Cross-mapping between CSA Cyber Trust and Cloud Security Alliance Cloud Controls Matrix v4

Date of Publication: 17-10-2023 (First edition)

A publication by

About the Cyber Security Agency of Singapore (CSA)

Established in 2015, CSA seeks to keep Singapore's cyberspace safe and secure to underpin our National Security, power a Digital Economy and protect our Digital Way of Life. It maintains an oversight of national cybersecurity functions and works with sector leads to protect Singapore's Critical Information Infrastructure. CSA also engages with various stakeholders to heighten cybersecurity awareness, build a vibrant cybersecurity ecosystem supported by a robust workforce, pursue international partnerships and drive regional cybersecurity capacity building programmes.

For more news and information, please visit www.csa.gov.sg

Contents

1 Introduction

CSA Cyber Essentials mark and Cyber Trust mark are tiered cybersecurity standards that are designed to support the cybersecurity needs of a range of organisations.

The Cyber Essentials mark takes on a baseline control approach and is intended to protect organisations against common cyberattacks. The Cyber Trust mark takes on a risk-based approach and is intended to enable organisations to put in place the relevant cybersecurity preparedness measures that commensurate with their cybersecurity risk profile.

Together, the Cyber Essentials mark and Cyber Trust mark provide a cybersecurity risk management framework for organisations.

Globally, the industry has seen a rise in cloud adoption[1]. As organisations embrace cloud, adversaries are also evolving their Tactics, Techniques and Procedures (TTPs) to target organisations in the cloud. Cloud exploitation cases have grown, and the industry has seen an increase in cases involving adversaries targeting cloud environments.[2]

The Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing that is developed by the Cloud Security Alliance. It is a tool for the systematic assessment of a cloud implementation and provides guidance on which security controls should be implemented by which actor within the cloud supply chain.

The "Cross-mapping between CSA Cyber Trust and Cloud Security Alliance Cloud Controls Matrix v4" document maps the cybersecurity preparedness domains in CSA Cyber Trust mark to the domains in the Cloud Security Alliance CCM v4.

2 Intended audience

The "Cross-mapping between CSA Cyber Trust and Cloud Security Alliance Cloud Controls Matrix v4" is intended to serve as an implementation guide to accompany the Cyber Trust mark certification document.

Cyber Trust mark is targeted at larger or more digitalised organisations that have gone beyond cyber hygiene. These organisations may have higher risk levels and would correspondingly invest in expertise and resources to manage and protect their Information Technology (IT) infrastructure.

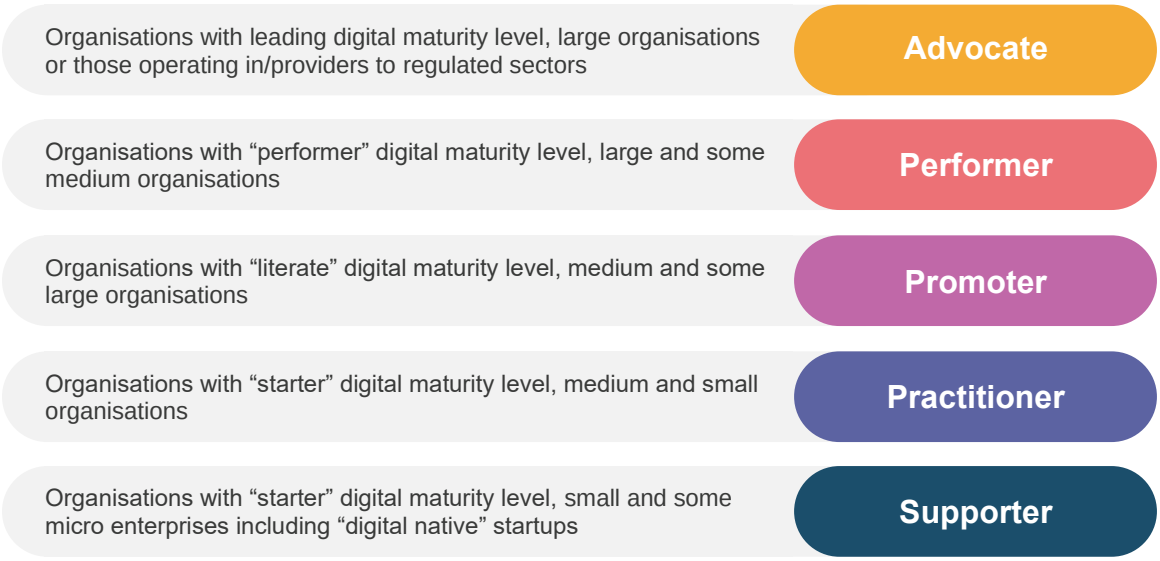
Therefore, this implementation guide is targeted at organisations that have cybersecurity personnel overseeing cybersecurity risk assessment in the organisation. These target organisations are those that have implemented cloud, and have mapped their cybersecurity controls to the Cloud Security Alliance CCM. The target organisations would also be those implementing or preparing to implement the cybersecurity preparedness domains in the Cyber Trust mark.

3 Scope of this document

The Cyber Trust mark takes on a risk-based approach to guide organisations in identifying gaps in their cybersecurity implementation. To address the differing risk levels of organisations, the Cyber Trust mark

[1] Cloud Security Alliance, 2022, *"Measuring Risk and Risk Governance"*
[2] CrowdStrike, 2023, *"2023 Cloud Risk Report"*

has five (5) cybersecurity preparedness tiers, with the associated indicative organisation profiles (Figure 1).



1 – Organisations of the same size may have different risk profiles, and correspondingly, need to be at different cybersecurity preparedness tiers
2 – Description of digital maturity level aligns to terminology in IMDA Digital Acceleration Index (DAI)

Figure 1 – Cyber Trust mark cybersecurity preparedness tiers and indicative organisation profiles

The Cyber Trust mark consists of twenty-two (22) cybersecurity preparedness domains, each focused around a specific cybersecurity theme (Figure 2 and Table 1). A series of cybersecurity preparedness statements are developed for each domain and organised into five (5) cybersecurity preparedness tiers.

