud providers deliver through the Internet.

7.2.6 Business Continuity

It is a good strategy for cloud providers to include information about business continuity, specifically the Disaster Recovery Plan (DRP). A Disaster Recovery Plan is the Information Technology planning component of Business Continuity Management that deals with IT infrastructural needs. It is a specific plan for the IT department to provide continuity and recovery of an organization's systems and communication capabilities [43]. It is important to cover the area of DRP in the contract because it helps the institution figure out what will happen

when a disaster occurs, i.e., the systems go down for hours. With robust and well-tested disaster recovery strategies, it will minimize interruptions, mitigate severe impacts, reduce downtime, and improve security.

Findings

8. Third-Party Review Procedures

This section will discuss how higher education institutions review providers before implementation. The information acquired will be used to examine how PreK-12 institutions can follow a similar journey.

8.1 Higher Education Reviews in Action

A long procedure exists for agreeing to and signing a contract with a cloud service provider. One big step is ensuring that the service provider meets the institution's requirements and is reviewed by the professional in charge of Third-Party Reviews.

Looking into how Adelphi University, a higher education institution, performs its review is beneficial to finding the best practices for a similar and efficient implementation in PreK-12. Figure 05 demonstrates their Triage Workflow Chart.

It is important to start by assessing the critical dependency of the provider and its impact on the institution. If it poses a high risk, then a full Third-Party Review (TPR) and Business Impact Analysis (BIA) will be performed, and we need to assess compliance issues. However, if the critical dependency is low, it will evaluate the significant compliance burden next.

The Third-Party Review assesses the security controls a third party has implemented to protect university information. These requirements depend on the type of information that will be

stored or processed by the third party [38]. When there is a High Risk in any entity, the Information Security Reviewer needs to ensure that there is no exposure to laws and regulations such as FERPA, HIPAA, PCI-DSS, GDPR, and Privacy Policy. If there is an exposure, we must implement controls to mitigate and lower the risk to continue our checklist.

Significant compliance burden refers to resources the provider uses to meet the compliance requirements set by the laws, regulations, standards, and the institution. Once again, if the provider falls under "Yes" in this category, it is marked as high risk, and the provider must follow the steps to perform a full TPR and BIA. We are also verifying that they address compliance. If there is no significant burden, the next step would be to check if the provider requires a login.

A login refers to gaining access to the application or website using the proper credentials to identify the users' identities. If the response is "No" for a login, the next question will be whether it is only public data. Public data includes information found in public records or sources without access restrictions. If no public data is involved, the next step will be to abort the provider as it does not meet the requirements.

On the other hand, if a login *is* required, the review must assess what information is needed, such as public or non-institution data. There is a low risk if it is *just* public and non-institution data, so we do not have to continue any review. With a low-risk vendor, the Information Security Reviewer can provide feedback from the review to the institution's procurement department. Based on the findings, the procurement department will decide if they enter into a contract with the vendor.

If the vendor is not using the data in the entity for the login, then we need to ask if the service can be integrated with a Single Sign-On (SSO) authentication. SSO mitigates the risk of

unauthorized users and focuses on centralizing the process of allowing institutions to use a single authentication server. Many institutions, such as Google Sign-in or their school platform, have an SSO in place. Having the SSO enables the institution and provider to implement and transition the services efficiently. SSO also provides a Medium Risk to the institution, so the reviewer will recommend a full TPR review, which will differ per institution.

If the vendor does not require integration with SSO, the reviewer will need to verify if the vendor supports Multi-factor Authentication (MFA). MFA is vital for a third-party service because it enhances the security of your account by requiring the user to identify themselves with an extra factor aside from the typical username and password. There are three most common factors: something you know, such as a password; something you have, like a smartphone with an authentication code generator; and something you are, like a biometric identity. The reviewer is looking into MFA specifically because if student data is involved, the institution and IT department need to ensure that it would not be quickly accessible through a compromised password. If the vendor supports MFA, that is great; now the reviewer will evaluate the involvement of IT with service administration. This means that IT needs to ensure that there is an easy integration and implementation of the service, so it is compatible with the systems and services the institutions already have. IT needs to actively monitor the configuration and setup of MFA within the vendor's systems. If IT is involved, then the third-party is deemed a Medium Risk, and a full TPR will be performed to finally have an accurate representation of the implementation of the service/provider in the institution. Contrarily, if there is no MFA, it will be considered a High Risk, and a TPR and BIA will need to be performed. This is also the result if there is no IT involvement.

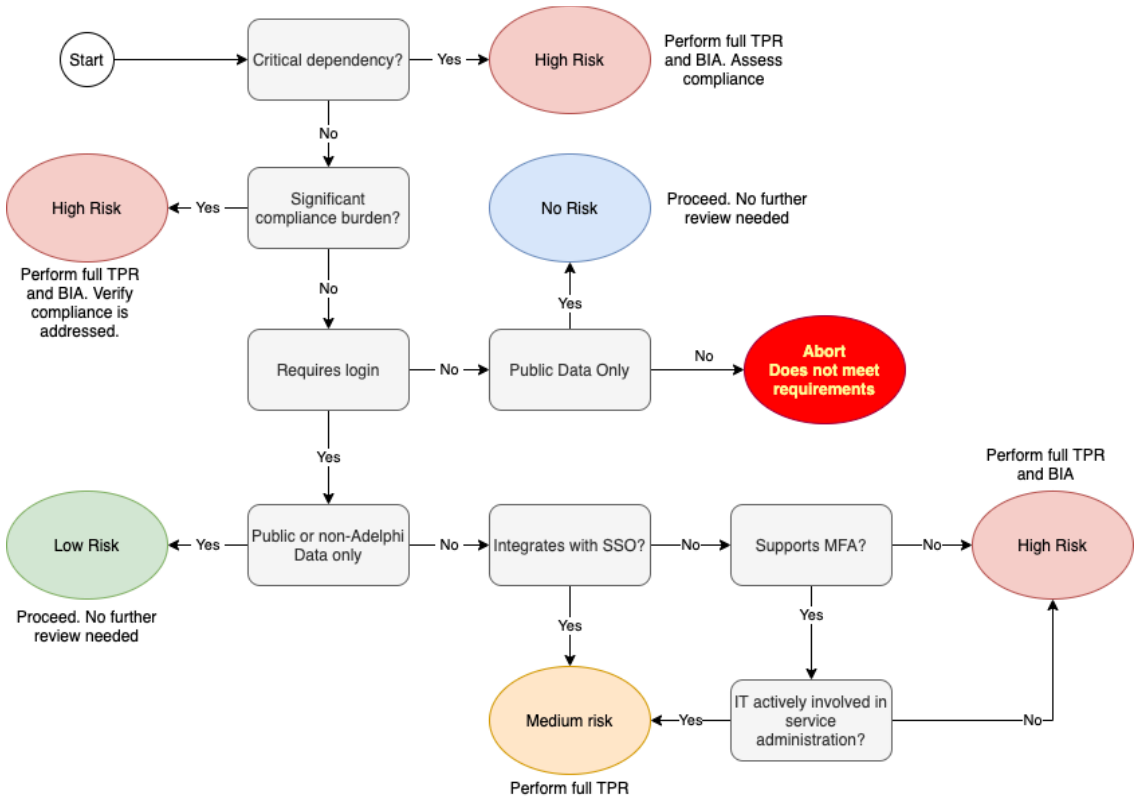


Figure 05 - Triage Workflow Chart

A flowchart outline such as the one described above provides the reviewer and committee in charge a better perspective of what to look for before accepting a new third-party vendor. They will go through each entity of the flowchart, answering the question with a "Yes" or "NO" response until they can determine if the provider is "No Risk," "Low Risk," "Medium Risk," or "High Risk." While following this flowchart ensures that every possible security and policy issue is addressed, higher institutions expect the VSA and HECVAT framework to be completed beforehand by the potential vendor.

Reviewing the vendor's VSA framework answers helps the institution understand the risk exposure associated with the third-party service provider. As mentioned in the previous section, VSA outlines a series of questions covering different sections. Each third-party provider will undergo an individualized VSA covering the specifics, such as a description of the purpose and

the security standards for the student data that will be collected. When necessary, the provider needs to provide additional information and reports regarding their system or data integration – this provides the reviewer with the full scope of how the provider functions. The provider's HECVAT will help the institution assess their vendor risk; depending on the level of risk, they will be asked for either a HECVAT Full or Lite. The reviewer will focus on data ownership, encryption methods, and proper certifications. Certifications will include ISO 27001 and SOC 2. ISO 27001 is a standard from the International Organization for Standardization for Information Security Management Systems (ISMS) that defines the requirements a company must adhere to to manage risks related to the security of the data owned [39]. Furthermore, SOC 2 ensures proper security controls are implemented to protect customer data.

