Adapting Industry Security and Privacy Controls for compliance with RA10173 in the Education Sector towards the New Normal

Danny Cheng
De La Salle University
*danny.cheng@dlsu.edu.ph**

Abstract: Two years of COVID-19 pandemic has transformed traditional work flows and accelerated the shift towards a more digital and remote mode of work, interaction, and collaboration. The education sector locally in part experienced a more significant impact as it traditionally relies heavily on physical or face-to-face interactions in delivering classes and even back office processes. The urgency to shift operations to a digital mode for continuity of the operations and learning activities introduced gaps and risks that were aggravated due to lack of resources, and awareness on ways to manage the new mode. The focus of information security and data privacy transferred from the borders or confines of the educational institution to the cloud and the endpoints where data is being accessed and processed. The uniqueness of the complexity and volume of data processing for the academic activities that interact with administrative processes also provided additional challenges to the implementation of security and privacy controls. This paper looks at the compliance requirements in the education sector with the objective of aligning and adapting industry security and privacy controls practices considering the trends and risks more associated and sometimes unique with the sector. Conflicts to basic and common controls that have served as acceptable practices in other industries are identified and discussed to provide recommendations on alternative or compensatory controls and approaches in order to still achieve compliance albeit imperfect. Finally, calibration or tiering of controls are also suggested to provide consideration to the limited resource availability of the education sector coming from multi-year challenges ranging from the shift to K-12 and the current pandemic.

Key Words: information security and privacy controls, privacy compliance, education sector, cloud security, data protection

1. INTRODUCTION

In 2012, Republic Act 10173 (RA10173) of the Republic of the Philippines otherwise known as the Data Privacy Act of 2012 was approved and published by the Philippine Congress. The regulation's main purpose is to ensure free flow of information while imposing the obligation to secure and protect personal data both in the government and private sector. (Philippine Fifteenth Congress, 2012) However, the regulation has largely gone unnoticed as the regulatory body mandated to enforce the new regulation had not been formed until March 7, 2016 (Newsbytes.PH, 2016). The Implementing Rules and Regulations (IRR) (NPC, 2016) were also not defined until August of 2016 with an initial grace period of 1 year before implementation became mandatory. Companies and institutions struggled to comply, from both a resource constraint perspective, and clarity of understanding of the actual requirements as it translates to the organization and industry. During this time, the full implementation of the K-12 transition has also begun with a projected transition period of 5 years or 2016-2021 (CHED). The introduction of K-12 provided another strain to the resources of educational institutions as they are either forced to focus on restructuring and retooling or prepare for a gap or lowered intake of students due to an additional 2 years of schooling as part of the shift. Then on the 15th of March 2020, the COVID-19 pandemic struck and the government declared the start of what would be a multi-year series of lockdowns for the country (CNN Philippines Staff, 2020). This forced the educational sector to urgently transition its operations both on the learning and administration side to an online and remote work paradigm which in turn introduced multiple gaps not just in privacy compliance but basic data protection requirements as well. Such gaps was evidenced by the development and subsequent publication of specific guidance by the National Privacy Commission (NPC) and the education sectors data privacy council to provide guidance for the implementation of online learning during the start of the pandemic (DP Council Education Sector, 2020). However, the published guidance only covered basic activities of data processing specific only to online learning activities. The effect of the pandemic did not only force learning to go online but also administrative and research based activities. Use of third-party solutions and services, personal devices, remote working environment, were not fully vetted and cannot be restricted due to the need to survive. This introduced new risks caused by new threats previously less evident and the blurring of borders that historically protected the data being processed.

This paper considers industry guidance looking on privacy and information security controls and provides a recommendation on their adaption and implementation considering the current state of resources and maturity of the sector as well as the complexities of data processing and nuances of the sector such as culture and the constitutional right to academic freedom for higher learning. Controls suggestions are also tiered in order to address constraints on resources of the sector.

2. METHODOLOGY

Literature review and cases are used as the methodologies for the research looking into areas on risks (Ulven & Wangen, 2021), challenges (Doce & Ching, 2018), complexities (Archuleta, 2006; Earp & Payton, 2001; Mantra, 2016) and controls (Fouad, 2021) in the education sector mapping them to a maturity model that is based on an existing Privacy Maturity Model (American Institute of Certified Public Accountants & Canadian Institute of Chartered Accountants, 2011) where the baseline and guiding maturity level descriptions are as follows:

1. Ad hoc – the private university is just starting on its journey to privacy compliance and most if not all efforts are conducted in an informal manner with record keeping and documentation minimally existing.
2. Repeatable – the private university privacy compliance efforts are on-going where some standardization of policies and procedures exist for core functions.
3. Defined – the private university has fully implemented baseline compliance requirements for privacy and documentation are complete as well.
4. Managed – monitoring of privacy compliance through defined metrics are being exercised to determine effectivity of implementation.
5. Optimized – regular review and feedback are used to ensure continuous improvement towards optimization of the given process.