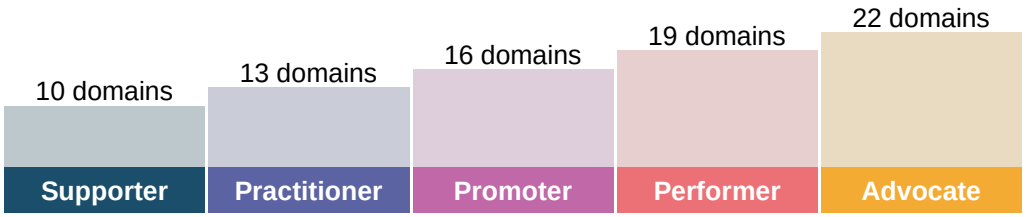


Figure 2 – Cyber Trust mark preparedness tiers and domains

Cross-mapping between Cyber Trust and CCMv4

Table 1 – Domains applicable for each cybersecurity preparedness tier

Tier	Supporter	Practitioner	Promoter	Performer	Advocate
Cyber governance and oversight					
1. Governance			●	●	●
2. Policies and procedure			●	●	●
3. Risk management	●	●	●	●	●
4. Cyber strategy					●
5. Compliance	●	●	●	●	●
6. Audit				●	●
Cyber education					
7. Training and awareness *	●	●	●	●	●
Information asset protection					
8. Asset management *	●	●	●	●	●
9. Data protection and privacy *	●	●	●	●	●
10. Backups *	●	●	●	●	●
11. Bring Your Own Device (BYOD)				●	●
12. System security *	●	●	●	●	●
13. Anti-virus/anti-malware *	●	●	●	●	●
14. Secure Software Development Lifecycle (SDLC)					●
Secure access and environment					
15. Access control *	●	●	●	●	●
16. Cyber threat management				●	●
17. Third-party risk and oversight					●
18. Vulnerability assessment			●	●	●
19. Physical/environmental security		●	●	●	●
20. Network security		●	●	●	●
Cybersecurity resilience					
21. Incident response *	●	●	●	●	●
22. Business continuity/ disaster recovery		●	●	●	●
No of domains	10	13	16	19	22

* Measures in Cyber Essentials mark

All five (5) tiers and twenty-two (22) cybersecurity preparedness domains are covered in the scope of this cross-mapping to the Cloud Security Alliance CCM.

Organisations that are Software-as-a-Service (SaaS) users and seeking direct cloud-specific implementation guidance for SaaS should refer to the “Cyber Essentials mark: Cloud Security Companion Guide” instead.

4 Acknowledgements

This companion guide is jointly developed between CSA and Cloud Security Alliance.

CSA has partnered with the following cloud services providers to further outline their respective cloud security best practices in alignment to the cloud security companion guides for Cyber Essentials and Cyber Trust:

– Amazon Web Services
– Microsoft Singapore
– Google Cloud

CSA has also sought inputs from the following cloud services providers:

– Huawei International Pte Ltd

CSA would like to acknowledge all industry partners for their support and contributions.

5 Approach for Cyber Trust

Due to the risk-based approach taken for the Cyber Trust mark, the cybersecurity preparedness statements in the twenty two (22) domains for Cyber Trust are organised into five (5) cybersecurity preparedness tiers.

The description of the statements in each cybersecurity preparedness domain are organised in escalating order – the statements start with descriptions of more basic or rudimentary implementation and increase in the level of involvement or intensity.

The description of the statements in the lower tiers of some cybersecurity preparedness domains are also consistent with the provisions in Cyber Essentials. Such statements may be drafted to reflect measures at implementation level, as Cyber Essentials is intended to provide more direct implementation guidance for smaller or less digitalised organisations.

At the higher tiers of Cyber Trust, the cybersecurity preparedness statements in some domains refer to the use of technology solutions. This is intended to reflect the use of technological measures in organisations at a higher risk level to better enable them to automate their operations, as well as to speed up and scale their management of cybersecurity.

Organisations typically start with the statements in the lowest cybersecurity preparedness tier and progressively move on to the subsequent cybersecurity preparedness statement(s) and/or tier(s). This is illustrated in Table 2.

Table 2 - Example of organisation progressively filling cybersecurity preparedness tier template

Preparedness tier	Description	Question	Organisation response *(Yes, No, Not applicable)*	Justification if "Not applicable"
Supporter	*Description*	*Question*		
Practitioner	*Description*	*Question*		
Promoter	*Description*	*Question*		
Performer	*Description*	*Question*		
Advocate	*Description*	*Question*		

Annex I shows visualisation depicting the mapping of each of the cybersecurity preparedness domains in Cyber Trust mark to the control specifications in CCMv4.

Annex II shows visualisation depicting the mapping of each of the five (5) tiers of Cyber Trust mark to the control specifications in CCMv4.

Annex III contains the mapping of the cybersecurity preparedness domains in Cyber Trust mark to the control specifications in CCMv4.

6 References

In preparing this document, reference was made to the following publication(s):

1. Cloud Controls Matrix v4 by Cloud Security Alliance

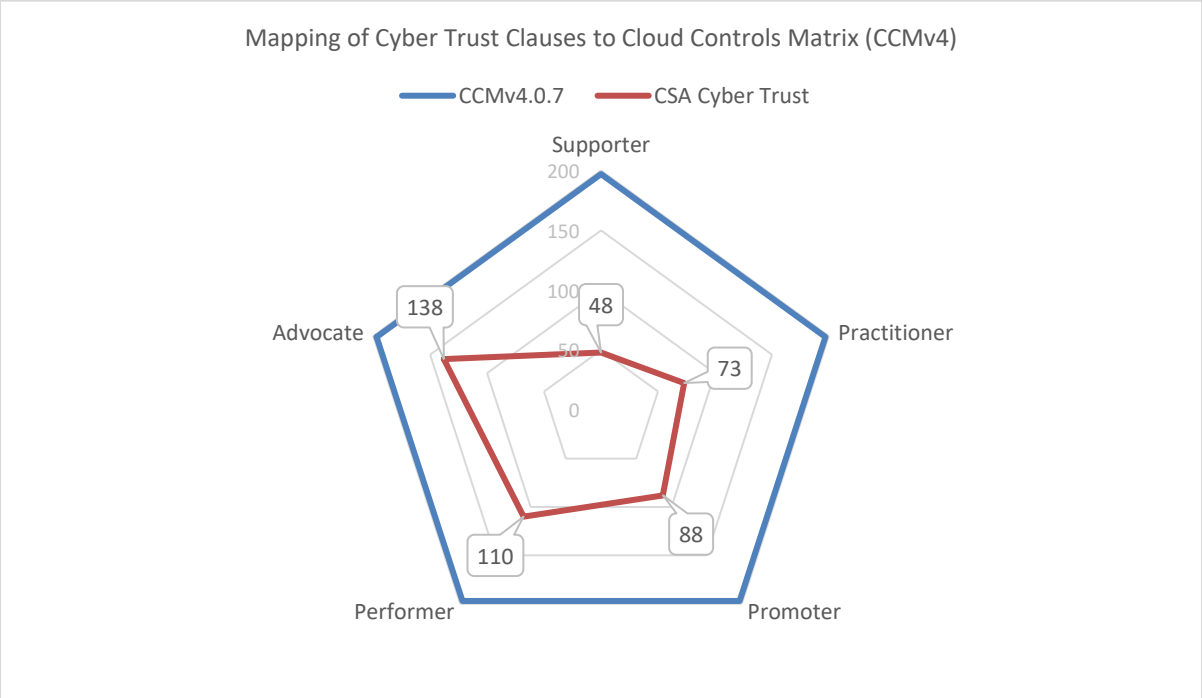
Acknowledgement is made for the use of information from the above publication(s).