The next step would be to conduct a Third-Party Review of the potential service to be provided by the higher institution (if they have one in place). Usually, the institution will have its own assessment as a ready-to-use template and complete it with as much detail as possible. Most of the information can be acquired from the VSA, HECVAT, or the additional documents that the vendor provided. The TPR will cover a set of requirements that the institution is looking for, including compliance with regulations, data protection, business continuity, authentication and auditing, and vendor security.

During the Third-Party Review, the reviewer looks at different assessment areas and ensures the vendor's service is in the desired state. If not, the vendor must explain their measures to reach that state. A desired state in the scenario of a TPR would be the ideal objective and situation for each requirement and will vary depending on the context being reviewed. For example, with compliance exposure, the desired state is None/Addressed. This means that while

assessing the service, the reviewer is looking for the vendor not to have potential exposure risks that can threaten the security of the collected PII.

A Business Continuity Worksheet will help with risk assessment and Service Level Agreements (SLAs). For risk assessment, the institution can determine potential risks involved in the provider's operations. With Business Continuity, SLAs can allow organizations to maintain continuity of services, emergency response, and recovery time.

A Vendor Service Risk Assessment with general questions can provide visibility into the risks of using third-party services and the potential impact on the institution. The document should contain questions that any reviewer can answer about the vendor based on the information and additional documents provided. Sample questions may include:

- What is the purpose of the service?
- What functionality is required?
- How critical is the risk of service unavailability?
- What student personal and private information will be provided to the vendor?
- Does the service support SSO, MFA, or Sign in with Google?

These questions are simple, but when answered in detail, can provide critical information about what will happen when the service is implemented. Knowing the purpose will help identify the vendor's focus and how it will integrate and function within the institution. Identifying the risk of service unavailability early on, due to a service disruption will lead to having mitigations ready when the time comes. It is better to know the potential risks ahead so that when it is High Risk, there is a backup that ensures that the data is secured. This also reduces downtime for the services so they can continue working correctly and there is no data loss.

A typical review happens before signing a contract. Reviewers will assess and report back to the Contracts and Procurement Department, stating the risks they have found and their recommendations. Now, it will be up to the higher administration to decide if they want to proceed with the third-party contract. The following section will put everything discussed about a TPR procedure in perspective by analyzing three vendors who have gone through the process and are used at Adelphi University.

9. Data Collection

Establishing security standards using flowcharts and questionnaires is a method for a higher education institution's Information Security department to create a more straightforward process when reviewing vendors. Three vendors that have gone through the TPR were examined to analyze potential differences between each vendor. I analyzed the vendors based on the documents provided and how they meet the requirements of Adelphi University's TPR Service Assessment Checklist and Flowchart [49, 50].

Vendor A - Digital Ticketing Service

It is important for a reviewer to clearly understand the vendor's scope and identify the service's purpose. The reviewer needs to understand the scope because it will allow them to accurately determine if the service aligns with the needs and goals of the institution. A clear understanding of the scope will ensure that the contract between the vendor and the institution reflects explicitly the services and obligations. The scope prevents future disagreements between parties. In the case of Vendor A, this digital ticketing service would serve as an app for sports fans to purchase tickets for home games [53]. Functionalities include a ticketing system for sports events with just a processing fee. Because the app deals with purchasing, a concern will be

PCI-DSS [48]. We must ensure we know how the user's credit card information is stored. Vendor A will be using a third-party cloud-based provider to process card payments, eliminating the action of collecting such information on the vendor's systems.

As mentioned above, the vendor should provide all necessary information, including their Privacy Policy. The document can be found on their website but should be given to the institution for review. After reading Vendor A's Privacy Policy, no inconsistencies were found where there would be a high risk of privacy or security breaches. The document states how the service will collect users' personal information (name, email, address, mailing address, phone number, and payment card information) through their websites, partners, and orders. However, users may refuse to supply information [51]. The policy also mentions how the information will be collected, explaining that the exchange will be handled over TLS-encrypted communication channels and their compliance with PCI standards. Something important mentioned in their Privacy Policy was the designated section for "Children." This section is imperative because it outlines how and when children should use their services. Vendor A states that products are not directed at persons under 13. Their personal information will be permanently deleted from the vendor's systems if they are underage. Having this clause ensures that the privacy of minors is kept confidential and aligns with the regulations set by COPPA. A practice that can be implemented to increase strict security measures would be to employ age verification during the registration process to improve the prevention of children under 13.

Lastly, the digital ticketing service provided their HECVAT-Full for the institution to review and have a starting point for an overall assessment of the service. Their HECVAT-Full gives the institution confirmation about the data, security policies, and compliance that are in place to protect sensitive information [52]. I determined Vendor A's host provider is Amazon

Web Services, and AWS will house the application and database. AWS will also host the institutional data, so the digital ticketing service company will not store it. This is relevant information because the reviewer can confirm that the organization is taking the extra step to enhance robust data security measures in a secure environment for sensitive data. Having the data stored in AWS ensures that Vendor A can continuously scale their resources for their needs and accommodate the volume of data, all while keeping up with the proper security and access controls to minimize the impact of risk incidents.

The Qualifiers Section of their HECVAT-Full indicated that Vendor A has a documented Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). However, the vendor should provide a reference to those documents and submit them along with the HECVAT. As of now, it has not been done and should be submitted for review. Having the BCP and DRP available for the organization can help the reviewer understand the IT plan to provide continuity and recovery procedures during and after the crisis.

The Authentication, Authorization and Accounting Section highlights and focuses on system authentication, restrictions, and password complexity. Vendor A answered "Yes" to the question, "Does your solution support single sign-on (SSO) protocols for user and administrator authentication?" Their system currently supports SSO via JSON Web Tokens. Passwords are standard with 2FA support. This means that once users are authenticated using SSO, they will receive a JWT token, which will be used to access services within the system, so they would not have to log in again. The system has the standard password requirements, so they will use username and password instances as their credentials. However, Two-Factor Authentication (2FA) is in development. Implementing 2FA into the system increases the layer of security by mitigating the risk of unauthorized access and requiring users to provide two different

authentication factors. This information provides the reviewer with an accurate representation of the steps and procedures the vendor has in place regarding authentication and authorization, which helps determine if the vendor is suitable to be implemented in the institution. It demonstrates that Vendor A meets the requirements to ensure that users can easily access their systems through SSO and secure the information inside the credentials through 2FA - creating a balance of usability and security for users' data.

Further on, Vendor A has created a series of establishments that will be used regarding password requirements. It includes enforcing a 90-day password iteration for password/passphrase expiration, using a link via email to document password reset procedures, having password complexity restrictions, and having 60 minutes of inactivity before locking the session. The password requirements established are within the best password security practices. Having password complexity restrictions such as minimum character length, uppercase, lowercase, number, and special characters ensures that passwords become more challenging to implement in a brute-force attack. 90-day iteration minimizes the risk of compromised passwords across the network because passwords are regularly updated, and users are discouraged from using similar repetitions. Locking the session after 60 minutes of inactivity ensures that measures are in place to help protect against unauthorized access and data leakage because users will have to sign back in to regain access to their system.

The Vendor A's Data Section contains questions and information about how the vendor handles and protects data. Vendor A answered "Yes" to important questions about sensitive data encryption, data backup, ownership, and data removal. To further elaborate, the vendor encrypts their sensitive data before transmitting it using TLS 1.2 features, ensuring unauthorized users can not read or tamper with the data between the client and the server. TLS1.2 is a secure encryption

protocol that protects sensitive data transmitted over networks [41]. Through TLS 1.2, data protection is evident because all data is encrypted, ensuring data integrity throughout transmission. Its functionalities include verification that data has not been modified or tampered with. The ownership right to all data, inputs, outputs, and metadata-based *is* retained by the institution, not the vendor. This comes from their documents provided that the institution owns all the data collected from customers and ticket sales, and institutions will have the data available after completion, breach, or cancellation of service before a database dump occurs. With ownership, the institution *can* request the removal of the data, and the vendor can delete all client data within 90 days. Their HECVAT-Full answers to the Data Section provide the reviewer with the necessary information to guarantee that the vendor falls within good standing for the institution to agree.

The Policies, Procedures, and Processes section gives the overview of how Vendor A will handle its internal documentation, policies, and procedures, aiming to assess the governance structure and practices in the specific areas. Reviewing their answers, Vendor A complies with major regulations that will benefit their client. They comply with applicable breach notification laws to inform their clients about affected individuals. This prompts the institution to protect itself from identity theft. Following breach notification laws also demonstrates how vendors and clients are continuing to build on their trust relationship because there is transparency and accountability. While they addressed that information to their client per the contract, it does not state how quickly the institution will be notified about the breach or the vendor's process for notifying the appropriate staff. Vendor A must provide the outline to the reviewer so it can be considered when assessing the third-party service. They state they will comply with the Institution's IT policies regarding user privacy and data protection. To ensure the accuracy of the

response, the vendor must review the Institution's IT policies and see how it will fit with their service.

