Gap Analysis Report

Mapping of the Association of Banks in Singapore Cloud Computing Implementation Guide 2.0 to Cloud Security Alliance Cloud Controls Matrix v3.0.1

CSA cloud security alliance®

Acknowledgments

Co-Chair:

Arun Vivek

Contributors:

Victor Chin
Francis Lee
Paul Lee
Anthony Lim
Moorthi Rathinam
Terence Siau
Steven Sim
Alex Siow
Yao Sing Tao

CSA Global Staff:

Hing-Yan Lee
Ekta Mishra
Haojie Zhuang
AnnMarie Ulskey (Design)

Table of Contents

1. Introduction 5
2. Background 5
    2.1 Working Group (WG) to Map ABS CCIG 2.0 to CCM 5
    2.2 CSA CCM 6
    2.3 ABS CCIG 2.0 6
    2.4 Controls Mapping and Terminologies 7
3. Mapping of ABS CCIG 2.0 to CCM 8
    3.1 Mapping Results Overview 8
    3.2 Gaps Analysis 9
4. Conclusion 11

1. Introduction

The financial services industry is one of the most critical sectors in any market, and financial institutions (FIs) face myriad regulations. In the case of Singapore FIs[1], for example, the Banking Act oversees banking institutions, the Securities and Futures Act governs capital market intermediaries, and the Insurance Act regulates insurers. Additionally, there are numerous guidelines, frameworks, and best practices recommended for FIs designed to improve operations, enhance governance, and reduce risks, among other goals. For example, the Monetary Authority of Singapore issued the Technology and Risk Management (TRM) Guidelines to help FIs minimize technology usage risk.

While challenging, it is imperative that conscientious FIs routinely review these available regulations, guidelines, frameworks, and best practices. These FIs should comply with mandatory regulations and carefully analyze which best practices and recommendations to adopt to reduce overall risk exposure and keep up with industry progress. This mammoth task gets exponentially difficult for FIs operating beyond a single country or regulatory space, especially when relevant regulations and frameworks are constantly evolving.

There are multiple frameworks and guidelines available in the technology space, such as the above-mentioned TRM, ISO/IEC 27001 & 27002, and ISACA COBIT. There are also ISO/IEC 27018, the recently published ISO/IEC 21878, FedRAMP, and the *Cloud Computing Implementation Guide (CCIG) 2.0*[2] issued by the Association of Banks in Singapore (ABS) that are specific to cloud computing and its related technologies.

The capacity to map frameworks is a useful and popular tool for FIs seeking compliance under multiple standards and best practices. The *Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)*[3]—currently at v3.0.1—provides Fis with this capability because it illustrates the relationship between *CSA's Security Guidance*[4] in 14 domains with more than 30 industry-accepted global security standards, regulations, and controls frameworks.

2. Background

2.1 Working Group (WG) to Map *ABS CCIG 2.0* to *CCM*

CSA convened a WG to map ABS CCIG 2.0 to CCM. This exercise aims to effectively evaluate the similarities and gaps between ABS CCIG 2.0 and the numerous frameworks mapped in the CCM. Singapore FIs that are already in line with ABS CCIG 2.0 can easily identify and fulfill additional controls (gaps) on top of the ABS CCIG 2.0 to achieve adherence to other targeted frameworks within CCM, which is useful when expanding to other markets.

[1] https://eservices.mas.gov.sg/fid

[2] https://abs.org.sg/docs/library/abs-cloud-computing-implementation-guide.pdf

[3] https://cloudsecurityalliance.org/research/cloud-controls-matrix/

[4] https://cloudsecurityalliance.org/research/guidance/

This gap analysis report accompanies the *CSA CCM v3.0.1 Addendum-Association of Banks in Singapore Cloud Computing Implementation Guide 2.0.*

2.2 CSA CCM

The *CSA CCM v3.0.1* is a cybersecurity control framework for cloud computing, composed of 133 control objectives structured in 16 domains covering all key aspects of the cloud technology. It can be used as a tool for the systematic risk assessment of cloud security controls implementation and provides guidance on which security controls to enable (and by which actor) within the cloud supply chain.

The controls framework is aligned to the *Security Guidance v4.0* and is currently considered a de-facto standard for cloud security assurance and compliance.