Annex I

Visualisation depicting mapping of Cyber Trust mark to CCMv4

Annex I shows visualisation depicting the mapping of each of the cybersecurity preparedness domains in Cyber Trust mark to the control specifications in CCMv4.

Figure 3 show the mapping of clauses in Cyber Trust to the CCMv4.



	Cloud Controls Matrix (CCMv4)	Cyber Trust Clauses Mapped to CCMv4				
		Supporter	Practitioner	Promoter	Performer	Advocate
# of clauses	197	48	73	88	110	138
Percentage	100%	24.4%	37.1%	44.7%	55.8%	70.1%

Figure 3 – Mapping of Cyber Trust clauses to CCMv4

Cross-mapping between Cyber Trust and CCMv4

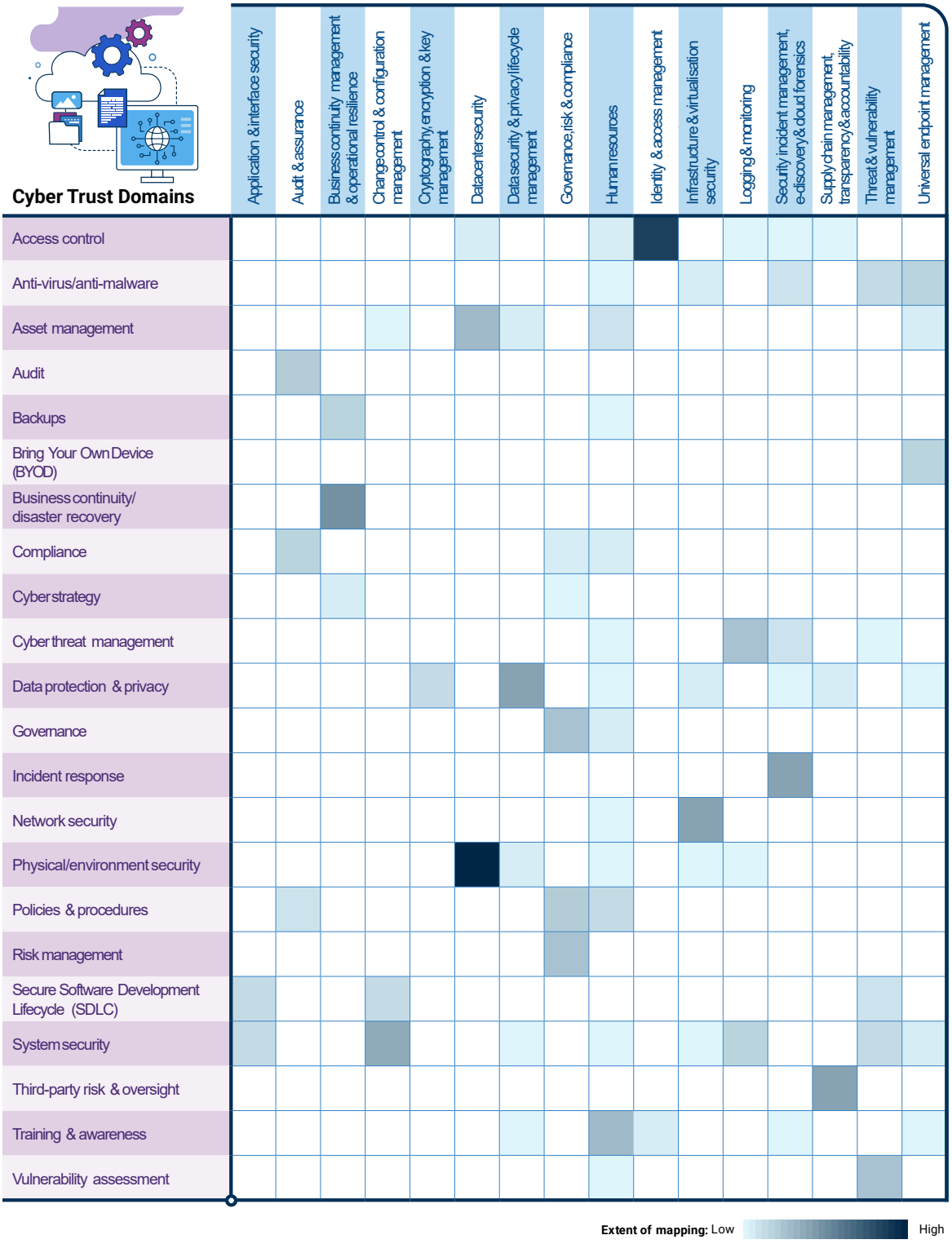


Figure 4 – Mapping of Cyber Trust domains to CCMv4 control domains

Annex II

Visualisation depicting mapping of Cyber Trust mark preparedness tiers to CCMv4

Annex II shows visualisation depicting the mapping of each of the five (5) tiers of Cyber Trust mark to the control specifications in CCMv4.