After reviewing Vendor A's HECVAT, Privacy Policy, and the institution's Vendor Service Risk Assessment, it was deemed a Medium Risk. Following the flowchart mentioned previously, the vendor does not contain a significant compliance burden, so the next step is to see if it requires a log-in. There is an integration with SSO that leads to the complete TPR being performed. After the procedure and review are approved, the mutual contract benefiting both parties has been signed, and the service is used to sell online tickets for the institution's sports games.

Vendor B – Foreign Transcript Evaluator

Vendor B provides academic evaluations and verifications of foreign studies and translation services. Each vendor will vary in the documents they provide before the TPR is performed. From Vendor B, the institution was given the HECVAT-Lite, Business Continuity Plan, Information Security Policy, Data Protection and Risk Management Policy, and Privacy Policy. These documents provide answers to specific sections in the HECVAT-Lite. The institution completed its Vendor Service Risk Assessment, so the service request was approved to move forward.

The Privacy Policy was short and straightforward compared to Vendor A because the activities involved evaluating transcripts. The company will collect the data entered to provide accurate service to the client; this includes (1) credit card information, (2) information released for evaluations, and (3) contact information [54]. The credit card information is necessary because clients will need to pay a fee for processing foreign transcripts, which will be stored until the transaction is complete. The student's foreign institution information is kept on file;

however, data storage and protection are secured based on privacy regulations addressed in their Data Protection and Risk Management Policy.

Vendor B provided its Data Protection and Risk Management Policy, which refers to how all parties to the company's data are treated with confidentiality. The policy explains what data is being collected and how it will be handled within the organization and adheres to the desired states that need to meet the applicable requirements of Data Protection of Adelphi's TPR Service Assessment Checklist [49].

The collected information includes personal information, identification, and necessary educational documents. The ability to request data retrieval is essential, especially when it is institution-owned data. Vendor B states that data will be removed from databases, archives, and backups upon the data subject's request, meeting the desired state. There are also specific practices in place to dispose of the data mentioned. The information is stored in the servers and maintained for five years before being deleted. From reading their Data Compliance, they are taking certain steps to ensure data protection – multiple-factor authentication, strong password etiquette, and limiting the transfer of data between company-used systems and reporting parties of the organization about any previous breaches or disasters [56]. Another critical step they take is to regularly review all policies and current legislation to ensure that the requirements for procedures are constantly met.

Vendor B was the first service reviewed that provided the institution with a BCP – DRP and Information Security Policy. Provided an example of what a disaster plan looks like. Vendor B attached their Business Continuity Plan focusing on the IT Disaster Recovery Process. The document outlines the process to recover servers and backups on the organization's devices if a disaster occurs. A disaster refers to a major crisis that affects the business. The document

included an overview of the specific components of the backup environment, different possible scenarios, and detailed recovery strategies for each [58]. The institution can visualize and understand how the vendor's data centers and backup configuration work, making them aware of the recovery plan and ensuring that their stored data can still be secured.

Scenarios ranged from simple recovery of files to the worst-case scenario of data center loss. A simple file recovery includes accidentally deleting and overwriting files or virus infections. The worst-case scenario would be the loss of the primary data center due to a natural disaster or human disaster. Detailed explanations about the scenarios and strategies ensure the institution understands the recovery time objective (RTO) based on the crisis [49]. Having a determined and feasible RTO helps the organization and its clients tentatively determine when operations need to be resumed before the crisis compromises the ability of the organization to function fully [43]. It serves as a set goal for how quickly the organization should try to get back on track after the disruption of a crisis and avoid critical dependencies on others. It is interesting to see a layout of a Disaster Recovery Process because it gives an idea of what PreK-12 institutions should look for when they start assessing third parties before agreeing to its terms. They will know how to recover the data and a step-by-step guide of what the organization is doing so there are no surprises.

An Information Security Policy creates the best-case scenario for protecting the institution's data, giving security awareness and the practices from the vendor's perspective [57]. Vendor B's policy outlines the limitations and restrictions that employees or any affiliated party must abide by regarding acceptable use. The policy applies to using information, electronic and computing devices, and resources to conduct day-to-day operations [57]. Their policy states that proprietary information is the vendor's property, and they implement high password security

measures to ensure restricted access and prohibited activities. The password security measures that are in place increase confidentiality and data protection because devices are secured with a password-protect screensaver. Access is minimal because users should not know others' login credentials. The Unacceptable Use section outlines prohibited activities, including unauthorized copying of copyrighted material, accessing data and accounts for non-business purposes, and disclosing confidential or proprietary information. The section forces the employees to adhere to guidelines to maintain the security and integrity of the organization. The document is simple to understand; explaining the activities helps the employees know what needs to be followed, and the institution knows how the organization keeps the employees in check. Clearly outlining the prohibitions and the acceptable use demonstrates that the organization is taking responsibility and accountability for protecting the students' data.

This vendor is considered Low-Risk because it has provided the HECVAT-Lite as its assessment as it is not processing critical data. Like Vendor A, their HECVAT-Lite more concisely covers the key components. After reading their HECVAT and additional documents, I found that the vendor already meets specific requirements based on Adelphi's TPR Service Assessment Checklist [49]. The findings are explained below.

Authentication and audit requirements include supporting MFA and meeting audit logs. In their HECVAT–Lite, Vendor B states that MFA is always required for their employees to access the systems and limit access to company-owned devices. Although the Vendor B method of MFA is not integrated through Security Assertion Markup Language (SAML), they explicitly state that they are leveraging strong MFA, using mobile apps and built-in authenticators such as Microsoft Hello, which servers to use an authentication factor as a method of signing in to the devices. Vendor B also states that audit logs, such as login history, are available to system

administrators if needed. This is useful because IT staff can access logs to perform their audits [55].

The institution conducted its Vendor Service Risk Assessment on Vendor B. They stated the service is at a high risk of service unavailability if caused by a service outage. It is considered high risk because they would not have the transcripts of international students evaluated at a particular time [59]. They provide a solution because they have relationships with other agencies offering similar services. This shows that the institution can continue providing translation and evaluation services for its international students. The information throughout stays accurate and consistent when comparing the answers to the Vendor Service Risk Assessment to the submitted documents. I did not find any discrepancies.

The most significant difference between Vendor A and Vendor B is their documents. Vendor A just provided their HECVAT-Full and Privacy Policy, while Vendor B was able to support their answers by providing additional policies and plans to help evaluate how they can fit into the institution. Reviewing and analyzing Vendor B's third-party review using the Adelphi TPR Checklist determined that Vendor B is considered a Low to Medium Risk. It is on the Low-Risk scale because they completed the HECVAT-Lite, designed mostly for vendors not dealing with critical services, such as translating transcripts. They completed an assessment questionnaire and provided additional information that supports their business continuity plans and notification of recent breaches, keeping them in good standing. Vendor B has not completed the Cloud Security Alliance self-assessment nor related independent certifications, which assess the risk as Medium. It raises the challenge of understanding its results by evaluating cloud security controls and measures. However, Vendor B does not bring a significant compliance burden as its shared policies provide the reviewer with further insight into specific controls and

practices that *are* in place. Moving further along the Triage Workflow Chart, it will be deemed a Medium Risk due to its support with MFA. It leads to IT staff being involved in administering and overlooking its controls. Vendor B is another great example of how an institution goes through the process of carefully reviewing a third-party to make sure that the service provided fits the needs they are looking for.

Vendor C – Productivity and Note-taking Web Application

The last vendor reviewed was a productivity and note-taking web application. The institution has used the application's free version in the past; however, they want to upgrade to help keep track of the organization's happenings. Vendor C is very similar to the previous vendor reviewed because they have gone through the full TPR procedure to have an agreement with the institution.

Vendor C's Privacy Policy has been the lengthiest one so far. Through the document, they explain in detail how the application collects information in various ways, including some of the following: (1) information necessary and required to create an account, (2) payment information to process subscriptions, (3) contact information for communication services, and (4) browser information for third-party advertising technology partners [60]. Their Privacy Policy mentions payment information; it is essential to note that the transactions will be done through a third-party service, which limits the PCI-DSS exposure. No compliance exposure needs to be addressed in risks related to FERPA, HIPAA, or GDPR [49]. No student, medical, or GDPR-related PII is used for this application. Once again, the application helps administrators improve productivity. The Privacy Policy mentions that the vendor will store the information received as long as the client uses the Services and the contract is active. Like Vendor A, Vendor C has a section dedicated to Children's Information. While there is no specified age, if children's

information is collected without parental consent, the vendor will remove the data as soon as possible. Vendor C serves a higher education institution, so there is no worry about children-focus rules and regulations. Still, it helps to understand how the application functions if it encounters such problems in primary and secondary education administration.