The controls in the *CCM* have been mapped against industry-accepted security standards, regulations, and control frameworks including, but not limited to: ISO 27001/27002/27017/27018, NIST SP 800-53, AICPA TSC, ENISA Information Assurance Framework, German BSI C5, PCI DSS, ISACA COBIT, NERC CIP, and many others.

2.3 *ABS CCIG 2.0*

The *ABS CCIG 2.0* was released by the Association of Banks in Singapore in August 2019 for FIs to use when entering into cloud outsourcing arrangements, as well as the ongoing management of these arrangements.

A statement from the ABS CCIG 2.0 reads:

> *"The recommendations that lie within have been discussed and agreed by members of the ABS Standing Committee for Cyber Security (SCCS) with the intent to assist FIs in understanding approaches to due diligence, vendor management and key controls that should be implemented on an on-going basis in Cloud outsourcing arrangements.*
>
> *Additionally it can be used by Cloud Service Providers (CSPs) to better understand what is required to achieve successful Cloud outsourcing arrangements with FIs.*
>
> *The guiding principle that controls in the Cloud must be at least as strong as those which the FIs would have implemented had the operations been performed in-house should apply."*

2.4 Controls Mapping and Terminologies

The *Methodology for the Mapping of the CCM*[5] provides detailed steps for the mapping exercise. Some pertinent content and terminologies are summarized in the following section for easier reference.

Mappings: *CCM as a base to ABS CCIG 2.0*

Each control (criterion) in the *CCM* is matched to a control(s) in *ABS CCIG 2.0* to make an equivalency determination. This approach considers which *CCM* controls are associated with the criteria in other established frameworks—and to what degree they are equivalent to each other. This comparison generates an estimate on the extent of new efforts necessary to incorporate other frameworks (using the *CCM* as a base).

Gap Identification and Analysis: No Gap, Partial Gap, and Full Gap

A gap identification is essentially an analysis (of two or more frameworks) that seeks to determine the level of semantic equivalence between frameworks that concludes with three potential outcomes: no gap, partial gap, and full gap. The following considerations must be analyzed to identify which of those three conclusions apply.

> - No gap: For a specific CCM control and its requirements, there is an equivalent control or set of controls (in the candidate framework) that fully satisfies the requirements of a corresponding control in the CCM.
> - Partial gap: For a specific CCM control and its requirements, there is a control or set of controls (in the candidate framework) that do not fully satisfy the corresponding control requirements in the CCM. For the 'partial gap' case to hold, there should be at least one control in the candidate framework of semantic equivalence to a requirement in the CCM control. The relevant control(s) in the candidate framework should then be cited in the work package.
> - Full gap: For a specific CCM control and its requirements, there is no control or set of controls (in the candidate framework) of semantic equivalence. Essentially, this means that the CCM control is entirely unaddressed by any control in the candidate framework.

Furthermore, a gap analysis provides indicators on how much effort may be necessary to bridge gaps between required frameworks.

[5] https://downloads.cloudsecurityalliance.org/assets/research/cloud-controls-matrix/ccm-mapping-methodology.pdf

3. Mapping of *ABS CCIG 2.0* to *CCM*

3.1 Mapping Results Overview

The following pie chart illustrates the breakdown of the mapping results from *ABS CCIG 2.0* to *CCM*. The WG determined the *ABS CCIG 2.0* had no gap with 55 controls, partial gaps with 33 controls, and full gaps with 45 *CCM* controls.