The controls recommendation references existing regulations (NPC, 2016, 2018; Philippine Fifteenth Congress, 2012), standards (ISO, 2017, 2019), and frameworks (National Institute of Standards and Technology, 2018, 2020; NIST, 2020) to determine the baseline controls requirements for an organization in the sector. The recommended controls practices for an educational institution were developed based on the tiering of the capabilities of the institution in relation to the mentioned maturity level guidance. Existing ISO standards documents (ISO, 2013, 2017, 2019), frameworks (National Institute of Standards and Technology, 2018, 2020; NIST, 2020), and other publications (Huang et al., 2020) were used as reference for requirements with respect to the capabilities dimension requirements. Table 1 shows the guiding principles for the security and privacy controls of an educational institution in determining the actual controls practice recommendations in accordance with their level. To limit the scope of the research, the risks considered will focus mostly on those introduced by the pandemic that caused a massive shift in how educational institutions function (Fouad, 2021; Kelly et al., 2021; Ulven & Wangen, 2021).

Table 1. Guiding principles defined based on (American Institute of Certified Public Accountants & Canadian Institute of Chartered Accountants, 2011) focusing on security and privacy controls

Capability	Level 1	Level 2	Level 3	Level 4	Level 5
Security Controls	Controls that deal with policies and the human aspect are used in this level to ensure feasibility of implementation	Enhancement of controls selection to include commonly available solutions that aims to prevent risks without the need for heavy investments.	Incorporate controls that require investments for remote access, third party management, and incident management	Use of centralized management tools and incorporation of review process.	Definition of metrics for continuous improvements
Privacy Controls	Focus on data collection sources and data protection officer appointment.	Ensure data steward appointment and expand data collection sources to external entities or third parties.	Development of privacy management program.	Incorporate review and change management processes.	Incorporate third party reviews and anticipation of changes in environment.

3. CONTROLS AND THE CASE OF THE EDUCATION SECTOR

We focus on one specific impact caused by the pandemic where everyone was forced to work remotely. This impact served as the trigger to a multitude of consequential activities that made data protection and compliance more difficult in the education sector. The urgent move to remote work while at the same time sustaining the academic and administrative operations of an educational institution triggered the increase in use of cloud services, personal devices, various communication mediums, transfer of sensitive data beyond the logical and physical borders of the institution, cross-border transfers resulting in increased regulatory compliance requirements, non-standard data processing activities and the rush to digitalization that may conflict with compliance requirements. To address the scenario, a snapshot of adapting industry controls while considering the limitations and complexities of the sector and following the guiding principles in table 1 to not just adapt but provide a roadmap is shown on table 2. The alignment to regulatory requirements are also shown in the table as it maps to the 32 point checklist of compliance (NPC, 2017) provided by the regulator.

Table 2 Snapshot of Security and Privacy controls on levels to consider limitations and maturity of the institution in relation to 32 point checklist privacy compliance requirements from the regulator.

Level 1	Level 2	Level 3	Level 4	Level 5
Define or strengthen policies on acceptable use of resources, non-disclosure agreements for administrators and staff processing sensitive data, Security and Privacy Policies for cloud based systems, Separation of work and personal workspace and information use, data processing storage and retention policies, password policies, BYOx policies, and security awareness campaigns	Use of endpoint security included with operating systems, enabling automatic system updates on personal devices, require use of secure connections only to websites and systems (e.g. HTTPS), provisioning of personal and work accounts on personal workstations.	Use of multi-factor authentication, virtual private networks, and storage encryption for key personnel, Only use official platforms only for data processing activities. Ensure proper contract execution with third-party partners.	Formalized vetting and monitoring of third-party partner, vulnerabilities, and compliance with policies. Use of in-house or outsourced events monitoring solutions to detect incidents. Conduct reviews on change management and incident management.	Defining disaster recovery and continuity plans considering migration of core systems and processing to third-party. Formal risk management is in place to calibrate use of controls.
Privacy Compliance 32 point checklist				
17. Implement appropriate and sufficient organizational security measures;	**18.** Implement appropriate and sufficient physical security measures.;	**18.** Implement appropriate and sufficient physical security	**20** Compliance with DPAs Data Breach Management	**20** Compliance with DPAs Data Breach Management Requirements **21**.

	19. Implement appropriate and sufficient technical security measures.;	measures.; **19.** Implement appropriate and sufficient technical security measures.;	Requirements **21**. Maintaining data privacy requirements for third parties.	Maintaining data privacy requirements for third parties.

