Gap Analysis Report on Mapping CSA's Cloud Controls Matrix to 'Guideline on Effectively Managing Security Service in the Cloud'

cloud security alliance®

Acknowledgments

Co-Chair:

Kai Chen

Working Group Members:

Diego Fernandez Vazquez
Aditya Bhelke
Rosita Hoving
Andrea Knoblauch
Chunxiong Mao
Amirtharaj Thankaraj
Water Zhang

CSA Staff:

Jane Chow
Hing-Yan Lee
Ekta Mishra
Zhuang Haojie

Table of Contents

Introduction

Background of Cloud Controls Matrix

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The CSA CCM provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the CSA Security Guidance in 14 domains. The foundations of the CSA CCM rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP and will augment or provide internal control direction for service organization control reports attestations provided by cloud providers.

As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry. The CSA CCM strengthens existing information security control environments by emphasizing business information security control requirements, reduces and identifies consistent security threats and vulnerabilities in the cloud, provides standardized security and operational risk management, and seeks to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud.

Background of 'Guidelines on Effectively Managing Security Service in the Cloud'

The document, hereinafter referred to as 'The Guideline', was developed by CSA's Cloud Security Services Management Working Group. Based on the shared security responsibility model, specific security responsibilities are divided between the cloud service provider and cloud customer in different cloud service deployment environments (e.g. IaaS, PaaS, and SaaS) and, where applicable, cloud security service providers offering Security-as-a-Service (SecaaS) for cloud platforms. For each security responsibility there are one or more security features or functions defined to support it. The document provides guidance on how to fulfil cloud controls (based on CCM) by using third-party security products and services.

CCM – The Guideline Mapping

The CSA's Cloud Security Service Management WG conducted the mapping of CSA CCM version 3.0.1 to The Guideline. The main objective of this work is to provide an overview of the differences between the security recommendations listed in The Guideline and CSA CCM controls.

Based on the Methodology for the Mapping of the Cloud Controls Matrix:

Mappings – CCM as Base to The Guideline

Each control (criteria) in the CCM is initially matched to a control(s) in The Guideline to make an equivalency determination. This approach considers which CCM criteria are associated with the criteria in other established frameworks—and to what degree they are equivalent to each other—thus, estimating the extent of new efforts necessary to incorporate other frameworks (using the CCM as a base).

Reporting Gap Identification and Analysis

Gap summaries identify full gaps and partial gaps. Full gaps are specific criteria (controls) not included in another framework. Partial gaps include similar criteria (controls) that exist but do not fully match. A completed gap analysis can help inform planning efforts related to determining the appropriateness of extending existing compliance documentation to match another framework. For the purposes of the CCM, a 'gap analysis' specifically lists and explains the gaps between controls in the CCM and another framework.

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

A gap identification is essentially an analysis (of two or more frameworks) that seeks to determine the level of semantic equivalence between frameworks. During the gap identification process, three potential cases are considered: no gap, partial gap and full gap. To identify which of those three scenarios apply, the following must be considered:

1. 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.
2. 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 requirements of the corresponding control in the CCM. In order for the 'partial gap' case to hold, there should be at least one control in the candidate framework that is 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.
3. Full gap: For a specific CCM control and its requirements, there is no control or set of controls (in the candidate framework) that is of semantic equivalence. Essentially, this means that the CCM control is completely 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.

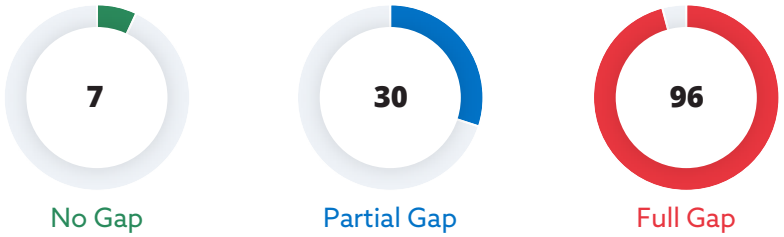
The mapping result shows that gaps exist between The Guideline and CSA CCM version 3.0.1. An analysis of the gaps and why they exist are addressed in subsequent chapters.

Mapping – CCM as Base to The Guideline

Summary of the Mapping Result

Among 133 controls in CSA CCM, there are 96 controls that The Guideline does not have semantic equivalence to, and 30 controls that partially satisfy the corresponding control in CCM.

Using CCM as a Base



Gap Analysis

The gaps between The Guideline and CSA CCM version 3.0.1 come from the following domains:

No.	Domain		% Full Gap	% Partial Gap	% No Gap
1	AIS	Application and Interface Security	25.00%	25.00%	50.00%
2	AAC	Audit Assurance and Compliance	100.00%	0.00%	0.00%
3	BCR	Business Continuity Mangement and Op Resilience	72.73%	18.18%	9.09%
4	CCC	Change Control and Configuration Management	60.00%	40.00%	0.00%
5	DSI	Data Security and Information Lifecycle Mangement	100.00%	0.00%	0.00%
6	DSC	Datacenter Security	55.56%	33.33%	11.11%
7	EKM	Encryption and Key Management	25.00%	75.00%	0.00%
8	GRM	Governance and Risk Management	100.00%	0.00%	0.00%
9	HRS	Human Resources Security	90.91%	0.00%	9.09%
10	IAM	Identity and Access Management	38.46%	53.85%	7.69%