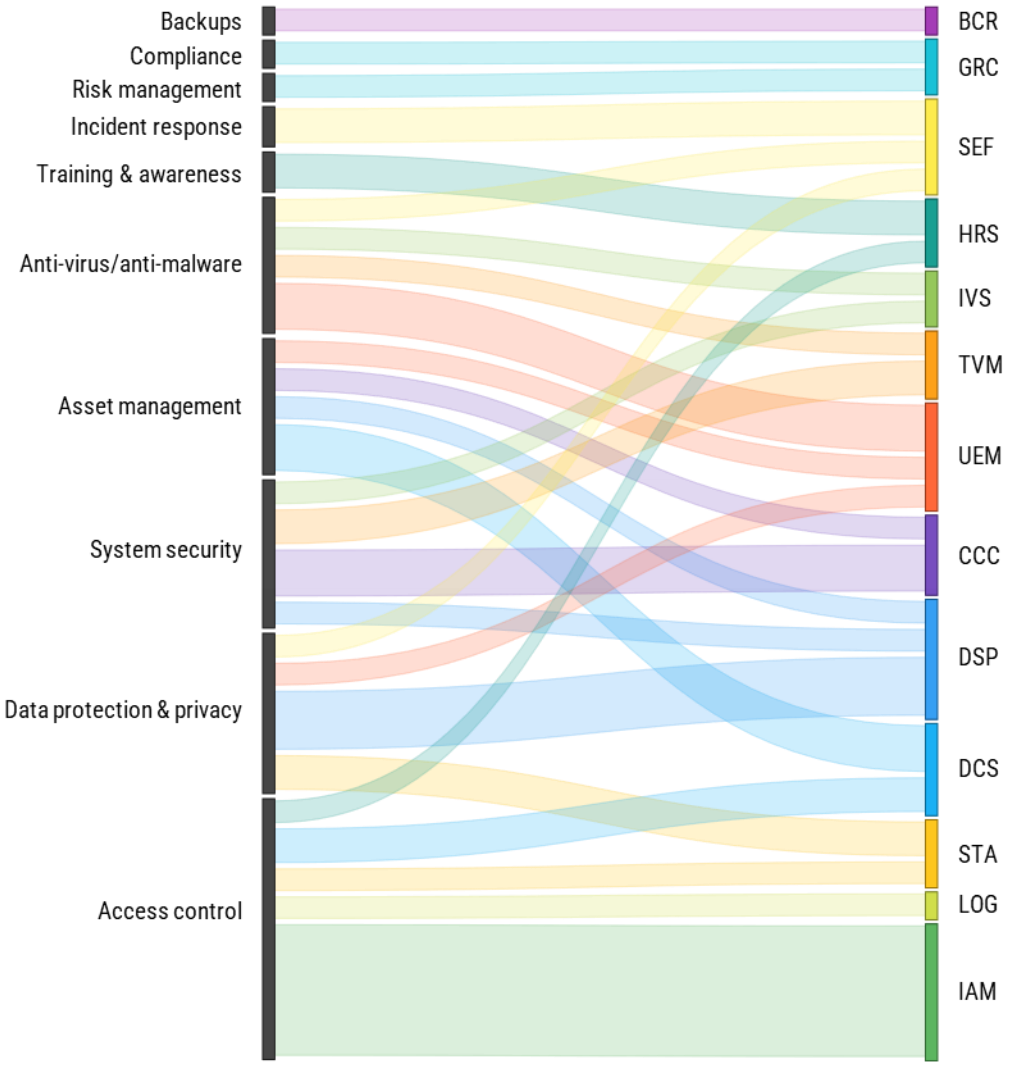


Figure 5 – Mapping of Cyber Trust "Supporter Tier" to CCMv4 control domains

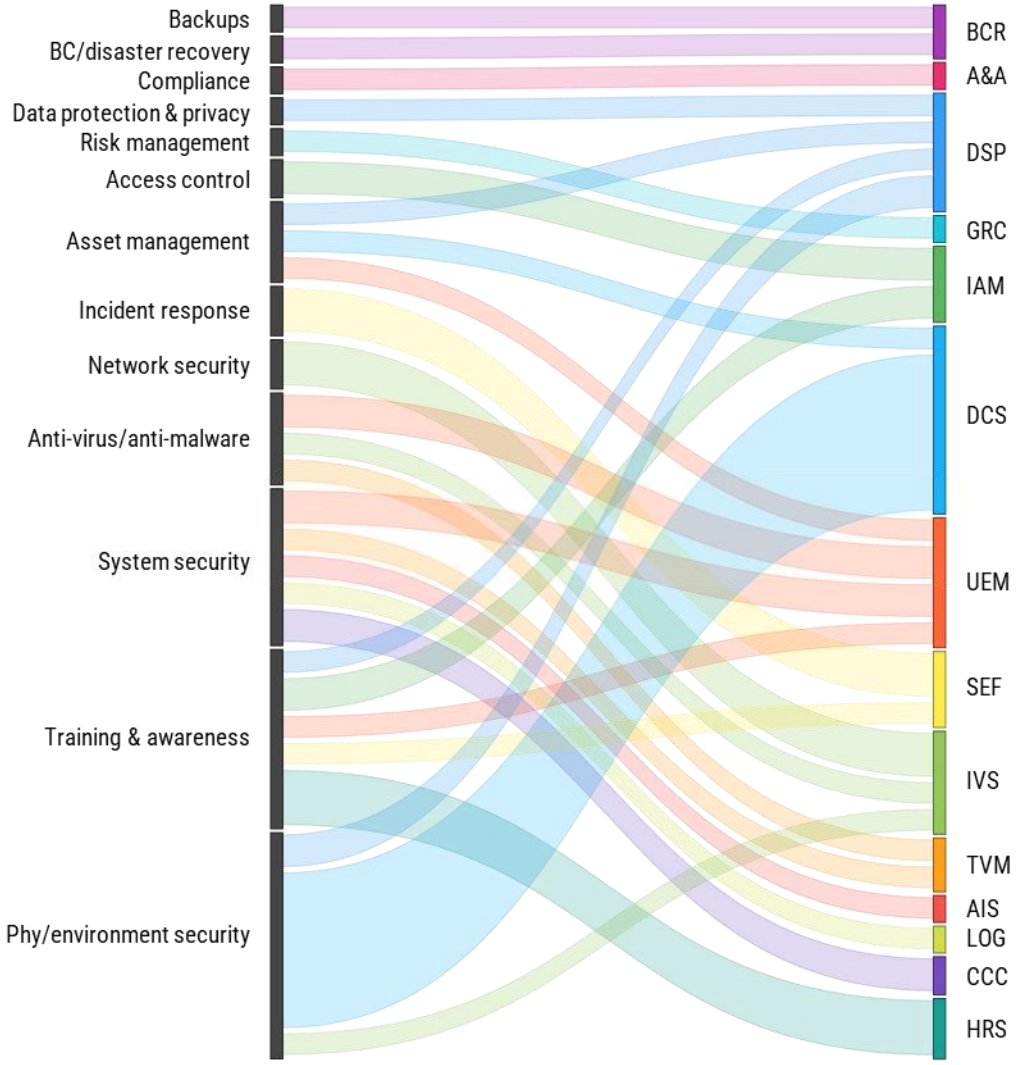


Figure 6 – Mapping of Cyber Trust "Practitioner Tier" to CCMv4 control domains

Cross-mapping between Cyber Trust and CCMv4

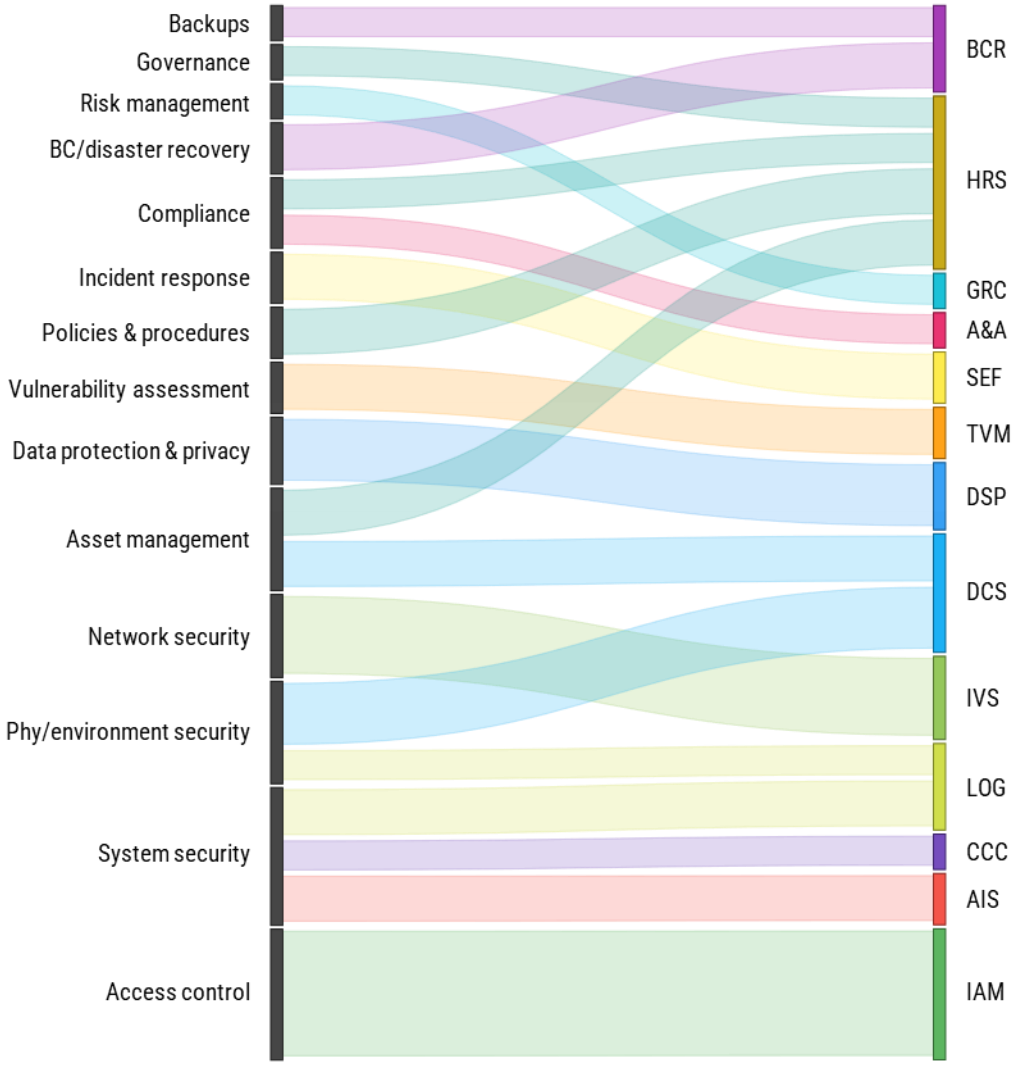


Figure 7 – Mapping of Cyber Trust "Promoter Tier" to CCMv4 control domains

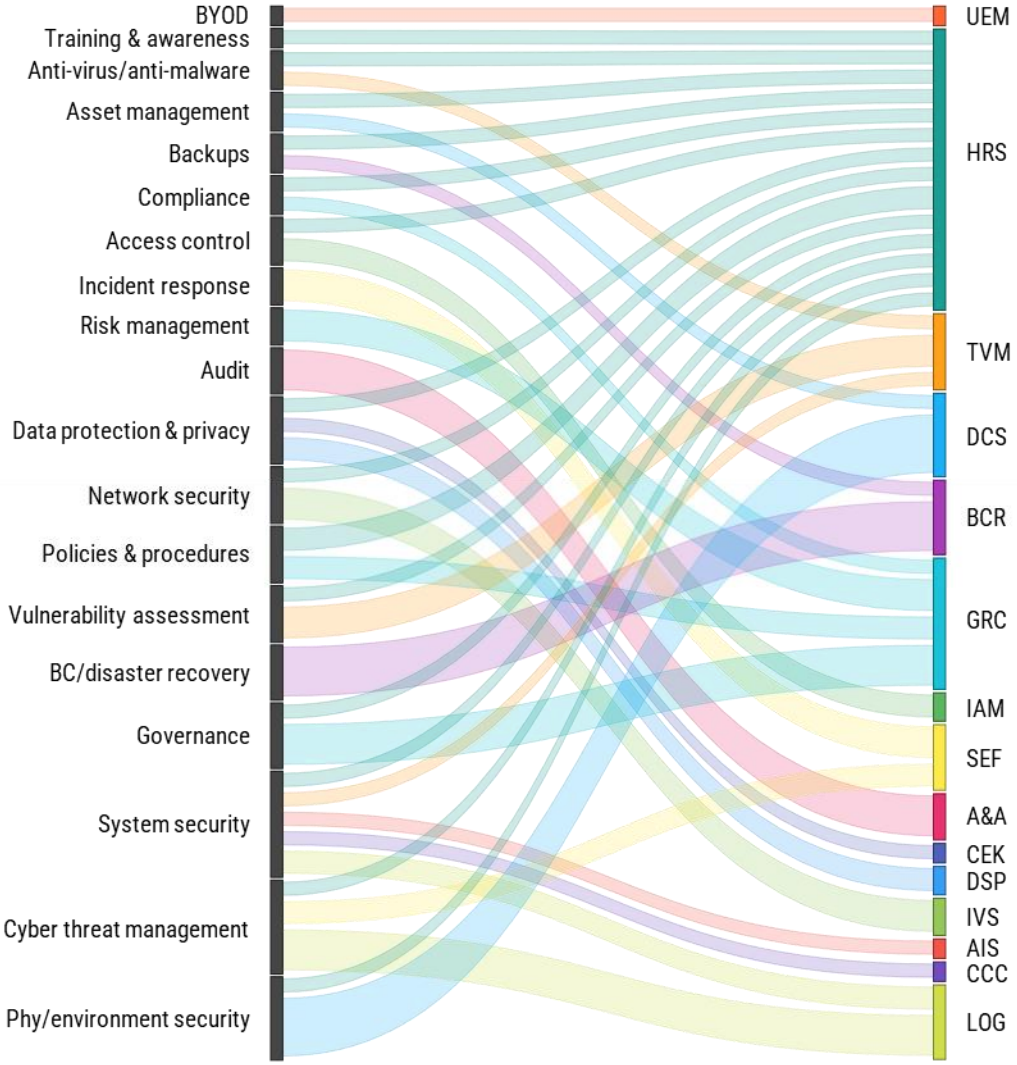


Figure 8 – Mapping of Cyber Trust "Performer Tier" to CCMv4 control domains

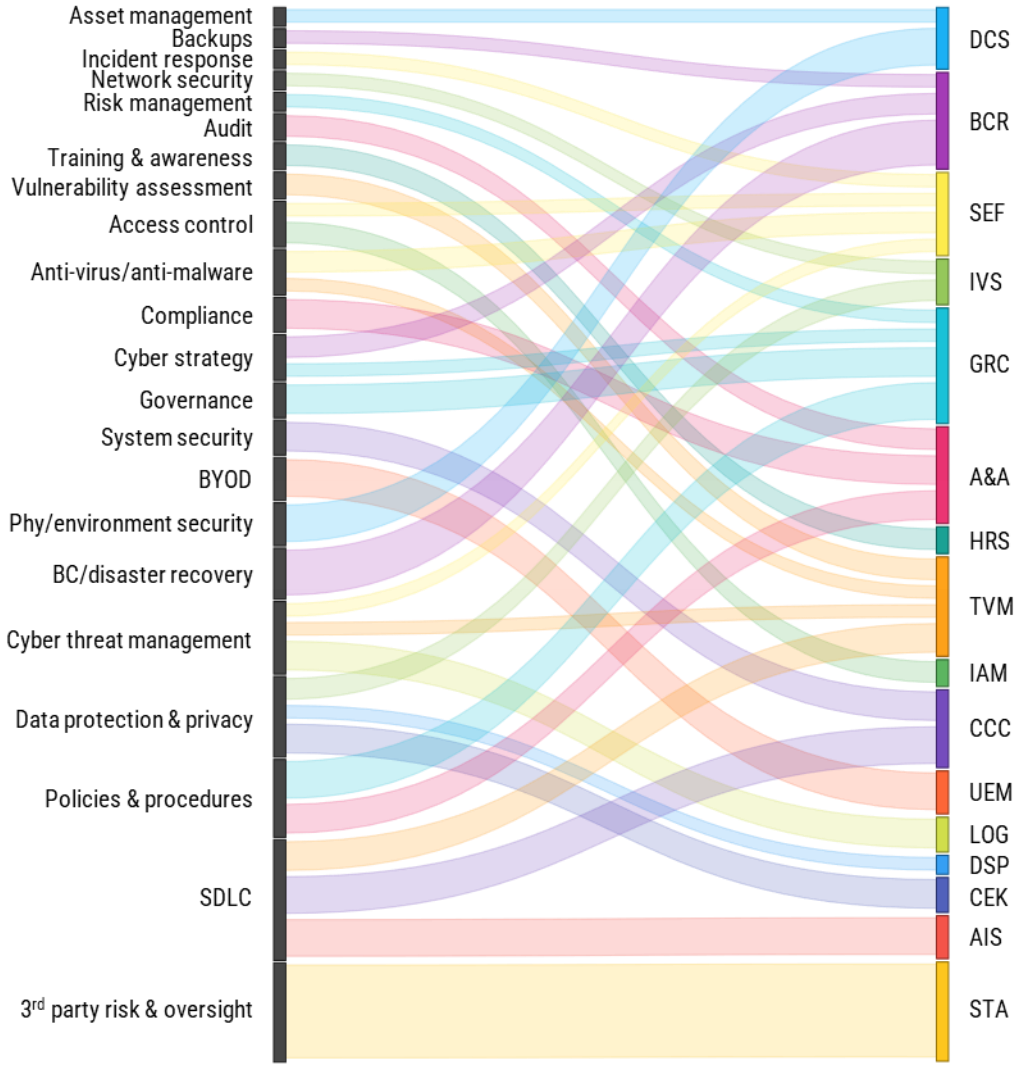


Figure 9 – Mapping of Cyber Trust "Advocate Tier" to CCMv4 control domains

Annex III

Mapping of Cyber Trust mark to CCMv4

Cyber Trust			CCMv4 Controls
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.1	Domain: Governance		
B.1.1	Supporter	Domain is not assessable for this tier	
B.1.2	Practitioner	Domain is not assessable for this tier	
B.1.3	Promoter		HRS-08
B.1.4	Performer		GRC-06 HRS-09
B.1.5			GRC-01 GRC-04
B.1.6			GRC-03
B.1.7	Advocate		GRC-05 GRC-07
B.1.8			GRC-02
B.2	Domain: Policies and procedures		
B.2.1	Supporter	Domain is not assessable for this tier	