4. ANALYSIS AND ASSESSMENT

Prioritizing administrative controls for level 1 aims at jumpstarting compliance efforts of the institution without an immediate introduction of capital outlay to consider resource constraints. However, remaining at level 1 does not equate to operational compliance as the goal stated by the NPC. Rather, level 1 aims to provide quick action and initiate the compliance journey as compliance generally starts at level 3 going to level 5 as an ideal condition. Although policies and procedures generally can be crafted to work with existing resources, some recommended policies can come in conflict with the culture and nature of the sector.

One such case would be the BYOx or Bring Your Own (Anything) policy (e.g. BYOD for Bring Your Own Device or BYOC for Bring Your Own Cloud). Generally, such policies would need to incorporate management and monitoring of their usage by the institution. Such can cause privacy concerns not just in the education sector but in other sectors as well. The education sector differs in that culturally and historically, such practices are non-existent and not considered. To mitigate the concerns, other sectors such as financial or business processes outsourcing sectors would provide physical or virtual company issued resources that can be managed as they are property of the company and there are explicit regulatory and contractual obligations that would encourage such practices. However, for the education sector, such direct regulations and contractual obligations do not exist and given the recent history and priorities of the sector, resources that can be allotted to such facilities would be limited at best. Hence policies crafted for the sector should focus instead of avoidance, and minimization or reduction of the risks involved in BYOx such as limiting local or personal storage of data to the minimum extent necessary. Such practice is not ideal but is a bridge for the gap instead of non-action as a response. Awareness campaigns can also be used to reduce unintentional and non-malicious incidents.

Another case is the whitelisting of cloud services and applications that can be used to perform one's duties and responsibilities. Referring to the financial and outsourcing sector, such policies and practices are well understood and can be clearly implemented as data from clients requires protection from both regulatory and contractual obligations. In the case of the education sector, users of data crosses between administrative and academic domains where the latter is covered by the constitutional provision on academic freedom in higher education institutions (Constitutional Commission, 1986). This runs in contrary to hard restrictions on use of tools and technology as well as strict vendor assessment and management practices. The provision of academic freedom requires that there should not be undue or unreasonable interference. As such, policies on cloud services and applications for the academic community may need to focus more on guidance and self-evaluation criterion similar to the Higher Education Community Vendor Assessment Toolkit (HECVAT) (EDUCASE, 2021) rather than the traditional prescriptive or restrictive practices for such policies. This constraint is still debatable and may evolve over time as the interpretation of undue and unreasonable would still need to be properly defined or contextualized.

There is also the students in the sector being both the source and consumer of data in the institution. Similar to consumer stakeholders for the other sectors, students are not employees of the educational institution but rather are its customers. However, unlike regular customers for other sectors, students not only participate in academic activities but also certain administrative and research activities as well that is not commonly present in customers of other sectors. Aside from challenges previously mentioned, their wide gamut or range of age introduces other concerns such as inclusion of minors that affects consent collection and policies on data collection such as video recording of online learning sessions as education data is considered sensitive personal information under RA10173. As such, consent and policies should not only consider data flow and protection but also go in-depth on the purpose and retention of the collected data where data are at risk of multiple secondary use purposes that may not be previously communicated given the complexity of processing in an educational institution.

Lastly, there is also the potential of regularizing collaborations and interactions with foreign institutions and counterparts as the pandemic has nudged everyone to get accustomed to online or virtual interactions and collaborations. Making such activities mainstream increases the exposure and compliance requirements for the sector and its institutions as the various jurisdictions that will participate will have its own regulatory compliance requirements that has to be considered. Unlike other sectors, it can be a normal occurrence for the education sector that one interaction or activity will have a multitude of participating jurisdictions that is again uncommon for other sectors. The volume of such interactions or activities significantly increase the complexity of controls adoption for the sector. Common solutions such as binding corporate rules and contractual obligations may not be flexible enough to account for the flexibility needed by an educational institution. As such, it is recommended that detailed rules and obligations be formalized that drill down to specific activities so that the complexity of processing can be accounted for. Balancing between formalizing and the need to have flexibility should always be considered when defining the rules or obligations.

5. CONCLUSIONS AND RECOMMENDATIONS

The paper provided insights and recommendations on tiering and contextualization of industry accepted privacy and security controls for the education sector to consider its environment and constraints that make the sector unique to other industry sectors. The cases presented provide only a small snapshot on the journey towards elevating educational institution's use of controls to be at par with other sectors. Such journey needs to be taken as the risks previously less evident have now been put front and center due to the pandemic and the upcoming new normal where remote work is seen to be a central pillar. The education sector is not immune to attacks and breaches and should be prepared and implement due diligence to protect the privacy and security of the data entrusted to the institution in the new normal. Further work needs to be conducted to fully contextualize the industry standards and practices to the sector balancing the residual risks introduced by the contextualized controls recommendations that would otherwise not be present for other sectors. Study should also be conducted on how continuous monitoring and improvement systems from other sectors can be effectively contextualized and justified for the education sector to allow for a more agile sector and institution that can respond to future changes in privacy and security requirements and environments.

