CSA CYBERSECURITY CERTIFICATION

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Date of Publication: 09-10-2023 (Second edition)

A publication by

CSA SINGAPORE

SG CYBER SAFE | CYBER TRUST

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

This document contains the mapping between the clauses in ISO/IEC 27001:2022 and the Cyber Trust mark developed by the Cyber Security Agency of Singapore (CSA).

ISO/IEC 27001:2022 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organisation. ISO standards are internationally agreed by experts, and it is estimated there are over 286 ISO/IEC 27001 certificates issued to Singapore[1].

Organisations that are certified in ISO/IEC 27001:2022 and wish to assess this against Cyber Trust mark may refer to the following mapping:

a) Annex I maps the mandatory clauses (i.e. clauses 4 – 10) in ISO/IEC 27001:2022 to the cybersecurity preparedness domains in Cyber Trust mark; and

b) Annex II maps the Annex A information security controls reference clauses in ISO/IEC 27001:2022 to the cybersecurity preparedness domains in Cyber Trust mark.

Organisations that are certified in Cyber Trust mark and wish to assess this against ISO/IEC 27001:2022 may refer to the mapping in Annex III, which maps the cybersecurity preparedness statements in Cyber Trust mark to ISO/IEC 27001:2022.

[1] Source – ISO Survey 2022

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Figure 1 and Table 1 show the mapping of clauses in Cyber Trust to a subset of the mandatory clauses (i.e. clauses 4 – 10) in ISO/IEC 27001:2022.

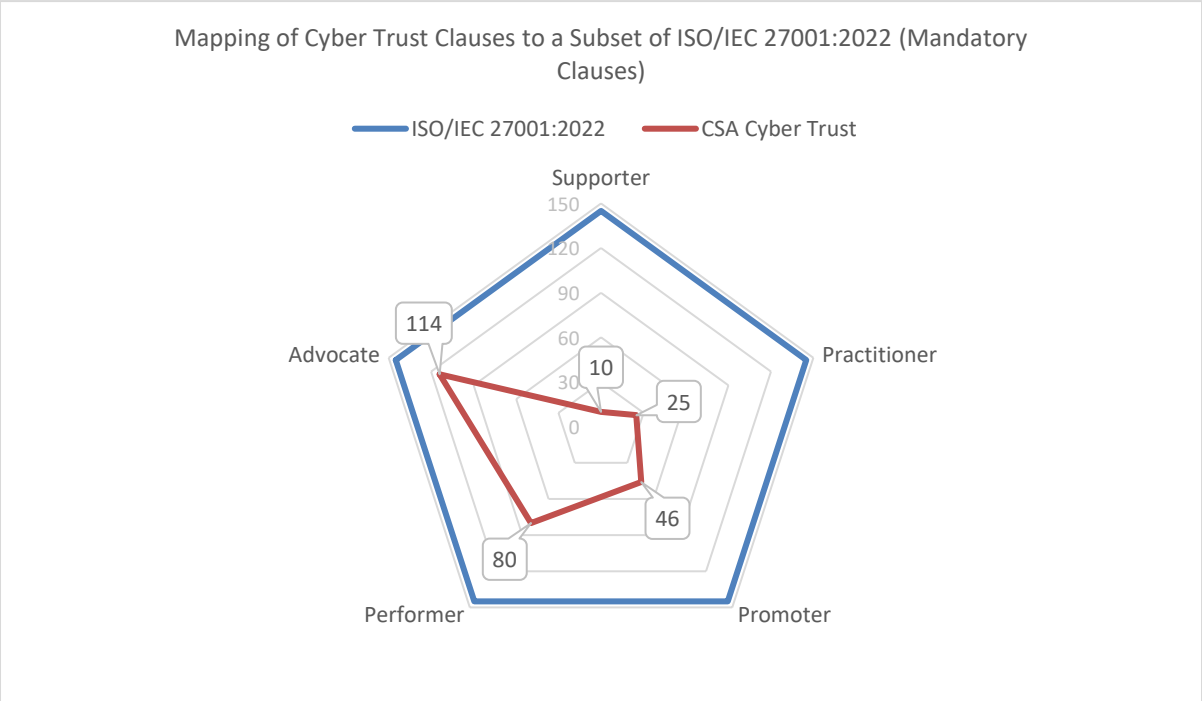

Figure 1 – Mapping of Cyber Trust clauses to subset of ISO/IEC 27001:2022 (Mandatory Clauses)

	ISO/IEC 27001:2022 (Mandatory Clauses)	Cyber Trust Clauses Mapped to ISO/IEC 27001:2022				
		Supporter	Practitioner	Promoter	Performer	Advocate
# of clauses	145	10	25	46	80	114
Percentage	100%	6.9%	17.2%	31.7%	55.2%	78.6%

Table 1 – Mapping of Cyber Trust clauses to subset of ISO/IEC 27001:2022 (Mandatory Clauses)

There are a total of 145 requirements in the mandatory clauses (i.e. clauses 4 – 10) of ISO/IEC 27001:2022.