B.2.2	Practitioner	Domain is not assessable for this tier	
B.2.3	Promoter		HRS-02 HRS-13
B.2.4	Performer		HRS-02
B.2.5			GRC-01 GRC-04
B.2.6			HRS-13
B.2.7	Advocate		A&A-01 GRC-01 GRC-03 GRC-04
B.2.8			A&A-01 GRC-01 GRC-02
B.2.9			A&A-05 A&A-06
B.3	Domain: Risk management		
B.3.1	Supporter		GRC-02
B.3.2			GRC-02
B.3.3	Practitioner		GRC-02

Cross-mapping between Cyber Trust and CCMv4

Cyber Trust			CCMv4 Controls
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.3.4			GRC-02
B.3.5	Promoter		GRC-02
B.3.6			GRC-02
B.3.7	Performer		GRC-02 GRC-03
B.3.8			GRC-02 GRC-06
B.3.9			GRC-02
B.3.10	Advocate		GRC-02
B.3.11			GRC-02
B.3.12			GRC-02
B.4	Domain: Cyber strategy		
B.4.1	Supporter	Domain is not assessable for this tier	
B.4.2	Practitioner	Domain is not assessable for this tier	
B.4.3	Promoter	Domain is not assessable for this tier	
B.4.4	Performer	Domain is not assessable for this tier	
B.4.5	Advocate		GRC-05 BCR-01 BCR-03
B.4.6			GRC-05
B.4.7			
B.4.8			
B.4.9			
B.5	Domain: Compliance		
B.5.1	Supporter		GRC-07
B.5.2	Practitioner		A&A-04
B.5.3	Promoter		HRS-13
B.5.4			A&A-04
B.5.5	Performer		GRC-07
B.5.6			HRS-13
B.5.7	Advocate		A&A-01 A&A-04
B.5.8			A&A-04 A&A-06
B.5.9			