Vendor C also included their Incident Response Plan (IRP) and Disaster Recovery Plan. The IRP focuses on establishing specific controls to detect security vulnerabilities and incidents and the vendor's response to breaches. In summary, their policies focus on detecting information security weaknesses, forcing users to report vulnerabilities as soon as possible, ensuring proper scanning and reporting mechanisms are in place for the service, and, lastly, the procedures to recover operations after a disaster. While their IRP/DRP does not specify the exact RTO, through the explanations provided about the phases in which the organization will manage and assess disruptive threats, it is appropriate to determine that they have a plan for a desirable and feasible RTO [61,62]. Secondary workflows are also in place [49]. The responder notifies the management so they can alert the proper engineering team and coordinate the assessment procedures to determine recovery time. If necessary, the team will provide the details of how a relocation will occur so team members can prepare beforehand. This will put the Recovery phase in action to restore temporary operations. We have reviewed two versions of a DRP, and they have both provided the institution with enough information and details. The plans outline the procedures and protocol necessary to ensure that while the organization is recovering the systems, the institution knows how the data collected is handled in a disaster. This currently puts Vendor C in a Low-Risk area for having applicable desired states regarding Business Continuity.

For Authentication and Audit, Vendor C integrates with SSO with SAML. With SAML, you can enable a single sign-on (SSO) experience for your users across any two applications that

support SAML protocol and services, allowing an SSO to perform several security functions on behalf of one or more applications. This alleviates the need to remember login credentials constantly and increases the system's security. Vendor C provided the institution its SAML SSO configuration worksheet, allowing IT administrators to manage team access and keep information more secure. The worksheet specifies how to enable SAML SSO for a single workspace; this helps IT administrators understand how to incorporate this into their system depending on their Identity Provider Setup - in this case, Google [64]. Another authentication method Vendor C has in place is Sign-in with Google, which helps you quickly and securely sign in to third-party apps or services with your Google Account.

Vendor C had their System and Organization Controls 3 (SOC 3) report as part of additional documents, as SOC 3 can be freely distributed publicly to other organizations. The report assures clients that the vendor has the correct controls and processes for protecting sensitive customer confidential data [63]. They have not provided a completed HECVAT assessment; however, the vendor shared their different policies that can supplement the questionnaire. Reading the policies carefully can give the same insights as a HECVAT. Vendor C shared their Business Continuity plans with the institutions, which is something we can check off the checklist. The vendor stated in the Privacy Policy that they will communicate security, privacy, and administrative issues with the client. Most importantly, they will try different methods of communication to notify clients about a security system breach. They mentioned that they would notify the client. The vendor did not mention the procedure they would take or if they had recent breaches. This information can assess the risk as Medium due to the lack of appropriate response to breach notification.

The Vendor Service Risk Assessment clearly stated the purpose for requesting this service implementation. We know that the service will be used by the facility's administrators rather than students because of the scope of what they are trying to accomplish with the note-taking web application. There is a low risk of service unavailability because there is already an integration with team communication software that can serve as a backup if information is lost during downtime [65]. The information the institution provides includes but is not limited to name, email address, password, team role, and profile picture. However, the data the application collects is only name and email address, consistent with their privacy policy. Regarding signing up, the service supports SSO with SAML and Sign-in with Google. A new question in Vendor C's assessment is if the service comes into scope for Title IV Third Party Servicer (TPS). The question does not pertain to the vendor's scope, which once again is to help keep track of necessary fixes of the organization. No student data or privacy is involved because administrators will handle the application - so the answer was non-applicable.

The vendor is considered a Medium Risk because no critical risk or significant compliance burden is specified and explained through their documentation and reports. The productivity and note-taking application requires a login to access the administrators' data and files stored in their workspace. The application integrates SSO for authentication to access its services. This leads the institution to perform its full TPR, and findings will be given to the procurement department so they can decide if they will enter an agreement with Vendor C.

Recommendations and Best Practices

10. Possible PreK-12 Implementation

There are many services that primary and secondary institutions are using as services and instructional tools. Many institutions have implemented basic ones such as Google Workspace or Microsoft Office. However, there are diagnostic tools that provide safe and reliable learning assessments for students, school management systems for faculty to facilitate administrative tasks, and scholarship management software for parents to manage their students' enrollment and financial services. Primary and secondary schools are slowly implementing these tools and software into their schools. However, institutions must implement and follow a rigorous review before they agree to have their member's data collected.

The reviewer will obtain the proper information from the third-party to determine the specific areas where the service or software will be installed, such as school devices. Aside from specifying areas, the third party needs to address what services that third-party will provide. Examples include enhancing academic performance and stating what are the security measures. Security and performance requirements can be developed by the institution's IT and Security Department.

Creating a Third Party Review Procedure focused specifically on PreK-12 will address the gaps between institutions and acknowledge that differences must be considered in a vendor assessment. There are differences between a PreK-12 and a higher education, including their IT team and their complexity within their scope for institutional requirements. The difference between a higher education IT department and a PreK-12's could be the size of the personnel involved. In colleges and universities, the IT and Security departments tend to be larger due to

the scale and complexity of the operations constantly performed. In higher education, the team may consist of network and system administration and security specialists who work together to maintain the proper functions of the institution's infrastructure and ensure data security and privacy compliance. In contrast, PreK-12 schools may have a smaller IT and Security team focusing on smaller tasks. Tasks may include managing technology needs and maintaining devices and software. The staff may be small but have to handle different responsibilities, one of them being reviewing possible vendors that can be integrated into the school system to facilitate student and administration's workflow. Additionally, higher education requirements may differ for a primary and secondary school. Higher education may have complex role structures, advanced student-oriented programs, and research activities that require robust and specialized technologies. On the other hand, primary and secondary schools may have more straightforward objectives, such as aligning with the Department of Education standards and fostering learning opportunities related to an outlined curriculum. Some schools may have research activities for students, but they may not be as complex as in a university.

Therefore, my implementation will benefit their IT personnel in organizing and managing their workflow more efficiently. A PreK–12 implementation will ensure the vendor technology solutions closely align with the institution's specific needs and cloud service requirements. They will have a proper checklist and guidelines they can follow to determine whether or not the service poses a risk and later make their final decision.

The sample TPR implementation can start with a Triage Workflow Chart. Like a higher education institution, PreK-12's Information Technology department should create a Triage Workflow Chart that outlines what they will look for when reviewing the service and, depending on its response, lead to more questions to get the full scope of its risk and future steps. Having

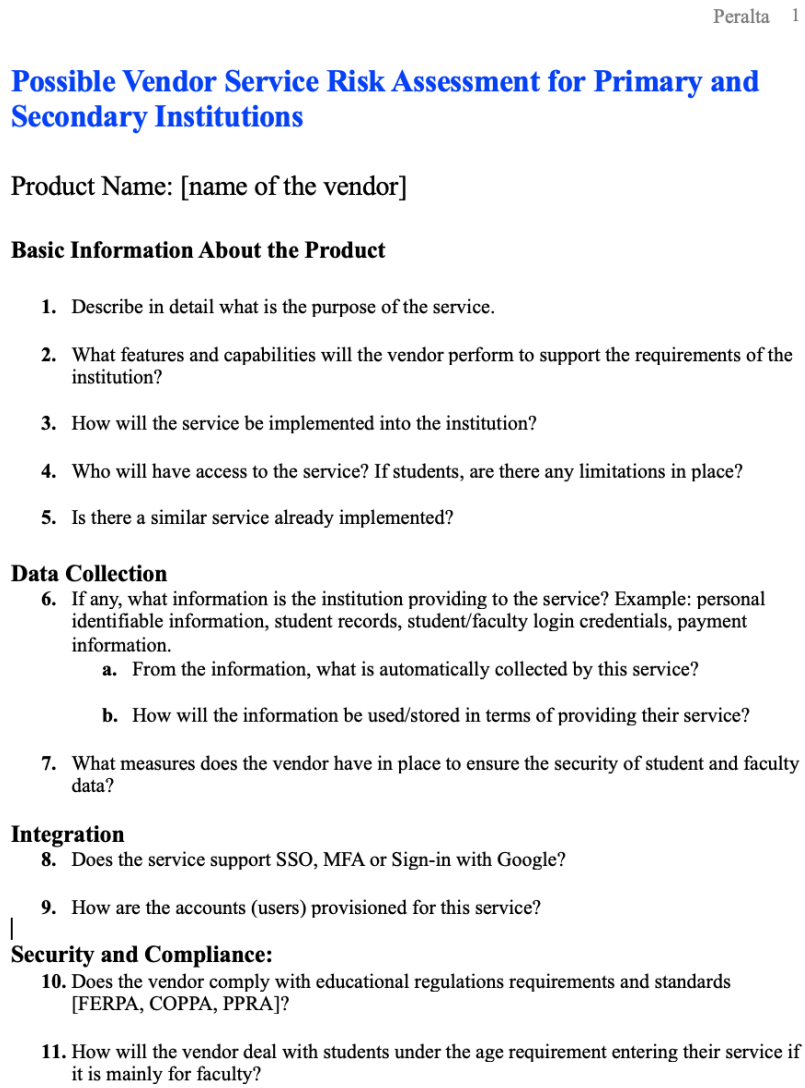
the chart will allow for efficient assessment of the third party. It is important to know what potential risk the third-party poses to the institution. The vendor should also comply with completing a VSA or similar questionnaire, so it gives the reviewer details about the vendor's compliance, data governance, and security protocols. The questionnaire will be reviewed; if needed, the reviewer will ask for clarification on certain questions. Clarification can explain where the data is stored, and answers can include Amazon Web Services, Google Cloud, or Microsoft Azure. After clarification and questionnaires are reviewed, the next step will be to create a TPR and Business Impact Assessment based on the chart and questionnaire assessment. Having a good understanding of all the important privacy and security procedures that the third-party offers will allow the reviewer to come to a good conclusion about the safety usage of the service/software for children.