The clauses in the “Advocate” tier of Cyber Trust mark map to 114 of these 145 requirements in the mandatory clauses of ISO/IEC 27001:2022. Cyber Trust mark is designed such that to meet a (higher) tier, the clauses in the lower tiers would also be met. For this reason, at the “Advocate” tier, the 114 clauses would include those in the lower tiers, i.e. “Performer”, “Promoter”, “Practitioner” and “Supporter”.

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Figure 2 and Table 2 show the mapping of clauses in Cyber Trust to a subset of the Annex A clauses in ISO/IEC 27001:2022.

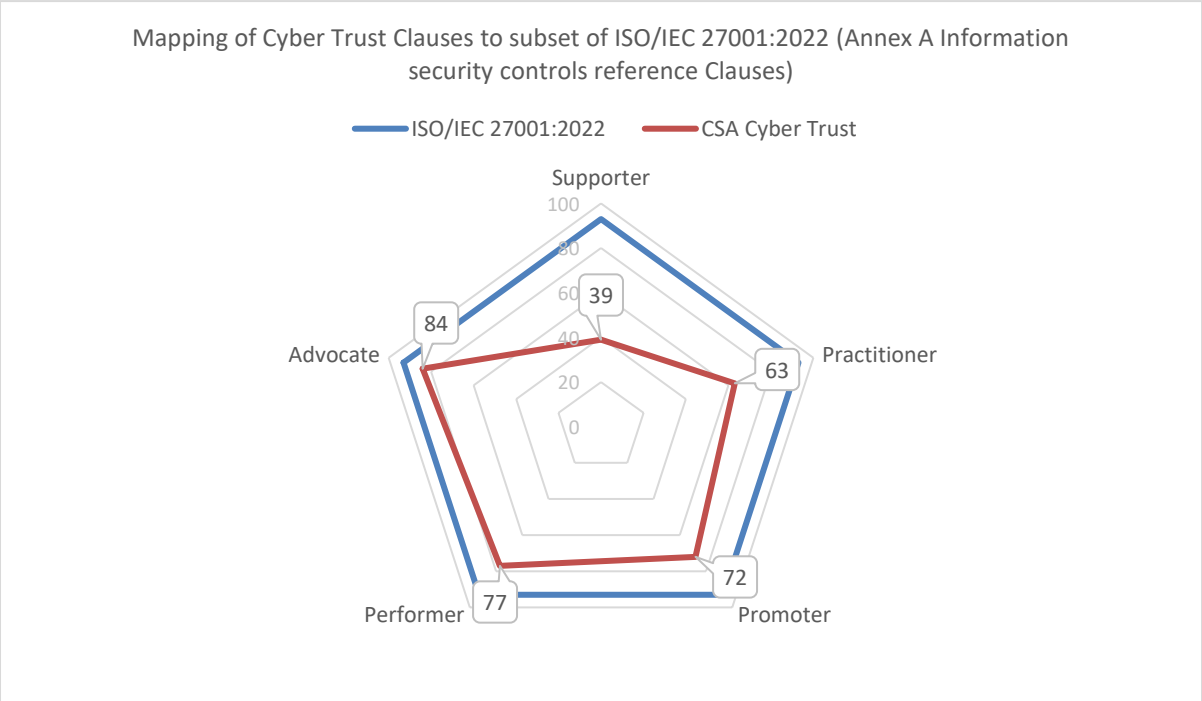

Figure 2 – Mapping of Cyber Trust clauses to subset of ISO/IEC 27001:2022 (Annex A Clauses)

	ISO/IEC 27001:2022 (Annex A Information security controls reference clauses)	Cyber Trust Clauses Mapped to ISO/IEC 27001:2022				
		Supporter	Practitioner	Promoter	Performer	Advocate
# of clauses	93	39	63	72	77	84
Percentage	100%	41.9%	67.7%	77.4%	82.8%	90.3%

Table 2 – Mapping of Cyber Trust clauses to subset of ISO/IEC 27001:2022 (Annex A Clauses)

There are a total of 93 information security controls reference clauses in Annex A of ISO/IEC 27001:2022. These are not mandatory and serve as a reference for organisations to consider their applicability in the context of their business.

The clauses in the “Advocate” tier of Cyber Trust mark map to 84 of these 93 information security controls reference clauses in Annex A of ISO/IEC 27001:2022. Cyber Trust mark is designed such that to meet a (higher) tier, the clauses in the lower tiers would also be met. For this reason, at the “Advocate” tier, the 84 clauses would include those in the lower tiers, i.e. “Performer”, “Promoter”, “Practitioner” and “Supporter”.