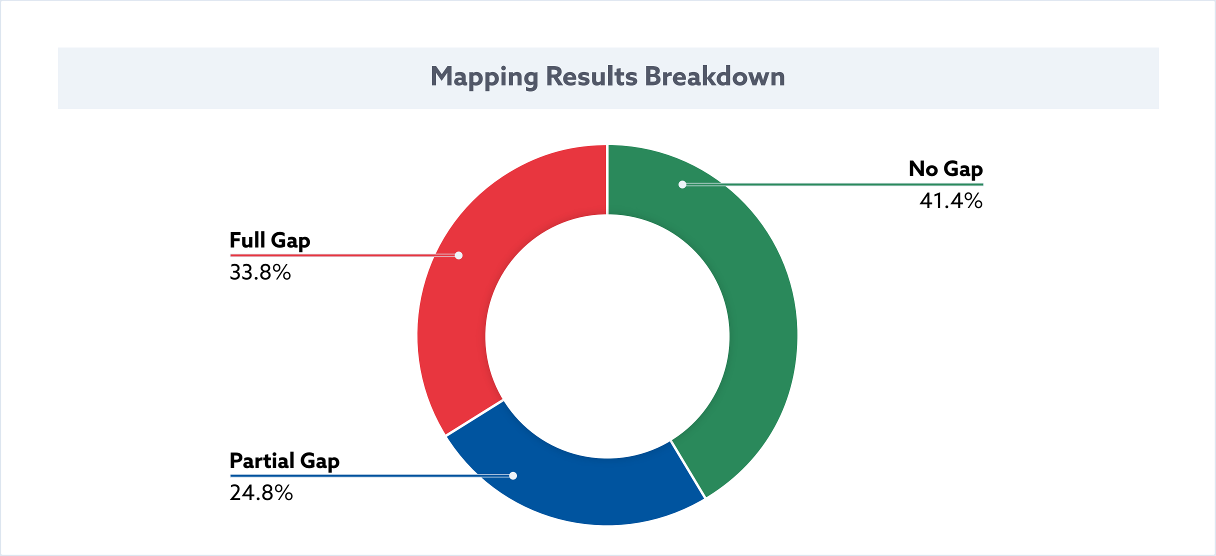

Figure 1

3.2 Gaps Analysis

The following table provides a further breakdown of the gaps between *ABS CCIG 2.0* and *CCM* across each of the 16 domains in *CCM*.

			Number of controls				%		
No	CCM Domains		Total	No Gap	Partial Gap	Full Gap	No Gap	Partial Gap	Full Gap
1	Application & Interface Security	AIS	4	3	0	1	75.0	0.0	25.0
2	Audit Assurance & Compliance	AAC	3	1	2	0	33.3	66.7	0.0
3	Business Continuity Management & Op Resilience	BCR	11	9	2	0	81.8	18.2	0.0
4	Change Control & Configuration Management	CCC	5	2	2	1	40.0	40.0	20.0
5	Data Security & Information Lifecycle Management	DSI	7	5	1	1	71.4	14.3	14.3
6	Datacenter Security	DCS	9	6	2	1	66.7	22.2	11.1
7	Encryption & Key Management	EKM	4	4	0	0	100.0	0.0	0.0
8	Governance & Risk Management	GRM	11	2	7	2	18.2	63.6	18.2
9	Human Resources Security	HRS	11	0	1	10	0.0	9.1	90.9
10	Identity & Access Management	IAM	13	12	1	0	92.3	7.7	0.0
11	Infrastructure & Virtualization	IVS	13	5	5	3	38.5	38.5	23.1
12	Interoperability & Portability	IPY	5	0	2	3	0.0	40.0	60.0
13	Mobile Security	MOS	20	0	0	20	0.0	0.0	100.0
14	Sec. Incident Management, E-Disc & Cloud Forensics	SEF	5	4	0	1	80.0	0.0	20.0
15	Supply Chain Management, Transparency & Accountability	STA	9	2	6	1	22.2	66.7	11.1
16	Threat & Vulnerability Management	TVM	3	0	2	1	0.0	66.7	33.3

The following bar chart illustrates the gaps between *ABS CCIG 2.0* and each of the 16 *CCM* domains (represented by the domain IDs on the x-axis). A more extensive green section describes significant similarities in specific domains between *ABS CCIG 2.0* and *CCM*. Conversely, a larger red area translates to bigger differences in domains. The orange sections, strictly speaking, do not convey sufficient information about the similarities and differences as the overlaps in a 'partial gap' could be anywhere in between.