Based on reviewing the methods and TPR procedures used by a higher education institution, a TPR procedure and vendor assessment toolkit can be created focusing on primary and secondary education. A Triage Workflow Chart is the first step because it leads to questioning how the institution will use the service and how it affects them in the long run. A similar chart to Figure 05 can be utilized, and it will be designed by each institution's Information Security Officer to cater to the institution's requirements and concerns. Secondly, each institution should create a Vendor Service Risk Assessment that prompts the answers to necessary questions to determine the probability and impact the service will have, along with questions about compliance with children's protection regulations. Thirdly, the implementation includes a sample vendor assessment tool (like HECVAT) but focuses on how we can manipulate it for primary and secondary - named Primary and Secondary Vendor Assessment Questionnaire

(PS-VAQ). The PS-VAQ is a general questionnaire that vendors can complete and could be accepted by many PreK-12s.

10.1 Possible Vendor Service Risk Assessment for Primary and Secondary Institutions

Figure 06 is a sample of a possible Vendor Service Assessment for Primary and Secondary Institutions. The worksheet is divided into sections, with questions that the reviewer can answer based on the information and documents received from the vendor.



Peralta 1

Possible Vendor Service Risk Assessment for Primary and Secondary Institutions

Product Name: [name of the vendor]

Basic Information About the Product

1. Describe in detail what is the purpose of the service.
2. What features and capabilities will the vendor perform to support the requirements of the institution?
3. How will the service be implemented into the institution?
4. Who will have access to the service? If students, are there any limitations in place?
5. Is there a similar service already implemented?

Data Collection

6. If any, what information is the institution providing to the service? Example: personal identifiable information, student records, student/faculty login credentials, payment information.
   a. From the information, what is automatically collected by this service?
   b. How will the information be used/stored in terms of providing their service?
7. What measures does the vendor have in place to ensure the security of student and faculty data?

Integration

8. Does the service support SSO, MFA or Sign-in with Google?
9. How are the accounts (users) provisioned for this service?

Security and Compliance:

10. Does the vendor comply with educational regulations requirements and standards [FERPA, COPPA, PPRA]?
11. How will the vendor deal with students under the age requirement entering their service if it is mainly for faculty?

Figure 06: Possible Vendor Service Risk Assessment for Primary and Secondary Institutions

The first section of the worksheet is to get basic information about the vendor, such as their name and details about the service, which will help understand the functions of the service and how it will play a role in the institution. The second section is about data collection. The professional in charge of reviewing the vendor needs to know what information they will be providing to them and how it will be handled/modified. The third section is about integration into the already in-place operating systems. Questions include how the service can be integrated into SSO, MFA, or Google Sign-In. Knowing how users will log in to the system clears up concerns about security and access control with authentication methods. The Last section focuses on security and compliance for PreK-12, especially for underage students; we want to ensure the service complies with education and privacy regulations. Complying with such regulations ensures that the data of students and other users is always kept confidential. Depending on specific requirements and standards the institution wants to meet, the assessment can be modified to fit them better.

10.2 Primary and Secondary Vendor Assessment Questionnaire (PS-VAQ)

Figures 07-13 are the sample PS-VAQ implementation. Vendors should complete the questionnaire as best as they can. The questions in this questionnaire were derived from our data collection analysis and the requirements and standards developed in Section 7. This implementation aims to simplify the process that the IT Department of a PreK-12 institution does when deciding to agree to a new service. It will be used as another technique when reviewing the privacy and security measures that the vendor takes to ensure confidentiality, integrity, and availability of their service for users. The simplified questionnaire offers an organized approach for individuals to evaluate services, even if they possess minimal background knowledge of IT

security. The questions in this assessment are meant to be straightforward and have understandable wording for both the vendor and the reviewer. Compared to the HECVAT, the PS-VAQ lays a specific criterion for vendors to prioritize functionality, compliance with educational regulatory requirements, and communication efforts. It focuses on essential areas relevant to PreK-12 education, trying to tailor to possible challenges within their environment. The HECVAT focuses on privacy and security controls, considering system and data infrastructure and Change Management; some of these needs are unique to higher education [37]. With this said, only some sections apply to a reviewer in a lower education field who may be looking for a concise assessment. The PS-VAQ is similar to HECVAT as it assesses appropriate areas of possible risk but takes a different approach in focusing on how the vendor provides adequate service delivery methods to their clients. Vendors will explain how they can meet the general needs of a school through the reliability and accessibility of their products. The questionnaire will address the necessary privacy requirements to safeguard cloud-based student data and inquire about strategies to alleviate concerns about handling minor's data. Here, institutions can look for policies and procedures the vendor may have about data collection, usage, and sharing. Another aspect that makes the PS-VAQ stand out is its questions about engagement and satisfaction. While these questions may not necessarily deal with assessing risk, it is important to know how an organization is not just about gaining a client but also ensuring they retain them and allowing them to provide feedback to continue their improvement efforts.

Part 1 is General Information. This section is about obtaining information about the vendor, including their name, product, and contact information. Contact information is essential because it demonstrates a point of contact that can answer questions and address concerns. It also enables good communication, support, and trust between users and vendors.

Primary and Secondary Vendor Service Assessment		
Completed By:		
Date		
	Questions	**Vendor's Answers**
Part 1: General Information		
GEN - 01	Vendor Name	
GEN - 02	Product Name	
GEN - 03	Product Description	
GEN - 03	Vendor Contact Name	
GEN - 04	Vendor Contact Title	
GEN - 05	Vendor Contact Email	
GEN - 06	Vendor Contact Phone Number	

Figure 07 - Part 1: General Information

Part 2 is Documentation. The section ensures that the IT professional understands the vendor's practices and policies. It will allow the reviewer to assess whether they align with their requirements. First, there are questions regarding whether the organization has a Privacy Policy and Terms of Service. Questions about CAIQ refer to acquiring insight into whether the organization has completed the survey about the security capabilities of a Cloud Service Provider they are working with. Having the CAIQ Star Certification can play a critical role in gaining trust from the institution and ensuring there is transparency and security within cloud computing. The questions were inspired by HECVAT standard security and certification questions.

Part 2: Documentation		
DOC - 01	Does the organization have a data privacy policy? If so, please attach the link to the policy.	
DOC - 02	Does the organization have a Terms of Service? If so, please attach the link to the document.	
DOC - 03	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, ISO 27001, etc.)	
DOC - 04	Has the vendor completed Cloud Security Alliance (CSA) self assessment or CAIQ? If so, please attach a copy of the results for reviewal.	
DOC - 05	Has the organization hold any certifications (SOC 2, CAIQ STAR certification)?	

Figure 08 - Part 2: Documentation

Part 3 is Data. The section has questions concerning data storage and management, controls, and procedures for deleting data. Questions 1-5 ask about the collection of specific data. It is important to know what data the institution provides is being collected. We want to know how it will be stored and used while it is in the data center. Vendors want to perform their operations for high performance and at a grander scale, so they would opt for a host. Asking about a vendor's host option can help the professional understand the organization's suitability and how the environment interacts and deals with cloud data. Questions about encryption are necessary because they give an overview of the organization's measures for protecting sensitive data and mitigating opportunities for unauthorized access. Vendor B provided the higher education institution with its Data Protection and Risk Management Policy, which gave the idea of including it in the questionnaire because, if applicable, it can provide detailed information about data security, privacy, and procedures for risk management. Overall, the reviewer can confirm the organization's objectives of ensuring trust and following the CIA Triad. Questions 9 – 12 ask who has ownership, access, and sharing rights if third parties are involved. Questions 13 – 14 focus on figuring out the procedures when it comes to the deletion of data. The section met with data collection and transparency requirements discussed in Section 7. The vendor is demonstrating full transparency by providing details about their data collection methods and what controls they have in place regarding data encryption and backups. In addition, maintaining clear documentation outlining their data handling ensures the institution has full transparency between the operations that are taking place and vendor's communication in a scenario of compliance exposure. To reiterate, there should not be a risk of FERPA, COPPA, PPRA, or

HIPAA in services where they are applicable. If there is a possible risk, the appropriate controls should also be stated.