Annex I

Mapping of ISO/IEC 27001:2022 (Mandatory Clauses) to Cyber Trust mark

Clause	ISO/IEC 27001:2022 (Mandatory Clauses)	Cyber Trust *Note: An asterisk (*) indicates that the Cyber Trust clause **does not fully map** to the ISO/IEC clause*				
		Supporter	**Practitioner**	**Promoter**	**Performer**	**Advocate**
4	Context of the Organization					
4.1	Understanding the Organization and its context					
4.1 para 1						B.4.5
4.2	Understanding the needs and expectations of interested parties					
4.2 para 1a		B.5.1		B.1.3		B.4.5
4.2 para 1b		B.5.1		B.1.3		B.4.5
4.2 para 1c		B.5.1		B.1.3		B.4.5
4.3	Determining the scope of the information security management system					
4.3 para 1						
4.3 para 2a						B.4.5
4.3 para 2b						B.4.5
4.3 para 2c						B.4.5
4.3 para 3						
4.4	Information security management system					
4.4 para 1						B.4.6
5	Leadership					
5.1	Leadership and commitment					

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Mandatory Clauses)	Cyber Trust *Note: An asterisk (*) indicates that the Cyber Trust clause **does not fully map** to the ISO/IEC clause*				
		Supporter	**Practitioner**	**Promoter**	**Performer**	**Advocate**
5.1 para 1a					B.1.5	B.1.7 B.3.10 B.4.9
5.1 para 1b					B.1.5	B.1.7 B.3.10 B.4.9
5.1 para 1c					B.1.5	B.1.7
5.1 para 1d				B.1.3		B.1.7
5.1 para 1e					B.1.6	B.1.7 B.4.9
5.1 para 1f					B.1.5	B.1.7
5.1 para 1g					B.1.6	B.1.7
5.1 para 1h					B.1.5	B.1.7
5.2	Policy					
5.2 para 1a				B.8.3 B.9.5 B.9.7	B.2.4 B.3.7 B.9.8 B.10.6 B.11.4 B.12.8 B.12.9 B.12.10 B.19.8	B.2.8 B.8.8 B.9.11 B.9.12 B.9.13 B.10.9 B.10.10 B.11.7 B.12.12 B.12.13 B.21.8
5.2 para 1b				B.2.3 B.8.3 B.9.5 B.9.7	B.2.4 B.2.6 B.3.7 B.9.8 B.10.6 B.11.4 B.12.8 B.12.9 B.12.10	B.2.8 B.8.8 B.9.11 B.9.12 B.9.13 B.10.9 B.10.10 B.11.7 B.12.12 B.12.13 B.21.8
5.2 para 1c				B.8.3 B.9.5 B.9.7	B.2.4 B.3.7 B.9.8 B.10.6 B.11.4 B.12.8	B.2.8 B.8.8 B.9.11 B.9.12 B.9.13 B.10.9 B.10.10 B.11.7

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Mandatory Clauses)	Cyber Trust *Note: An asterisk (*) indicates that the Cyber Trust clause **does not fully map** to the ISO/IEC clause*				
		Supporter	**Practitioner**	**Promoter**	**Performer**	**Advocate**
					B.12.9 B.12.10	B.12.12 B.12.13 B.21.8
5.2 para 1d					B.2.4 B.3.7	B.2.8
5.2 para 2e					B.2.4 B.3.7	B.2.8
5.2 para 2f				B.2.3	B.2.6	
5.2 para 2g				B.2.3	B.2.6	
5.3	Organizational roles, responsibilities, and authorities					
5.3 para 1				B.8.5	B.1.4 B.3.8 B.5.6 B.9.9 B.10.7 B.12.7 B.13.7 B.19.9 B.20.8	B.3.11 B.4.8 B.5.9 B.16.10
5.3 para 2a				B.8.5	B.1.4 B.3.8 B.5.6 B.9.9 B.10.7 B.12.7 B.13.7 B.19.9 B.20.8	
5.3 para 2b				B.8.5	B.1.4 B.9.9 B.10.7 B.12.7 B.13.7 B.19.9 B.20.8	B.3.11 B.4.8 B.5.9 B.16.10
6	Planning					
6.1	Actions to address risks and opportunities					
6.1.1	General					

