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

Thesis Defense

Ashley Peralta, B.S. Information Systems

Overview

1. Introduction and Relevance
2. Methodology
3. Findings
4. Implementation
5. Closing

Why is this important?

- Adoption of cloud computing has grown rapidly over the years.
  - Institutions are in the process of transitioning from in-house infrastructure to cloud computing.

- Institutions are storing and accessing confidential information on a daily basis through virtual services which leads to the concern of privacy and security.

- It is important to understand the difference between privacy and security.

Methodology and Source Base

- Researching how cloud service providers maintain efficient and effective measures and policies to manage the cloud data of education systems.
    - Comprehensive literature review
    - Analyzed three major education-based privacy laws, adjacent standards and regulations.
    - Created privacy and security standards based on cloud security frameworks and questionnaires.
    - Analyzed a Third Party Review procedure
    - Data Collection: Reviewing vendors already in place
    - Implementation for Primary and Secondary Education

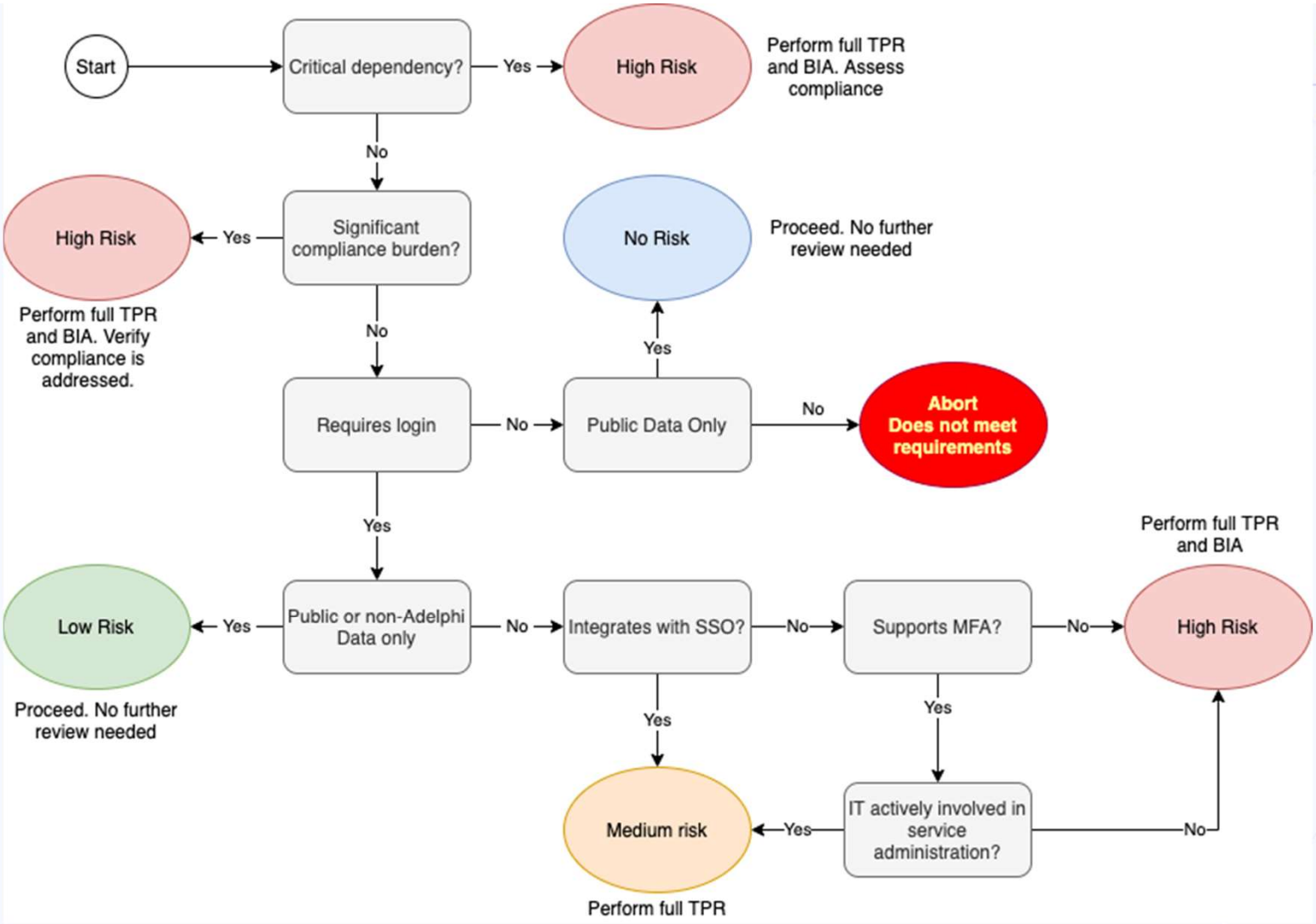
Privacy Laws, Standards and Regulations

	Scope
Family Educational Rights and Privacy Act (FERPA)	limits the disclosure of PII from children's education records without the proper consent.
Children's Online Privacy Protections Act (COPPA)	regulates the personal information collected online by website and services.

Protection of Pupil Rights Amendment (PPRA)	regulates the disclosure of certain types of information about children from surveys and evaluations.
US Health Insurance Portability and Accountability Act (HIPAA)	protects privacy by limiting what information can be shared about patients.
Payment Card Industry Data Security Standard (PCI DSS)	designed to ensure that services handle credit card information in a secure environment

Implementation for PreK-12 Education

- **The Process**
  - Developed privacy and security standards based on my analysis of
    - **Higher Education Community Vendor Assessment Toolkit (HECVAT)** and
    - **Adelphi University IT Department's Third Party Review**
  - Developed a sample implementation of a **Primary and Secondary Vendor Assessment Questionnaire (PS-VAQ)** in accordance with those standards
    - Followed by a **Vendor Service Risk Assessment**


Start
Critical dependency?
Yes
High Risk
Perform full TPR and BIA. Assess compliance
No
High Risk
Yes
Significant compliance burden?
No Risk
Proceed. No further review needed
Perform full TPR and BIA. Verify compliance is addressed.
No
Yes
Requires login
No
Public Data Only
No
Abort
Does not meet requirements
Yes
Perform full TPR and BIA
Low Risk
Yes
Public or non-Adelphi Data only
No
Integrates with SSO?
No
Supports MFA?
No
High Risk
Proceed. No further review needed
Yes
Yes
Medium risk
Yes
IT actively involved in service administration?
No
Perform full TPR

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	

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? (eg. 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)?	

Part 3: Data		
DATA - 01	What data is being collected and what are its usuage 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?	

Part 6: 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 Instituiton 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 resonable time period?	

Part 4: Governance, Compliance, and Standards		
GCS - 01	Is the contract established and maintained with cloud-related special interest groups and other relevent 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 (eg. GDPR)?	
GCS - 04	How does the organization comply with relevant student privacy regulations (eg. 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.	

Part 5: Authenication 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 intregation with other authenticaion 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 functionalites outside their scope of work? How would the process look like?	

Part 7: 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?	

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?

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?

Benefits of a PreK-12 Implementation

- **PreK-12 schools may not have a full staffed IT team compared to a higher education institution.**
  - Will benefit their IT personnel in organizing and managing their workflow more efficiently.
  - Ensures that technology solutions and resources provided by vendors closely align with the institution's specific needs and requirements.
  - Will have a proper guidance system that they can follow to determine whether or not a prospective service should be implemented.
- **The vendor will gain new clients and continue building client and service trust relationships.**

QUESTIONS :)