Cross-mapping between Cyber Trust and CCMv4

Cyber Trust			CCMv4 Controls
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.6	Domain: Audit		
B.6.1	Supporter	Domain is not assessable for this tier	
B.6.2	Practitioner	Domain is not assessable for this tier	
B.6.3	Promoter	Domain is not assessable for this tier	
B.6.4	Performer		A&A-01 A&A-05
B.6.5			A&A-03
B.6.6			A&A-06
B.6.7	Advocate		A&A-05
B.6.8			A&A-06
B.7	Domain: Training and awareness		
B.7.1	Supporter		HRS-11 HRS-12
B.7.2	Practitioner		IAM-02 IAM-15 UEM-01 SEF-07 DSP-01 HRS-04 HRS-11 HRS-12
B.7.3			HRS-11 HRS-13
B.7.4	Promoter		
B.7.5			
B.7.6	Performer		
B.7.7			HRS-11
B.7.8			
B.7.9	Advocate		HRS-11
B.7.10			
B.7.11			HRS-13
B.8	Domain: Asset management		
B.8.1	Supporter		UEM-04 DCS-01 DCS-05 DCS-06 CCC-04 DSP-02

Cross-mapping between Cyber Trust and CCMv4

Cyber Trust			CCMv4 Controls
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.8.2	Practitioner		DSP-02 UEM-04 DCS-06
B.8.3	Promoter		DCS-01 HRS-02
B.8.4			DCS-05
B.8.5			HRS-09
B.8.6	Performer		DCS-06
B.8.7			HRS-02
B.8.8	Advocate		DCS-06
B.8.9			DCS-06
B.8.10			
B.9	Domain: Data protection and privacy		
B.9.1	Supporter		DSP-01 DSP-03 DSP-17 DSP-19 UEM-11