11	IVS	Infrastructure and Virtualization	46.15%	46.15%	7.69%
12	IPY	Interoperability and Portability	80.00%	20.00%	0.00%
13	MOS	Mobile Security	100.00%	0.00%	0.00%
14	SEF	Security Incident Managment, E-Disc and Cloud Forensics	100.00%	0.00%	0.00%
15	STA	Supply Chain Managment, Transparency and Accountability	100.00%	0.00%	0.00%
16	TVM	Threat and Vulnerability Management	0.00%	66.67%	33.33%

Table 1 – Breakdown of gaps in mapping

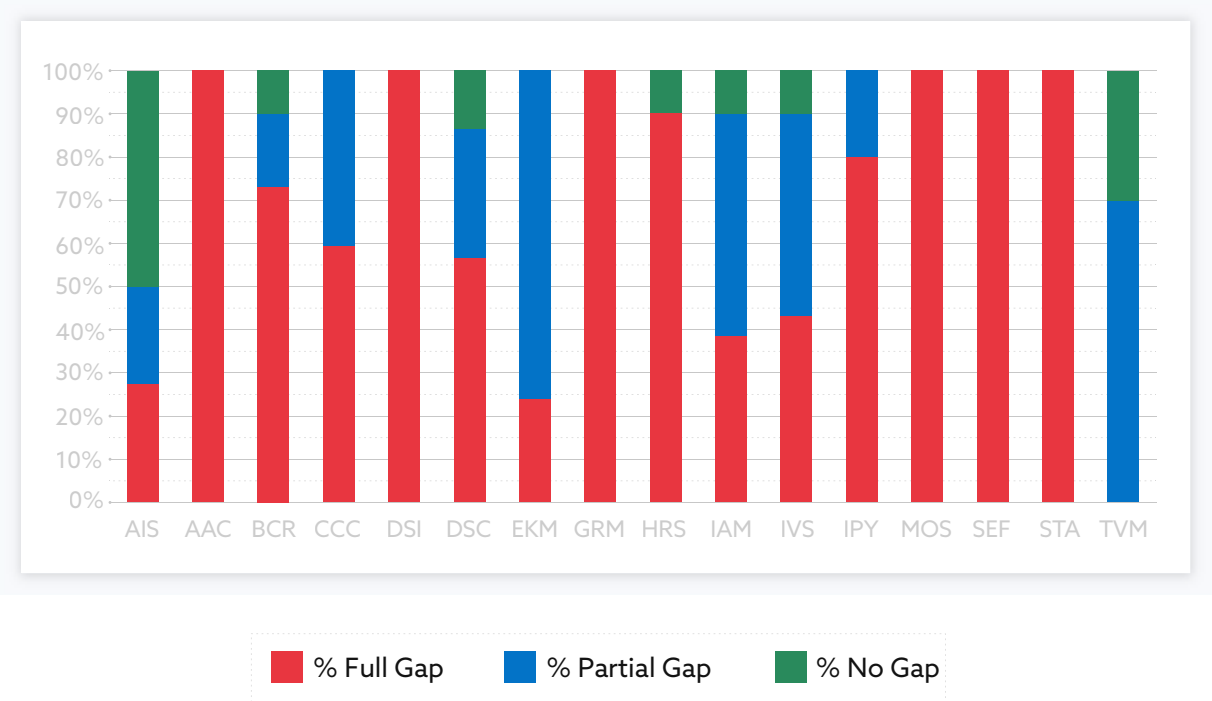


Chart 1 – Gaps in mapping sorted by domain

As The Guideline largely focuses on technical security service development and management in the cloud, aspects such as cloud security planning, governance and operational management are not elucidated. This aligns with the break down (Table 1 and Chart 1) where domains from which full gaps originate (rows highlighted in Table 1) slant toward functional application and management.

Recommendations To The Audience

The Guideline mainly serves as a cloud security technical guideline in building a cloud platform and deploying a cloud business environment, where it covers common security responsibilities, infrastructure, virtualization, host, middleware, application, data security and operation & maintenance, etc. Heavily focused on security technology requirements and implementation measures for cloud service systems, The Guideline provides in depth guidance on how to achieve cloud controls by using third-party commercially available security products and services.

Despite the technical content in The Guideline, the percentage of Full Gap and Partial Gap of technical controls are still high. This can be attributed to the fact that controls embedded within The Guidelines are not a direct and intentional match to controls described in the CCM.

For example, Cloud Log Audit (ID# 3.2.7.7) in The Guideline covers classification and management of log audits but this is not found under the CCM umbrella. While it is not directly mappable, The Guidelines and CCM cover different aspects of security controls in the same domains and should be referenced together to form a holistic set of security controls.

Users of The Guideline should understand the gaps lie largely in the functional domains of CCM. The purpose of this mapping is to bring users of The Guideline a step closer to being CCM compliant if they wish to, by understanding what it takes to go from The Guidelines to CCM. This helps to refine planning efforts in assessing the compatibility of extrapolating existing security controls to match another framework.