Part 3: Data		
DATA - 01	What data is being collected and what are its usage in the Cloud Service Provider's data center?	
DATA - 02	How will be the data be collected and stored?	
DATA - 03	What will be the hosting option for such data?	
DATA - 04	Provide details about how the organization will process credit card information. If applicable, how are you complying with PCI-DSS?	
DATA - 05	Provide details about how medical information will be stored and processed. How are you complying with HIPAA regulations?	
DATA - 06	How does the organization ensure data integrity and confidentiality?	
DATA - 07	How do you encrypt client data?	
DATA - 08	Are regular backup being performed? If so, how are they encrypted?	
DATA - 09	Do you have a Data Protection and Risk Management Policy? If so, please provide details or documentation.	
DATA - 10	Who has ownership of the data from the institution?	
DATA - 11	Which groups of staff (individual contractors and full-time) have access to personal and sensitive data handed to you?	
DATA - 12	Do you share institution's data with third parties that you are in contract with? What are the purposes for such and are there restrictions/limitations?	
DATA - 13	What steps are taken to ensure that data is permanently data or returned to the institution after termination of contract?	
DATA - 14	How will data be deleted from backups as well?	

Figure 09 - Part 3: Data

Part 4 is Service. This section focuses on allowing the vendor to speak more about their service regarding delivery, engagement, and management. Questions are derived from thinking about how the questionnaire can stand out and be geared toward possible children's usage. Questions 1 and 2 address the concern about parental consent. Vendors need to explain how their service conveys the importance of parent involvement and continuing their commitment to transparency and compliance. Question 3 asks about customization options based on users or age. Some web applications can be utilized by faculty and students, but not everyone can access

all available options. Another example is that all students in the school have access to a platform to read books, answer questions, and improve their reading; however, some book content may be too harsh or not considered age-appropriate for younger students. Considering these scenarios, if institutions see that the vendor provided information content restriction and tailored options for specific users, it will alleviate the worry of what a child may have access to when using the service. Question 4 refers to vendors explaining if they have opt-in and opt-out mechanisms in place, which will help assess their management within privacy settings and even if they comply with CCPA, discussed in Part 5 of the questionnaire. Question 5 deals with understanding how a vendor is interested in prioritizing how their service can assist schools in fostering a good education for their students, especially if their purpose is a learning tool. The vendor should answer this question if they deal with student learning purposes. Questions 6-7 will help vendors demonstrate that they care about user engagement by accepting feedback and improving the long-term satisfaction and reliability of service.

Part 4: Service		
SER - 01	How will the organization involve parents and/or guardians in the service delivery process to ensure alignment with needs and proper consent?	
SER - 02	If the service requires parental consent, what procedures does the organization follow to obtain consent and ensure it is being respected?	
SER - 03	Will there be restrictions on the type of content provided by the services? For example, will there will be different aspects of a service depending on their role or age?	
SER - 04	What parts of the service have opt-in and opt-out mechanisms and how is it managed?	
SER - 05	If applicable, how does the organization ensure its service aligns with general educational goals?	
SER - 06	Can the users provide feedback to the organization?	
SER - 07	How will the organization address any challenges that may occur in the future in effectively continuing to deliver services for students, faculty, and administration in PreK-12 setting?	

Figure 10 - Part 4: Service

Part 5 is Governance, Compliance, and Standards. There are just a few questions. However, they meet the requirements for transparency and compliance. Questions refer to data protection compliance, such as GDPR - a privacy regulation explained in a previous section. There are questions about student privacy, such as those related to FERPA, COPPA, and PPRA. There should not be a risk of exposure in services where these regulations are applicable. If there is a possible risk, the appropriate controls should be stated in the assessment or through additional documentation. Including questions about security assessment, audits, and testing ensures that vendors are up-to-date with standards and aware of potential vulnerabilities. This also ensures that policies and procedures are constantly updated. There are questions about third parties. Sometimes, vendors will resort to third parties to complete some processes. An example is Vendor A, who used a third party to process payment of tickets. That is why the reviewer must know how the vendor handles data and how it is secured. Lastly, questions 7 and 8 pertain to state-level regulations, specifically the California Consumer Privacy Act. These two questions can help educational institutions assess how vendors comply with CCPA and determine the effectiveness of the vendor's practices for ensuring commitment to protecting consumer personal information. The institution can evaluate a vendor's responsibility to comply with the appropriate laws and regulations in this section.

Part 5: Governance, Compliance, and Standards		
GCS - 01	Is the contract established and maintained with cloud-related special interest groups and other relevant entities?	
GCS - 02	Are the policies and procedures reviewed and updated at least annually?	
GCS - 03	How does the organization comply with relevant data protection regulations (e.g. GDPR)?	
GCS - 04	How does the organization comply with relevant student privacy regulations (e.g. FERPA, COPPA, PPRA).	
GCS - 05	Do you conduct regular security assessments, audits, or penetration testing? If yes, please provide details.	
GCS - 06	Are there any third-party data processors involved in handling the data? If yes, provide details of their security measures.	
GCS - 07	Does the organization comply with the California Consumer Act (CCPA) regarding information collection, usage, and protection? If applicable, how does it pertain to PreK-12 children's data in educational settings?	
GCS - 08	If the organization is compliant with the CCPA, describe how it is taking certain steps to handle clients' (including children's) information.	

Figure 11 - Part 5: Governance, Compliance, and Standards

Part 6 is about Authentication and Access Control. Questions focus on password policies, authentication methods, and access control. Like our sample Vendor Service Risk Assessment, there is a question about supporting Single Sign-on (SSO), Multi-factor Authentication, or Google Sign-in. This question is brought up again so the vendor can provide more details about how their solutions include authentication protocols that can be integrated with the institution. Different services can be directly for solely just faculty or students; however, there could be services that both users can use. That is why there is a question to ask if users have different log-in requirements. Some children may be unable to log in through MFA, so navigating the site and accessing the services can be difficult. Questions related to password policy and techniques were derived from HECVAT as they have specific and detailed questions about resetting and

password complexity that can be useful for primary to higher education. Lastly, questions about access control mechanisms will give detailed information about the vendor's safeguards. Asking such questions can reveal how vendors grant access and permissions to resources and data. Overall, this section aims to learn more about how to protect user accounts and authorized access.

Part 6: Authentication and Access Control		
AAC - 01	Does your solution support Single Sign-on (SSO), Multi-factor Authentication, or Google Sign-in?	
AAC - 02	What is the process for authentication integration with the system already at hand?	
AAC - 03	Do login requirements differ from students and faculty users?	
AAC - 04	Does your application support integration with other authentication and authorization systems?	
AAC - 05	Do you have documented password reset procedures?	
AAC - 06	Does the system have password complexity and/or restrictions?	
AAC - 07	How frequently are users required to change their passwords?	
AAC - 08	Are there procedures for resetting or forgetting a password?	
AAC - 09	Are there measures in place to prevent weak passwords and preventing data breach attacks?	
AAC - 10	What are the procedures taken to prevent unauthorized access to sensitive data or organization resources?	
AAC - 11	Does the organization implement role-based access control to manage user permissions?	
AAC - 12	Can users request access to additional functionalities outside their scope of work? How would the process look like?	

Figure 12 - Part 6: Authentication and Access Control

Part 7 is based on the standard for Business Continuity Planning. The questions help the institution know about the vendor's preparedness for a disaster and recovery plans to continue operations. Vendors reviewed provided a document about the BCP and DRP, so asking vendors if they have the documents was a great question. However, the information may be confidential for some organizations, so there is a question about whether the institution can review those

documents beforehand. Aside from having detailed and efficient plans in place, we need to ask if they have been tested in the past and what were the outcomes. Knowing this can help the reviewer mitigate the concern of possible risks for data loss and low chance for recovery. While we can see results from the summary of tests, sometimes circumstances change, and new scenarios may have probability and impact. That is why we ask the vendor for a time frame for updating their DRP or IRP.