B.9.2			SEF-07
B.9.3			STA-03 STA-09
B.9.4	Practitioner		DSP-06
B.9.5	Promoter		DSP-01 DSP-04
B.9.6			DSP-05
B.9.7			DSP-01 DSP-04
B.9.8	Performer		DSP-17
B.9.9			DSP-06 HRS-09
B.9.10			CEK-04
B.9.11	Advocate		CEK-01 CEK-03 CEK-05
B.9.12			IVS-01 IVS-03
B.9.13			DSP-01
B.10	Domain: Backups		
B.10.1	Supporter		BCR-08

Cross-mapping between Cyber Trust and CCMv4

Cyber Trust			CCMv4 Controls
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.10.2	Practitioner		BCR-08
B.10.3			
B.10.4	Promoter		
B.10.5			BCR-08
B.10.6	Performer		BCR-08
B.10.7			BCR-08 HRS-09
B.10.8	Advocate		
B.10.9			
B.10.10			BCR-08
B.11	Domain: Bring Your Own Device (BYOD)		
B.11.1	Supporter	Domain is not assessable for this tier	
B.11.2	Practitioner	Domain is not assessable for this tier	
B.11.3	Promoter	Domain is not assessable for this tier	
B.11.4	Performer		UEM-01
B.11.5	Advocate		UEM-05
B.11.6			UEM-04
B.11.7			UEM-01 UEM-11
B.12	Domain: System security		
B.12.1	Supporter		TVM-01 TVM-03 CCC-01 CCC-03 CCC-06 DSP-07 IVS-03
B.12.2	Practitioner		LOG-07 UEM-06 AIS-07 UEM-03 CCC-02
B.12.3			AIS-07 CCC-09 TVM-01
B.12.4	Promoter		CCC-06
B.12.5			LOG-01 LOG-02