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Mandatory Clauses)	Cyber Trust *Note: An asterisk (*) indicates that the Cyber Trust clause **does not fully map** to the ISO/IEC clause*				
		Supporter	**Practitioner**	**Promoter**	**Performer**	**Advocate**
6.1.1 para 1			B.3.3* B.5.2*			B.8.10*
6.1.1 para 1a			B.3.3 B.5.2			
6.1.1 para 1b			B.3.3 B.5.2			
6.1.1 para 1c						
6.1.1 para 2d			B.3.3 B.5.2			
6.1.1 para 2e1			B.3.3 B.5.2			B.8.10
6.1.1 para 2e2						
6.1.2	Information Security risk assessment					
6.1.2 para 1a1					B.3.9	
6.1.2 para 1a2						
6.1.2 para 1b						
6.1.2 para 1c1		B.3.1	B.3.4 B.19.2	B.3.5	B.3.7 B.19.9	
6.1.2 para 1c2			B.19.2		B.19.9	
6.1.2 para 1d1		B.3.2		B.3.5	B.3.7 B.19.10	B.19.12
6.1.2 para 1d2		B.3.2		B.3.5	B.3.7 B.19.10	B.19.12
6.1.2 para 1d3		B.3.2		B.3.5	B.3.7 B.19.10	B.19.12
6.1.2 para 1e1		B.3.2		B.3.5	B.3.7 B.19.10	B.19.12
6.1.2 para 1e2		B.3.2			B.19.10	B.19.12
6.1.2 para 2			B.3.4			
6.1.3	Information security risk treatment					
6.1.3 para 1a			B.5.2 B.19.2		B.18.7 B.19.9	B.18.8 B.18.9 B.18.10 B.18.11

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Mandatory Clauses)	Cyber Trust *Note: An asterisk (*) indicates that the Cyber Trust clause **does not fully map** to the ISO/IEC clause*				
		Supporter	**Practitioner**	**Promoter**	**Performer**	**Advocate**
6.1.3 para 1b			B.5.2		B.18.7	B.18.8 B.18.9 B.18.10 B.18.11
6.1.3 para 1c						
6.1.3 para 1d						
6.1.3 para 1e			B.5.2		B.18.7	B.18.8 B.18.9 B.18.10 B.18.11
6.1.3 para 1f				B.3.6		
6.1.3 para 2						
6.2	Information security objectives and planning to achieve them					
6.2 para 1				B.3.6*	B.1.6*	B.3.11*
6.2 para 2a					B.1.6	
6.2 para 2b						
6.2 para 2c						
6.2 para 2d					B.1.6	B.3.11
6.2 para 2e						B.3.11
6.2 para 2f				B.3.6	B.1.6	
6.2 para 2g					B.1.6	
6.2 para 3						
6.2 para 4h				B.3.6	B.1.6	
6.2 para 4i					B.1.6	
6.2 para 4j				B.3.6	B.1.6	
6.2 para 4k				B.3.6	B.1.6	
6.2 para 4l						
6.3	Planning of changes					
6.3 para 1				B.3.6	B.1.6	B.1.7 B.1.8 B.2.7 B.4.8 B.4.9

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Mandatory Clauses)	Cyber Trust *Note: An asterisk (*) indicates that the Cyber Trust clause **does not fully map** to the ISO/IEC clause*				
		Supporter	**Practitioner**	**Promoter**	**Performer**	**Advocate**
7	Support					
7.1	Resources					
7.1 para 1				B.7.5		B.4.7 B.7.11
7.2	Competence					
7.2 para 1a					B.7.8	
7.2 para 1b				B.21.4	B.7.8	
7.2 para 1c					B.7.8	B.7.10
7.2 para 1d						
7.3	Awareness					
7.3 para 1a		A.1.4 (a) B.7.1	A.1.4 (e) B.7.2	B.2.3		
7.3 para 1b			A.1.4 (d) B.7.2	B.2.3 B.21.4		
7.3 para 1c						
7.4	Communication					
7.4 para 1				B.5.3	B.2.6 B.19.8	B.1.8 B.3.11 B.9.13 B.10.9 B.13.9 B.16.10 B.17.9 B.19.11 B.21.8 B.22.9
7.4 para 1a				B.5.3	B.2.6 B.19.8	B.1.8 B.3.11 B.9.13 B.10.9 B.13.9 B.16.10 B.17.9 B.19.11 B.21.8 B.22.9
7.4 para 1b					B.2.6 B.19.8	B.1.8 B.3.11 B.9.13 B.10.9 B.13.9