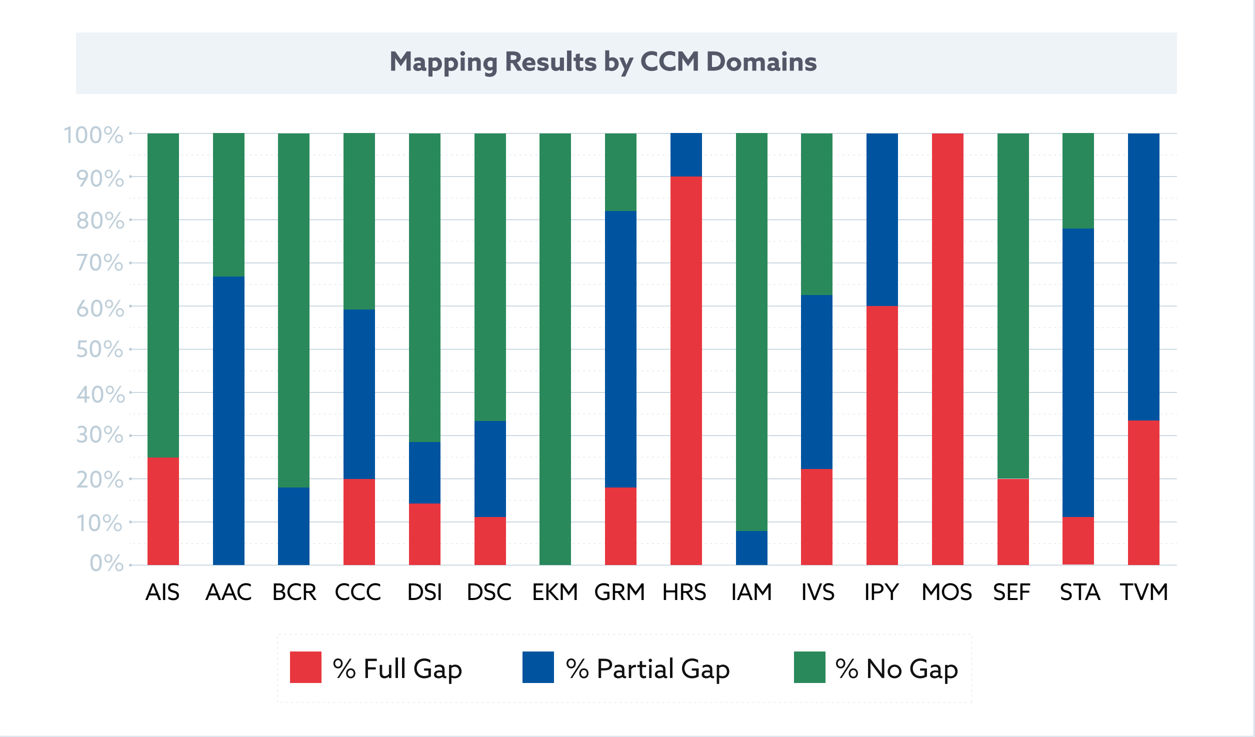

Figure 2

Key observations from the mapping results:

- In general, there are more similarities than differences between the two frameworks
- The two frameworks have full overlaps in the Encryption & Key Management domain
- The two frameworks have only minor differences in the Identify & Access Management domain
- The most considerable differences between the two frameworks stems from the absence of controls in the following two domains that were required in the CCM:
  - Mobile Security (MOS)
  - Human Resources Security (HRS)

4. Conclusion

There are subtle differences between the ABS CCIG 2.0 and the CCM in terms of the target audience. The ABS CCIG 2.0 is intended as a guide to help FIs manage cloud outsourcing arrangements, such as the due diligence assessments of CSPs to technical aspects such as cryptographic key management, penetration testing, and disaster recovery. The CCM was designed as a tool for the direct and systematic assessment of cloud providers and cloud implementations.

The by-proxy nature in which FIs assess the CSPs using ABS CCIG 2.0 means that the absence of controls in certain CCM domains is understandable, as they can be unfeasible to evaluate or implement. For example, while the ABS CCIG 2.0 does not address Human Resources Security (HRS), the likely explanations for this omission are that FIs don't want to impose human resources policies (employment agreements, terminations, etc.) on CSPs, or they can't.

As a highly-regulated sector, an overarching caveat is reiterated in ABS CCIG 2.0: "The guiding principle that controls in the Cloud must be at least as strong as those which the FIs would have implemented had the operations been performed in-house should apply."

As such, FIs—it can be argued—would need to fully satisfy themselves that they can exert an appropriate amount of control over a CSP before solidifying a working relationship to avoid getting into trouble with regulators.

Ultimately, the mapping results from ABS CCIG 2.0 to CSA CCM serve as a useful tool for FIs to perform a holistic security assessment of CSPs from both a local (Singapore) and international (CCM) lens.