Development of Privacy Controls in Cloud Certifications: A Case Study of Cisco's Cloud Controls Framework (CCF)

Introduction

Representing a major evolution of computer technology, cloud computing has become a dominant model for delivering information technology (IT) infrastructure, components, and applications. While it offers tremendous benefits, such as efficiency, flexibility, and reduced costs, it also creates challenges on data protections for both users and providers. To protect users from exploitation, cloud services providers have been more focusing on security, data privacy, and compliance of regulations. Especially, privacy concerns (i.e., unauthorized access, loss of privacy, data replication, and regulatory violations) have drawn a lot of attention considering the large amount of data stored, processed, and used in the cloud environment.

To maintain user's trust and meet compliance, cloud service providers are expected to prioritize privacy protections for their users in the digital age. Cloud certifications and standards have been implemented to demonstrate service providers' compliance with privacy principles and regulations. However, with the fast-moving development of cloud services, traditional baseline on information protection mechanisms have limitations on addressing the new threats to information privacy. Meanwhile, unlike security protection mechanisms that have already been well-established, there are no widely applied comprehensive guidelines or a set of controls that privacy practitioners can rely on as a set of baseline protections. Therefore, it is essential that privacy-focused controls are developed so that it can bridge the gap between general data privacy protection and cloud computing security and serve as the baseline criteria for organizations to evaluate, manage, and protect users' privacy.

Currently, there are initiatives from governments, organizations, and cloud service providers that it is necessary to develop different strategies to leverage cloud certifications for organizations to better comply with data protection and emphasize privacy in this era. For example, one such initiative from organizations is the development of SOC 2 Compliance by the American Institute of CPAs (AICPA), which includes an additional section focusing on privacy criteria. Similarly, in October 2019, the International Organization for Standardization (ISO) published ISO/IEC 27701 – Privacy Information Management System. It is an extension to ISO 27001, and it focuses on the data privacy protections regarding Personally Identifiable Information (PII) controllers and processors.

More recently, one of the cloud service providers have joined the movement in establishing standards to protect user's information in the cloud. On May 5, 2022, Cisco Systems, Inc. published the Cloud Controls Framework (CCF), which is a publicly available framework that includes a comprehensive set of international and national security compliance and certifications. In its initial version, the CCF aggregates multiple standards, certifications, regulations, and guidelines to help organizations to meet the requirements of different criteria. The framework is expected to be updated as security compliance frameworks and regulations evolve. Each control in CCF has been assigned to one of the 15 domains, identified with a control type (process, people, or technology), and checked if it maps to other privacy documents.

Method and Preliminary Findings

We conducted a focused investigation of CCF to evaluate its performance, specifically on privacy protections, by comparing it with four existing cloud certifications and standards. Our evaluation included the following list of standards and certifications that are publicly available:

- ISO/IEC 27001 (2013 version, most recently one that is publicly available)

- FedRAMP (2021 version, latest)
- C5 (2020 version, latest)
- SOC 2 (2020 version, most recently one that is publicly available)
- CCF (2022 version, latest)

The four selected standards and certifications are highly regarded and have been applied nationwide. They are natural starting points to assess for adequately upholding privacy principles. For each of these certifications and standards, we identified the privacy-focused controls by detecting if the control name and/or description includes privacy-related keywords (i.e., “privacy”, “personal information”, “data protection”, “PII”). We also manually reviewed the description of each control to include the controls that imply privacy aspects (for example, some controls are originally built as security controls, but they may also indirectly cover privacy aspects). To evaluate the privacy performance of each standard and certification, we applied an extended and updated version of the Fair Information Practice Principles (FIPPs). Each privacy control was assigned one of the 13 privacy categories: 1) Notice, openness, and transparency; 2) User choice and consent; 3) Purpose, scope, and data minimization; 4) User access and control; 5) Safeguards; 6) Compliance and auditing; 7) Accountability and law enforcement; 8) Data retention and deletion; 9) Data privacy management; 10) Risk assessment; 11) Data accuracy and correction; 12) Cross-border data transfer; 13) Data sharing, disclosure, and limiting use.

Among all the five documents that we evaluated, CCF seems to have the highest level of comprehensiveness on covering the aspects of privacy protection in cloud computing since it maps to a variety of sources, including the other four certifications and standards selected. Results also show that CCF performs better than other four certifications regarding the number of privacy controls contained. Not only it includes two domains specifically related to privacy (*Data Security and Privacy Lifecycle Management* and *Privacy Handling & Security*), but also all the principles from FIPPs have been mentioned in CCF. In contrast, the other four certifications and standards are missing some of the privacy aspects defined in FIPPs. For example, FedRAMP and ISO/IEC 27001 did not include controls on user’s choice and consent, while C5 did not include controls related to purpose and scope. In addition, SOC 2 did not include controls that address compliance and auditing.

However, although CCF performs better than the other four selected documents on covering privacy aspects and includes controls addressing individual’s rights on privacy, in general, all these five documents focus more on security mechanisms, and the privacy protections from a user’s perspective are still lacking in the existing standards and certifications. A large percentage of the privacy controls in the selected documents are related to safeguards, risk assessment, and privacy management. Regarding the protection of PII, these privacy controls emphasize more on organization’s accountabilities to protect user’s personal information and the compliance with privacy regulations, instead of comprehensively describing how users are able to take control over their personal data. For example, the control *Automatic Processing of PII Requirements* in CCF includes the requirement of getting the Customer or Controller's instruction on how to handle the processing of PII, but it is about the organization’s responsibility to obtain user’s consent, instead of directly describing how users have control on the processing of their PII.

Overall, the latest developed cloud control framework by Cisco provide a comprehensive, detailed guideline for business and organization to meet requirements on data protections. While CCF has already established a set of security measures and addressed organization’s responsibilities, our evaluation possessed the potential for improvement on developing privacy-focused controls. Considering the importance of privacy as a human right, in the future updates,

we would suggest CCF to develop more privacy controls regarding user's control over their personal data so that the framework could satisfy user's needs on privacy protection as well.

Acknowledge
This work has been supported by Cisco. We want to acknowledge and thank all of those who have contributed to this work.