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Mandatory Clauses)	Cyber Trust *Note: An asterisk (*) indicates that the Cyber Trust clause **does not fully map** to the ISO/IEC clause*				
		Supporter	**Practitioner**	**Promoter**	**Performer**	**Advocate**
						B.16.10 B.17.9 B.19.11 B.21.8 B.22.9
7.4 para 1c				B.5.3	B.2.6 B.19.8	B.1.8 B.3.11 B.9.13 B.10.9 B.13.9 B.16.10 B.17.9 B.19.11 B.21.8 B.22.9
7.4 para 1d					B.2.6 B.19.8	B.1.8 B.3.11 B.9.13 B.10.9 B.13.9 B.16.10 B.17.9 B.19.11 B.21.8 B.22.9
7.5	Documented information					
7.5.1	General					
7.5.1 para 1a						
7.5.1 para 1b						
7.5.2	Creating and updating					
7.5.2 para 1a						
7.5.2 para 1b						
7.5.2 para 1c						B.2.7 B.4.9
7.5.3	Control of documented information					
7.5.3 para 1						
7.5.3 para 1a						
7.5.3 para 1b						

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Mandatory Clauses)	Cyber Trust *Note: An asterisk (*) indicates that the Cyber Trust clause **does not fully map** to the ISO/IEC clause*				
		Supporter	**Practitioner**	**Promoter**	**Performer**	**Advocate**
7.5.3 para 2c						
7.5.3 para 2d						
7.5.3 para 2e						
7.5.3 para 2f						
7.5.3 para 3						
8	Operation					
8.1	Operational planning and control					
8.1 para 1						B.4.5 B.4.6
8.1 para 2						B.4.5 B.4.6
8.1 para 3						B.4.5 B.4.6
8.1 para 4						B.4.5 B.4.6
8.2	Information security risk assessment					
8.2 para 1			B.3.4			B.3.12
8.2 para 2			B.3.4			B.3.12
8.3	Information security risk treatment					
8.3 para 1			B.3.3	B.3.6		
8.3 para 2			B.3.3	B.3.6		
9	Performance evaluation					
9.1	Monitoring, measurement, analysis and evaluation					
9.1 para 1a						B.2.8 B.4.8 B.4.9 B.16.10
9.1 para 1b						B.2.8 B.4.8

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Mandatory Clauses)	Cyber Trust *Note: An asterisk (*) indicates that the Cyber Trust clause **does not fully map** to the ISO/IEC clause*				
		Supporter	**Practitioner**	**Promoter**	**Performer**	**Advocate**
						B.4.9 B.16.10
9.1 para 1c						B.4.8 B.4.9 B.16.10
9.1 para 1d						B.4.8 B.4.9 B.16.10
9.1 para 1e						B.4.8 B.4.9 B.16.10
9.1 para 1f						B.4.8 B.4.9 B.16.10
9.1 para 2						
9.1 para 3						B.2.8 B.4.8 B.4.9 B.16.10
9.2	Internal audit					
9.2.1	General					
9.2.1 para 1						B.2.8
9.2.1 para 1a1						B.2.8
9.2.1 para 1a2						B.2.8
9.2.1 para 1b						B.2.8
9.2.2	Internal audit programme					
9.2.2 para 1					B.6.4	
9.2.2 para 2					B.6.4	
9.2.2 para 3a					B.6.4	
9.2.2 para 3b					B.6.5	
9.2.2 para 3c						B.6.8
9.2.2 para 4						
9.3	Management review					
9.3.1	General					
9.3.1 para 1					B.1.6	B.1.7 B.1.8

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Mandatory Clauses)	Cyber Trust *Note: An asterisk (*) indicates that the Cyber Trust clause **does not fully map** to the ISO/IEC clause*				
		Supporter	**Practitioner**	**Promoter**	**Performer**	**Advocate**
						B.2.7 B.4.9 B.6.7
9.3.2	Management review inputs					
9.3.2 para 1a					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9
9.3.3 para 1b					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9
9.3.2 para 1c					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9
9.3.2 para 1d1					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9
9.3.2 para 1d2					B.1.6	B.1.7 B.1.8 B.4.9
9.3.2 para 1d3					B.1.6	B.1.7 B.1.8 B.4.9 B.6.7
9.3.2 para 1d4					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9
9.3.2 para 2e					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9
9.3.2 para 2f					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9
9.3.2 para 2g					B.1.6	B.1.7 B.1.8

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Mandatory Clauses)	Cyber Trust *Note: An asterisk (*) indicates that the Cyber Trust clause **does not fully map** to the ISO/IEC clause*				
		Supporter	**Practitioner**	**Promoter**	**Performer**	**Advocate**
						B.2.7 B.4.9
9.3.3	Management review results					
9.3.3 para 1						
9.3.3 para 2						
10	Improvement					
10.1	Continual Improvement					
10.1 para 1						B.2.7
10.2	Nonconformity and corrective action					
10.2 para 1a1					B.6.6	B.2.7 B.2.9 B.3.12 B.5.8 B.6.8 B.12.13
10.2 para 1a2						B.2.7 B.2.9 B.3.12 B.5.8 B.6.8 B.12.13
10.2 para 1b1						B.2.7 B.2.9 B.3.12 B.5.8 B.6.8 B.12.13
10.2 para 1b2						B.2.7
10.2 para 1b3						B.2.7
10.2 para 1c						B.2.7 B.2.9 B.3.12 B.5.8 B.6.8 B.12.13
10.2 para 1d						B.2.7 B.2.9 B.5.8