6. REFERENCES

American Institute of Certified Public Accountants, I., & Canadian Institute of Chartered Accountants. (2011). AICPA/CICA Privacy Maturity Model. https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf

Archuleta, L. S. a. K. (2006). *Privacy Protection and Compliance in Higher Education: The Role of the CPO.* https://er.educause.edu/articles/2006/1/privacy-protection-and-compliance-in-higher-education-the-role-of-the-cpo

CHED. *CHED K to 12 Transition Program*. CHED. https://ched.gov.ph/k-12-project-management-unit/

CNN Philippines Staff. (2020). *Metro Manila to be placed on 'lockdown' due to COVID-19.* CNN Philippines. https://www.cnnphilippines.com/news/2020/3/12/COVID-19-Metro-Manila-restrictions-Philippines.html

THE 1987 CONSTITUTION OF THE REPUBLIC OF THE PHILIPPINES - ARTICLE XIV, (1986). https://mirror.officialgazette.gov.ph/constitutions/the-1987-constitution-of-the-republic-of-the-philippines/the-1987-constitution-of-the-republic-of-the-philippines-article-xiv/

Doce, L. J., & Ching, M. R. (2018). *RA 10173 and its challenges to Philippine state universities and colleges' compliance performance: the case of Mindanao State University - General Santos City.* https://doi.org/10.1145/3234781.3234789

DP Council Education Sector. (2020). Advisory No. 2020-1 Data Privacy and Online Learning.

https://www.privacy.gov.ph/wp-content/uploads/2020/10/DP-Council-Education-Sector-Advisory-No.-2020-1.pdf

Earp, J., & Payton, F. C. (2001). Data Protection in the University Setting: Employee Perceptions of Student Privacy. *Hawaii International Conference on System Sciences*, *8*, 8039. https://doi.org/10.1109/HICSS.2001.927152

EDUCASE. (2021, December 17, 2021). *Higher Education Community Vendor Assessment Toolkit*. EDUCASE,. https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit

Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*, *6*(2), 137-154. https://doi.org/10.1080/23738871.2021.1973526

Huang, R. H., Liu, D. J., Zhu, L. X., Chen, H. Y., Yang, J. F., Tlili, A., Fanc, H. G., & Wang, S. F. (2020). Personal Data and Privacy Protection in Online Learning: Guidance for Students, Teachers, and Parents. https://iite.unesco.org/publications/personal-data-and-privacy-protection-in-online-learning/

ISO. (2013). ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. In: (ISO) International Organization for Standardization.

ISO. (2017). ISO/IEC 29151:2017 [ISO/IEC 29151:2017] Information technology — Security techniques — Code of practice for personally identifiable information protection. In: (ISO) International Organization for Standardization.

ISO. (2019). ISO 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. In: (ISO) International Organization for Standardization.

Kelly, B., McCormack, M., Reeves, J., Brooks, D. C., O'Brien, J., Corn, M., faehl, S., Harris, E., Novik, K., Pesino, S., Romness, P., & Sawyer, G. (2021). *2021 EDUCAUSE Horizon Report® | Information Security Edition*. E. Publications. https://library.educause.edu/resources/2021/2/2021-educause-horizon-report-information-security-edition

Mantra, I. (2016). The Modeling of Information Security Classification With Risk Value Assesment Factor to Good Information Governance on The Indonesia Higher Education Sector. *JATISI*, *3*.

National Institute of Standards and Technology. (2018). Cybersecurity Framework Version 1.1. In: National Institute of Standards and Technology.

National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations. In: U.S. Department of Commerce.

Newsbytes.PH. (2016). *First on Newsbytes.PH | DOST exec named first commissioner of National Privacy Commission*. Newsbytes.PH. Retrieved April 30 from http://newsbytes.ph/2016/03/dost-exec-named-first-commissioner-of-national-privacy-commission/

NIST. (2020). The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. In: National Institute of Standards and Technology.

IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, KNOWN AS THE "DATA PRIVACY ACT OF 2012", (2016). https://www.privacy.gov.ph/wp-content/uploads/IRR-of-the-DPA.pdf

NPC. (2017). *The NPC Data Privacy Accountability and Compliance Checklist*. Retrieved from https://privacy.com.ph/site/wp-content/uploads/2017/10/NPC-32-Point-Compliance-Checklist.pdf

NPC. (2018). *NPC Privacy Toolkit*. Retrieved from https://www.privacy.gov.ph/wp-content/files/attachments/nwsltr/3rdToolkit_0618.pdf

AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES, (2012). https://www.privacy.gov.ph/wp-content/uploads/DPA-of-2012.pdf

Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*(2), 39. https://www.mdpi.com/1999-5903/13/2/39