Part 7: Business Continuity Planning		
When applicable please attach documentation to be reviewed		
BCP - 01	Does the organization have a detailed Business Continuity Plan?	
BCP- 02	Does the organization have a detailed Incident Response Plan?	
BCP - 03	Does the organization have Disaster Recovery Plan in place?	
BCP - 04	How will clients be communicated if a disaster occurs?	
BCP - 05	Can the Institution review your DRP and supporting documentation for BCP?	
BCP - 06	Has the previously mentioned plans been tested in the past? Please provide a summary of the most recent results.	
BCP - 07	Are the plans updated annually or at a reasonable time period?	

Figure 13 - Part 7: Business Continuity Planning

Part 8 is Notification of Breach and Termination of Contract. This section closes the sample PS-VAQ with questions about data breaches and termination. Questions 1- 4 deal with notification of breaches, while Questions 5-9 are about the termination of contracts. There will be scenarios where vendors may encounter a breach or a data risk, so they should plan how they will go about it. The clients and their organization need to know about a breach, but it will be up to them to see how much information they will release. There should be a log or tracker about past vulnerabilities and threats to outline what needs to be further worked on to avoid a potential incident. The second patch includes general questions about processes and management after

termination. As the contract ends, the institution needs to protect the data initially stored by the vendor and know the following steps to retrieve it. The questions provide transparency, accountability, and compliance for the vendor's side.

Part 8: Notification of Breach and Termination of Contract		
NBTC - 01	What are the procedures and processes taken in the event of a breach?	
NBTC - 02	How would you go about notifying clients and stakeholders about a breach?	
NBTC - 03	How much information is being released about the breach, in terms of details, extent, and affected areas?	
NBTC - 04	How do you keep track of security vulnerabilities and threats that have occurred?	
NBTC - 05	What would the circumstances that would allow for a termination of contract between both parties?	
NBTC - 06	Does the contract state their process for a termination of contract?	
NBTC - 07	For the data that is being collected and processed by the vendors, what will be the procedure for transferring back to the institution?	
NBTC - 08	Is there a time period where there will be a continuation of services until all necessary data is transferred back/removed?	
NBTC - 09	Would it be possible to transfer data to other vendor due to termination of contract?	

Figure 14 - Part 8: Notification of Breach and Termination of Contract

It is recommended that an educational institution have a Third Party Review procedure in place because it provides a structured framework for assessing and managing risks when agreeing to add a new service to the school facilities. The procedure will make the transition from reviewing to implementing a new service easier because the IT professional knows the key components to look out for and quickly evaluates the quality and reliability of the potential service based on the assessment. Just like the vendors can complete the HECVAT to provide the higher education institutions with insights about vendors' capabilities, security practices, and other procedures, the PS-VAQ will serve a similar purpose for primary and secondary education. The PS-VAQ is a general questionnaire that any prospective vendor can complete and an

assessment tool that can be used by multiple PreK-12 institutions across different districts. Having the PS-VAQ promotes consistency in vendor evaluation and TPRs with schools and any range of IT personnel. After reviewing a vendor's PS-VAQ, the reviewer can use the Vendor Risk Assessment Worksheet to evaluate the potential and visible risks associated with engaging with the vendor. The worksheet can be completed based on the analysis conducted by reviewing the completed questionnaires and additional documentation provided by the vendor.

My sample PreK-12 Third-Party Review procedure benefits the institutions and the vendors in multiple ways. Firstly, vendors gain new clients because they enter into a contract for a specific time frame to provide their service. More importantly, vendors gain clients as they continue building their client-service relationships. A strong relationship is built on trust, transparency, and accountability, which is evident when the vendor is engaged and committed to providing accurate responses and documentation about who they are. Clients know the full scope and can see that vendors take the TPR procedure seriously by providing a completed PS-VAQ and additional documentation when necessary. The results of such a procedure can ultimately lead the school to trust the vendor and its services, get into an agreement, and continue to renew the contract if everything is running smoothly. By adopting my version of a TPR tool at schools or later in districts, vendors can gain more insight into improving the current measures and processes in some areas of their organization. Vendors can identify and address potential risks through critical thinking and self-reflection about their operations, reducing the likelihood of experiencing vulnerabilities. This tool establishes consistent evaluation criteria when vendors are in the process of obtaining a new client. Lastly, having completed the PSQ-VAQ for one school, they will have a more straightforward process with other schools that may also start to use the questionnaire.

Conclusion

Cloud computing infrastructure has benefited a wide range of applications in different industries, specifically educational institutions. Through cloud computing, cloud services have enabled institutions to facilitate their operations and collaborations among different clients. Cloud computing provides scalability, customization, and cost-effectiveness for institutions looking to implement certain services; however, it is important to highlight that there are still concerns. By using such infrastructure, service providers can utilize a specific cloud deployment and service model to administer adequate resources that their clients are looking for efficiently. Education institutions rely on those providers for particular resources and trust that they are reliable, secure, and compliant with regulations and standards. Despite their usage of the service, some users will be concerned about the privacy and security of their cloud data. When using applications or web services, data is stored in cloud storage platforms, so clients are not fully aware of how the service works internally, only what is visible from the outside. Institutions have different services that school members constantly use, including learning tools for students and teachers, administrative applications for faculty, and SaaS such as Google Workspace or Microsoft Office. The members utilize the services provided to them, but it is up to the IT personnel to ensure that the services integrated into the school adhere to the best practices for privacy and security.

Higher education institutions like Adelphi University have a Third Party Review procedure that potential vendors go through before getting integrated. The Third-Party Review ensures that vendors meet a strict set of requirements focusing on data security, compliance, and

trust for the overall benefit of the institution. Thoroughly reviewing three important security questionnaires and frameworks, HECVAT, VSA, and CAIQ, facilitated the task of developing the best standards and requirements. Keeping such requirements and the example of a third-party review in mind, the data collection process was streamlined when analyzing the three vendors.

There was enough information to create a set of recommendations for primary and secondary education institutions. The Primary and Secondary Vendor Assessment Questionnaire is a general and standardized questionnaire aimed to help PreK-12 institutions assess third-party vendors' data security and privacy practices, touching base on requirements and aspects from Sections 7 and 8. Each school's IT department needs a Vendor Service Risk Assessment worksheet that institutions can modify to their specific standards and needs. This worksheet will help evaluate and manage the risks associated with the potential vendors.

Good practices are important when managing students' data to ensure that privacy and security are an advantage, not a concern. If schools and districts adopt this tool, it will benefit both the vendor and institutions by promoting excellent transparency, accountability, and trust in vendor relationships. The practices and implementations for primary and secondary education developed in this research aspire to mitigate this concern and ensure that students, teachers, faculty, and parents utilize a service that brings them workflow benefits.

References

1. Kässer, Matthias, et al. “Clearing the Air on Cloud: How Industrial Companies Can Capture Cloud Technology’s Full Business Value.” *McKinsey & Company*, 25 Feb. 2021, www.mckinsey.com/industries/automotive-and-assembly/our-insights/clearing-the-air-on-cloud-how-industrial-companies-can-capture-cloud-technologys-full-business-value.
2. Mell, Peter, and Timothy Grance. *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*. NIST, Sept. 2011.
3. Sun, Yunchuan, et al. “Data Security and Privacy in Cloud Computing.” *International Journal of Distributed Sensor Networks*, vol. 10, no. 7, Jan. 2019, p. 190903. *Research Gate*, journals.sagepub.com/doi/full/10.1155/2014/190903, https://doi.org/10.1155/2014/190903.
4. Robinson, Neil, et al. “Understanding the Implications for Security, Privacy and Trust.” *The Cloud: Understanding the Security, Privacy and Trust Challenges*, RAND Corporation, 2011, pp. 23–27. *JSTOR*, http://www.jstor.org/stable/10.7249/tr933ec.8.
5. N. Leavitt, “Is Cloud Computing Really Ready for Prime Time?” in *Computer,* vol 42, no. 1, pp. 15-20, Jan. 2009, doi: 10.1109/MC.2009.20.
6. Arpaci, Ibrahim, Kerem Kilicer, and Salih Bardakci. “Effects of Security and Privacy Concerns on Educational Use of Cloud Services.” Computers in human behavior 45 (2015): 93–98. Web.
7. Rodrigues, Joel J P C et al. “Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems.” *Journal of medical Internet research* 15.8 (2013): e186–e186. Web.