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Mandatory Clauses)	Cyber Trust *Note: An asterisk (*) indicates that the Cyber Trust clause **does not fully map** to the ISO/IEC clause*				
		Supporter	**Practitioner**	**Promoter**	**Performer**	**Advocate**
						B.6.8 B.12.13
10.2 para 1e						B.2.7 B.2.9 B.3.12 B.5.8 B.6.8 B.12.13
10.2 para 2						B.2.7 B.5.8 B.6.8
10.2 para 3f						B.2.7 B.5.8 B.6.8
10.2 para 3g						B.2.7 B.5.8 B.6.8

Annex II

Mapping of ISO/IEC 27001:2022 (Annex A Information security controls reference) to Cyber Trust mark

Clause	ISO/IEC 27001:2022 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
5	Organizational controls					
5.1	Policies for information security		A.4.4 (h) A.9.4 (d) B.13.2 B.21.2		B.1.5 B.1.6 B.2.4 B.2.5	B.1.7
5.2	Information security roles and responsibilities	A.9.4 (a) B.9.3 B.21.1	B.15.3	B.1.3 B.8.5 B.15.5	B.1.4 B.3.8 B.5.6 B.6.4 B.9.9 B.10.7 B.12.7 B.13.7 B.16.5 B.18.5 B.19.9 B.20.8 B.22.5	B.15.11
5.3	Segregation of duties			B.15.5		
5.4	Management responsibilities			B.5.3		
5.5	Contact with authorities	A.9.4 (a) B.21.1 B.9.2		B.1.3 B.21.4	B.16.5	
5.6	Contact with special interest groups					B.1.7 B.13.8 B.16.11
5.7	Threat intelligence				B.16.4 B.16.6 B.16.7	B.13.8 B.16.9 B.16.11
5.8	Information security in project management	A.6.4 (a), (b), (c), (d), (e) B.12.1	A.6.4 (g), (h) A.7.4 (d) B.12.2			
5.9	Inventory of information and other associated assets	A.2.4 (a), (d) B.8.1	A.2.4 (b), (c), (e), (f) B.8.2 B.22.2		B.8.6	B.8.8 B.8.9

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
5.10	Acceptable use of information and other associated assets	A.2.4 (g), (h), (i), (j), (k) A.3.4 (c), (d) B.8.1 B.9.1 B.9.3	A.1.4 (c) B.7.2	B.8.3 B.8.4 B.9.5	B.8.7	
5.11	Return of assets					
5.12	Classification of information			B.8.4 B.9.5		
5.13	Labelling of information	A.3.4 (a) B.9.1	A.3.4 (b) B.9.4	B.8.4		
5.14	Information transfer			B.9.6	B.9.8	B.9.12
5.15	Access control	A.5.4 (a) B.15.1	B.19.3	B.15.4 B.15.6 B.19.7	B.15.8 B.15.9 B.19.10	B.19.12
5.16	Identity management	A.5.4 (b) B.15.1	B.15.3	B.15.4 B.15.5		
5.17	Authentication information	A.5.4 (l), (n) B.15.1	A.1.4 (c) A.5.4 (p) B.7.2 B.15.2	B.15.6	B.15.7	B.15.11
5.18	Access rights	A.5.4 (c), (e), (g) B.15.1	A.5.4 (j), (k) B.15.2 B.15.3	B.15.4 B.15.5	B.15.8	B.15.10
5.19	Information security in supplier relationships	A.5.4 (h) B.15.1				B.17.5 B.17.6 B.17.7 B.17.8 B.17.9
5.20	Addressing information security within supplier agreements	B.9.3				B.17.5 B.17.6 B.17.7
5.21	Managing information security in the information and communication technology (ICT) supply chain					B.17.9
5.22	Monitoring, review and change management of supplier services					B.17.5 B.17.8