Cross-mapping between Cyber Trust and CCMv4

Cyber Trust			CCMv4 Controls
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.12.6			AIS-05 AIS-07
B.12.7	Performer		HRS-09 TVM-01 CCC-01 LOG-01
B.12.8			CCC-01
B.12.9			LOG-01 LOG-02
B.12.10			TVM-01 AIS-07
B.12.11	Advocate		CCC-03
B.12.12			CCC-02 CCC-06
B.12.13			CCC-03
B.13	Domain: Anti-virus/Anti-malware		
B.13.1	Supporter		TVM-02 UEM-09 UEM-10 IVS-09 UEM-02 SEF-07
B.13.2	Practitioner		UEM-10
B.13.3			TVM-02 UEM-09
B.13.4			IVS-09
B.13.5			
B.13.6	Promoter		
B.13.7	Performer		HRS-09 TVM-02
B.13.8	Advocate		SEF-01 SEF-08
B.13.9			
B.13.10			TVM-04
B.14	Domain: Secure Software Development Life Cycle (SDLC)		
B.14.1	Supporter	Domain is not assessable for this tier	
B.14.2	Practitioner	Domain is not assessable for this tier	
B.14.3	Promoter	Domain is not assessable for this tier	
B.14.4	Performer	Domain is not assessable for this tier	

Cross-mapping between Cyber Trust and CCMv4

Cyber Trust			CCMv4 Controls
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.14.5	Advocate		AIS-01 AIS-04
B.14.6			TVM-05 AIS-02
B.14.7			CCC-01 CCC-03 CCC-09
B.14.8			CCC-02 AIS-05 TVM-06 TVM-07
B.15	Domain: Access control		
B.15.1	Supporter		IAM-01 IAM-02 IAM-03 IAM-05 IAM-06 IAM-07 IAM-10 IAM-14 IAM-15 IAM-16 LOG-08 STA-12 HRS-10 DCS-03 DCS-09
B.15.2	Practitioner		IAM-03 IAM-08
B.15.3			IAM-03 IAM-08
B.15.4	Promoter		IAM-08
B.15.5			IAM-05
B.15.6			IAM-01 IAM-02 IAM-09 IAM-14 IAM-16
B.15.7	Performer		IAM-02
B.15.8			IAM-01
B.15.9			HRS-04
B.15.10	Advocate		SEF-07

Cross-mapping between Cyber Trust and CCMv4

Cyber Trust			CCMv4 Controls
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.15.11			IAM-09 IAM-10 IAM-11
B.16	Domain: Cyber threat management		
B.16.1	Supporter	Domain is not assessable for this tier	
B.16.2	Practitioner	Domain is not assessable for this tier	
B.16.3	Promoter	Domain is not assessable for this tier	
B.16.4	Performer		LOG-01 LOG-03
B.16.5			LOG-03 LOG-05 HRS-09
B.16.6			LOG-03 LOG-05
B.16.7			LOG-05 LOG-13
B.16.8			SEF-01 SEF-03
B.16.9	Advocate		LOG-05
B.16.10			LOG-13 SEF-07
B.16.11			LOG-07 TVM-04
B.17	Domain: Third-party risk and oversight		
B.17.1	Supporter	Domain is not assessable for this tier	
B.17.2	Practitioner	Domain is not assessable for this tier	
B.17.3	Promoter	Domain is not assessable for this tier	
B.17.4	Performer	Domain is not assessable for this tier	
B.17.5	Advocate		STA-09
B.17.6			STA-01 STA-02 STA-03 STA-04 STA-05 STA-06 STA-12
B.17.7			STA-12 STA-13
B.17.8			STA-13 STA-14

Cross-mapping between Cyber Trust and CCMv4

Cyber Trust			CCMv4 Controls
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.17.9			STA-08 STA-14
B.18	Domain: Vulnerability assessment		
B.18.1	Supporter	Domain is not assessable for this tier	
B.18.2	Practitioner	Domain is not assessable for this tier	
B.18.3	Promoter		TVM-01
B.18.4			TVM-07
B.18.5	Performer		HRS-09 TVM-01
B.18.6			TVM-03
B.18.7			TVM-09
B.18.8	Advocate		TVM-06
B.18.9			TVM-06
B.18.10			TVM-10
B.18.11			TVM-10
B.19	Domain: Physical/environmental security		
B.19.1	Supporter	Domain is not assessable for this tier	
B.19.2	Practitioner		DCS-03 DCS-15 IVS-08
B.19.3			DCS-01 DCS-02 DCS-03 DCS-04 DCS-05 DCS-06 DCS-07 DCS-08 DCS-09 DCS-10 DCS-12 DCS-13 DSP-16 DSP-19
B.19.4			DCS-07
B.19.5	Promoter		DCS-09 LOG-12
B.19.6			DCS-10
B.19.7			DCS-04
B.19.8	Performer		DCS-09

Cross-mapping between Cyber Trust and CCMv4

Cyber Trust			CCMv4 Controls
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.19.9			HRS-09 DCS-15
B.19.10			DCS-01 DCS-02 DCS-03 DCS-04
B.19.11	Advocate		-
B.19.12			DCA-01 DCA-02 DCA-03 DCA-04
B.20	Domain: Network security		
B.20.1	Supporter	Domain is not assessable for this tier	
B.20.2	Practitioner		IVS-03
B.20.3			IVS-09
B.20.4			IVS-07
B.20.5	Promoter		IVS-03 IVS-07
B.20.6			IVS-06 IVS-05
B.20.7	Performer		IVS-04
B.20.8			HRS-09 IVS-01
B.20.9			IVS-09
B.20.10	Advocate		IVS-09
B.20.11			IVS-09
B.21	Domain: Incident response		
B.21.1	Supporter		SEF-02 SEF-03
B.21.2	Practitioner		SEF-02 SEF-03 SEF-04
B.21.3	Promoter		SEC-02
B.21.4			SEF-04
B.21.5	Performer		SEF-03
B.21.6			SEF-01 SEF-06
B.21.7	Advocate		
B.21.8			SEF-07

Cross-mapping between Cyber Trust and CCMv4

Cyber Trust			CCMv4 Controls
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.22	Domain: Business continuity/Disaster recovery		
B.22.1	Supporter	Domain is not assessable for this tier	
B.22.2	Practitioner		BCR-11
B.22.3	Promoter		BCR-02
B.22.4			BCR-11
B.22.5	Performer		BCR-01
B.22.6			BCR-04 BCR-09
B.22.7			BCR-09
B.22.8			BCR-06 BCR-10
B.22.9	Advocate		BCR-04 BCR-09
B.22.10			BCR-06 BCR-07 BCR-10