8. Xue, Colin Ting Si, and Felicia Tiong Wee Xin. "Benefits and challenges of the adoption of cloud computing in business." *International Journal on Cloud Computing: Services and Architecture* 6.6 (2016): 01-15.
9. U.S. Department of Education. “Family Educational Rights and Privacy Act (FERPA).” *U.S. Department of Education*, 25 Aug. 2021, www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.
10. Google. “What Is a Public Cloud?” *Google Cloud*, cloud.google.com/learn/what-is-public-cloud.
11. Amazon Web Services. “What Is a Public Cloud? - Public Cloud Explained - AWS.” *Amazon Web Services, Inc.*, aws.amazon.com/what-is/public-cloud/.
12. ---. “What Is AWS? - Amazon Web Services.” *Amazon Web Services, Inc.*, 2019, aws.amazon.com/what-is-aws/.
13. Microsoft Azure. “What Is a Private Cloud - Definition | Microsoft Azure.” *Azure.microsoft.com*, azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-private-cloud .
14. GDPR.eu. “What Is GDPR, the EU’s New Data Protection Law?” *GDPR.eu*, 7 Nov. 2018, gdpr.eu/what-is-gdpr/#:~:text=The%20right%20to%20privacy%20is.
15. Wolford, Ben. “GDPR Compliance Checklist for US Companies.” *GDPR.eu*, 22 Mar. 2019, gdpr.eu/compliance-checklist-us-companies/.
16. U.S Office of Special Counsel. “The Privacy Act of 1974.” *Osc.gov*, osc.gov/Pages/Privacy-Act.aspx#:~:text=The%20Privacy%20Act%20provides%20protections.

17. OECD Better Policies For Better Lives. “About the OECD - OECD.” *Www.oecd.org*, www.oecd.org/about/#.
18. OECD. *THE OECD PRIVACY FRAMEWORK*. 2013.
19. Pesante, Linda. *Introduction to Information Security*. 2008.
20. National Cybersecurity Alliance. “You Can’t Have Privacy without Security.” *National Cybersecurity Alliance*, 13 Oct. 2016, staysafeonline.org/cybersecurity-for-business/you-cant-have-privacy-without-security/#:~:text=You%20can%20have%20security%20without.
21. Chandramohan, Dhasarathan, Thirumal Vengattaraman, and Ponnurangam Dhavachelvan. “A Secure Data Privacy Preservation for On-Demand Cloud Service.” *Journal of King Saud University. Engineering sciences* 29.2 (2017): 144–150. Web.
22. Demirol, Doygun, et al. “A Key Review on Security and Privacy of Big Data: Issues, Challenges, and Future Research Directions.” *Signal, Image and Video Processing*, vol. 17, no. 4, 2023, pp. 1335–43, https://doi.org/10.1007/s11760-022-02341-w.
23. Grabowski, Mark, and Eric P Robinson. *Cyber Law and Ethics*. Routledge, 13 July 2021.
24. Yan, Gujun. “Application of Cloud Computing in Banking: Advantages and Challenges.” *Www.atlantis-Press.com*, Atlantis Press, 1 July 2017, www.atlantis-press.com/proceedings/icpel-17/25882264.
25. Federal Trade Commission. “Gramm-Leach-Bliley Act.” *Federal Trade Commission*, Apr. 2021, www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/8/viii-1-1.pdf.

26. Reidenberg, Joel; Russell, N. Cameron; Kovnot, Jordan; Norton, Thomas B.; Cloutier, Ryan; and Alvarado, Daniela, "Privacy and Cloud Computing in Public Schools" (2013). Center on Law and Information Policy. 2.
27. United States Department of Education - Student Privacy Policy Office. “Protection of Pupil Rights Amendment (PPRA).” 22 Oct. 2020.
28. Mokhtar, Shamsul Anuar, et al. “Cloud Computing in Academic Institutions.” *Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication - ICUIMC ’13*, 2013, https://doi.org/10.1145/2448556.2448558.
29. Jansen, W., et al. *Guidelines on Security and Privacy in Public Cloud Computing*. U.S. Dept. of Commerce, National Institute of Standards and Technology, 2011.
30. Alenizi, Bayan A., et al. “Security and Privacy Issues in Cloud Computing.” *Journal of Physics. Conference Series*, vol. 1979, no. 1, 2021, pp. 12038-, https://doi.org/10.1088/1742-6596/1979/1/012038.
31. Al Rawajbeh, Mohammad, Issam Al Hadid, and Hassan Al-Zoubi. "Adoption of Cloud Computing in Higher Education Sector: An Overview." *International Journal of Technology & Engineering Studies* 5.1 (2019).
32. Google Workspace for Education. “Get Started with Education Fundamentals.” *Google for Education*, edu.google.com/intl/ALL_us/workspace-for-education/editions/education-fundamentals/.
33. Google Workspace for Education. *Foundational Tools for Teaching and Learning*.
34. Whitepaper, Security. *Google Workspace*. 2021.

35. Microsoft. “Free Microsoft Office 365 for Schools & Students | Microsoft Education.” *Microsoft.com*, 2019, www.microsoft.com/en-us/education/products/office.
36. Microsoft Learn. “What Is Intune for Education? - Intune for Education.” *Learn.microsoft.com*, 15 Apr. 2022, learn.microsoft.com/en-us/intune-education/what-is-intune-for-education.
37. EDUCAUSE. “Higher Education Community Vendor Assessment Toolkit.” *Library.educause.edu*, library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit.
38. Adelphi University Information Technology. “Third Party Review | Technology Services.” *Adelphi University*, www.adelphi.edu/it-services/third-party-review/.
39. ISO. “ISO/IEC 27001 Standard – Information Security Management Systems.” *ISO*, Oct. 2022, www.iso.org/standard/27001.
40. Singh, Ashish, and Kakali Chatterjee. “Cloud Security Issues and Challenges: A Survey.” *Journal of Network and Computer Applications*, vol. 79, Feb. 2017, pp. 88–115, https://doi.org/10.1016/j.jnca.2016.11.027.
41. Microsoft Learn. “Enable Transport Layer Security (TLS) 1.2 Overview - Configuration Manager.” *Learn.microsoft.com*, 3 Oct. 2022, learn.microsoft.com/en-us/mem/configmgr/core/plan-design/security/enable-tls-1-2.
42. Cloudflare. “What Is Transport Layer Security?” *Cloudflare*, 2021, www.cloudflare.com/learning/ssl/transport-layer-security-tls/.

43. Engemann, Kurt J, and Douglas M Henderson. *Business Continuity and Risk Management: Essentials of Organizational Resilience*. Brookfield, Conn., Rothstein Associates Inc, 2012.

44. Office of Information Technology Services. "Breach Notification and Incident Reporting." *Office of Information Technology Services*, its.ny.gov/breach-notification-and-incident-reporting#:~:text=NYS%20Information%20Security%20Breach%20and%20Notification%20Act.

45. Federal Student Aid. "Protecting Student Information | Knowledge Center." *Fsapartners.ed.gov*, 15 Oct. 2021, fsapartners.ed.gov/knowledge-center/library/dear-colleague-letters/2015-07-29/protecting-student-information#footnote1.

46. "Vendor Security Alliance." *Www.vendorsecurityalliance.org*, www.vendorsecurityalliance.org.

47. "The Continuous Audit Metrics Catalog | CSA." *Cloudsecurityalliance.org*, cloudsecurityalliance.org/artifacts/the-continuous-audit-metrics-catalog.

48. PCI Security Standards Council. *PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard Version 3.2.1 for Merchants and Other Entities Involved in Payment Card Processing*. July 2018.

49. Leune, Kees. *Medium/High Risk Service Assessment Checklist*. 2021.

50. Leune, Kees. *Triage Workflow Chart*. 2021.

51. Vendor A. *Privacy Policy*.

52. Vendor A. *HECVAT-Full*.

53. Vendor A. *Vendor Service Risk Assessment*.

54. Vendor B. *Privacy Policy.*

55. Vendor B. *HECVAT-Lite*.

56. Vendor B. *Data Protection and Risk Management Policy*.

57. Vendor B. *Information Security Policy*.

58. Vendor B. *Disaster Recovery Plan*.

59. Vendor B. *Vendor Service Risk Assessment*.

60. Vendor C. *Privacy Policy*.

61. Vendor C. *Incident Response Plan*.

62. Vendor C. *Disaster Recovery Plan*.

63. Vendor C. *SOC 3 Report*.

64. Vendor C. *SAML SSO Configuration Worksheet*.

65. Vendor C. *Vendor Service Risk Assessment.*

66. State of California Department of Justice. "California Consumer Privacy Act (CCPA)." *State of California - Department of Justice - Office of the Attorney General*, 13 Mar. 2024, oag.ca.gov/privacy/ccpa.

67. Deckert, Andrea. "Transitioning to Cloud-Based Services: Due Diligence Is Key." *Rochester Business Journal*, 27 Oct. 2020, rbj.net/2020/10/27/transitioning-to-cloud-based-services-due-diligence-is-key/.

68. Brenegan, Macy. "Educational Technologies during COVID-19." *Opentextbooks.clemson.edu*, opentextbooks.clemson.edu/sts1010fidlerfall2021/chapter/educational-technologies-during-covid-19/.