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
5.23	Information security for use of cloud services	A.2.4 (d) A.8.4 (e) B.8.1 B.9.3 B.10.1	A.4.4 (e), (g) A.6.4 (h) A.7.4 (d) B.12.2 B.13.2			B.17.5 B.17.6 B.17.7 B.17.8 B.17.9
5.24	Information security incident management planning and preparation	A.9.4 (a), (b) B.9.2 B.21.1	A.9.4 (d) B.13.5 B.21.2	B.21.3 B.21.4	B.16.5	B.21.8
5.25	Assessment and decision on information security events				B.21.6	B.13.10 B.16.9 B.16.11
5.26	Response to information security incidents		B.13.5	B.21.3	B.21.5 B.21.6	B.21.7 B.21.8
5.27	Learning from information security incidents		A.9.4 (c) B.21.2		B.21.5	B.21.7
5.28	Collection of evidence				B.16.6	B.13.10 B.21.8
5.29	Information security during disruption		B.22.2	B.22.3 B.22.4	B.22.5 B.22.6 B.22.7 B.22.8	B.22.9 B.22.10
5.30	ICT readiness for business continuity		B.22.2	B.22.3 B.22.4	B.22.5 B.22.6 B.22.7 B.22.8	B.22.9 B.22.10
5.31	Legal, statutory, regulatory and contractual requirements	B.5.1		B.5.4	B.5.5	
5.32	Intellectual property rights			B.5.4	B.5.5	
5.33	Protection of records			B.5.4 B.9.6 B.9.7	B.5.5 B.9.8	
5.34	Privacy and protection of personal identifiable information (PII)	B.5.1		B.5.4	B.5.5	
5.35	Independent review of information security		B.5.2			B.5.7 B.22.10

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
5.36	Compliance with policies, rules and standards for information security		B.5.2 B.20.4	B.12.4 B.18.4	B.12.8	B.2.7 B.2.8 B.2.9 B.5.7 B.11.6 B.12.11 B.12.12 B.12.13 B.13.9 B.18.9
5.37	Documented operating procedures	A.1.4 (b) B.7.1				
6	People controls					
6.1	Screening					
6.2	Terms and conditions of employment					
6.3	Information security awareness, education and training	A.1.4 (a) B.7.1	A.1.4 (d), (e) B.7.2 B.7.3	B.2.3 B.5.3 B.7.4 B.21.4	B.7.6 B.7.7	B.7.9 B.7.11
6.4	Disciplinary process	A.5.4 (h) B.15.1				
6.5	Responsibilities after termination or change of employment					
6.6	Confidentiality or non-disclosure agreements	A.5.4 (h) B.15.1				
6.7	Remote working		A.1.4 (c) B.7.2		B.15.9	
6.8	Information security event reporting	A.4.4 (l) B.9.2 B.13.1	A.1.4 (c) B.7.2		B.16.5 B.16.8	B.13.9 B.15.10 B.16.10 B.21.7 B.21.8
7	Physical controls					
7.1	Physical security perimeters		B.19.2 B.19.3 B.19.4	B.19.6		
7.2	Physical entry	A.5.4 (i) B.15.1	B.19.4	B.19.5	B.19.8 B.19.10	B.19.12
7.3	Securing offices, rooms and facilities	A.5.4 (i) B.15.1	B.19.3 B.19.4	B.19.6		

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
7.4	Physical security monitoring			B.19.6		
7.5	Protecting against physical and environmental threats		B.19.3			
7.6	Working in secure areas		A.1.4 (c) B.7.2			
7.7	Clear desk and clear screen		B.19.3			
7.8	Equipment siting and protection		B.19.3	B.19.7		
7.9	Security of assets off-premises		B.19.3			
7.10	Storage media	A.2.4 (a) A.2.4 (i) A.2.4 (j) A.3.4 (e) B.8.1 B.9.1	A.2.4 (m) B.8.2 B.19.3	B.8.3 B.19.7	B.8.7	
7.11	Supporting utilities		B.19.3			
7.12	Cabling security		B.19.3			
7.13	Equipment maintenance	A.2.4 (l) B.8.1	A.2.4 (m) B.8.2 B.22.2	B.22.4		
7.14	Secure disposal or re-use of equipment	A.2.4 (l) A.3.4 (e) B.8.1 B.9.1		B.19.7		
8	Technological controls					
8.1	User end point devices	A.4.4 (a) A.4.4 (f) B.13.1	A.4.4 (g) A.6.4 (h) B.12.2 B.13.2 B.19.3		B.11.4 B.15.9	B.11.5 B.11.6 B.11.7
8.2	Privileged access rights	A.5.4 (f) B.15.1		B.15.6		B.15.11
8.3	Information access restriction	A.5.4 (m) B.15.1		B.15.5	B.15.9	B.15.10 B.15.11
8.4	Access to source code					
8.5	Secure authentication		A.5.4 (o) B.15.2	B.15.6 B.20.5		B.14.5 B.15.11

Clause	ISO/IEC 27001:2022 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
8.6	Capacity management					
8.7	Protection against malware	A.4.4 (a), (b), (c), (d) B.13.1	A.1.4 (c) A.4.4 (e) B.7.2 B.13.2 B.13.3 B.13.4 B.13.5	B.13.6	B.13.7	B.13.9 B.13.10
8.8	Management of technical vulnerabilities	A.7.4 (a) B.12.1	A.7.4 (c), (d) B.5.2 B.12.2 B.12.3 B.20.4	B.12.4 B.12.6 B.18.3 B.18.4	B.12.10 B.18.5 B.18.6 B.18.7	B.5.7 B.12.11 B.12.13 B.13.9 B.18.8 B.18.9 B.18.10 B.18.11
8.9	Configuration management	A.6.4 (a), (b), (c), (d), (e) B.12.1	A.6.4 (g), (h) B.12.2	B.12.4	B.12.7 B.12.8	B.12.11 B.12.12 B.12.13
8.10	Information deletion	A.2.4 (l) B.8.1	A.2.4 (m) B.8.2			
8.11	Data masking					
8.12	Data leakage prevention	A.3.4 (c), (d) A.5.4 (d), (e), (g), (h) B.9.1 B.9.3 B.15.1	A.5.4 (k), (o) A.6.4 (h) B.12.2 B.15.2	B.9.6 B.15.5 B.15.6 B.20.5 B.20.6	B.9.8 B.9.9 B.9.10 B.15.8 B.15.9	B.9.11 B.9.12 B.11.7 B.15.11
8.13	Information backup	A.8.4 (a), (b), (e), (g), (h), (j) B.10.1	A.8.4 (c), (d), (f), (i), (k) B.10.2 B.10.3	B.10.4 B.10.5	B.10.6 B.10.7	B.10.8 B.10.10
8.14	Redundancy of information processing facilities		B.22.2	B.22.4		B.22.9
8.15	Logging		A.6.4 (f), (h) B.12.2	B.12.5	B.12.9 B.16.4 B.16.6 B.16.7	
8.16	Monitoring activities		A.6.4 (h) B.12.2		B.16.6 B.16.7 B.20.9	B.13.10

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Clause	ISO/IEC 27001:2022 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
8.17	Clock synchronization					
8.18	Use of privileged utility programs	A.5.4 (f) B.15.1				
8.19	Installation of software on operational systems	A.4.4 (j) B.13.1				B.12.11
8.20	Networks security	A.4.4 (f), (k) B.13.1	A.4.4 (g), (h), (i) B.13.2 B.20.2 B.20.3 B.20.4	B.12.4 B.20.5 B.20.6	B.20.7 B.20.8 B.20.9	B.20.10 B.20.11
8.21	Security of network services		B.20.2 B.20.3 B.20.4	B.20.5	B.20.7 B.20.9	B.20.10 B.20.11
8.22	Segregation of networks		A.6.4 (h) B.12.2	B.20.6		B.11.7
8.23	Web filtering		A.4.4 (e) B.13.2 B.13.4			
8.24	Use of cryptography				B.9.10	B.9.11
8.25	Secure development life cycle					B.14.5
8.26	Application security requirements	A.3.4 (c) A.4.4 (f), (k) A.6.4 (c) B.9.1 B.12.1 B.13.1		B.9.5 B.9.6 B.9.7	B.9.8 B.9.10	B.9.11 B.9.12 B.9.13 B.14.6 B.14.8
8.27	Secure system architecture and engineering principles					B.14.5 B.14.6
8.28	Secure coding					B.14.5 B.14.6
8.29	Security testing in development and acceptance			B.12.6		B.14.7 B.14.8
8.30	Outsourced development					B.17.5 B.17.8
8.31	Separation of development, test and production environments			B.13.6		B.14.6

Clause	ISO/IEC 27001:2022 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
8.32	Change management		A.7.4 (b) B.12.2 B.12.3	B.12.6		B.12.11 B.14.6 B.14.7 B.14.8
8.33	Test information					
8.34	Protection of information systems during audit testing				B.6.4 B.6.5 B.6.6	B.6.7

Annex III

Mapping of Cyber Trust mark to ISO/IEC 27001:2022

Cyber Trust			ISO/IEC 27001:2022 Clauses
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		4.2 para 1a, 1b, 1c 5.1 para 1d A5.2[2], A5.5
B.1.4	Performer		5.3 para 1, 2a, 2b A5.2
B.1.5			5.1 para 1a, 1b, 1c, 1f, 1h A5.1
B.1.6			5.1 para 1e, 1g 6.2 para 2a, 2d, 2f, 2g, 4h, 4i, 4j, 4k 6.3 para 1 9.3.1 para 1 9.3.2 para 1a, 1b, 1c, 1d1, 1d2, 1d3, 1d4, 2e, 2f, 2g A5.1
B.1.7	Advocate		5.1 para 1a, 1b, 1c, 1d, 1e, 1f, 1g, 1h 6.3 para 1 9.3.1 para 1 9.3.2 para 1a, 1b, 1c, 1d1, 1d2, 1d3, 1d4, 2e, 2f, 2g A5.1, A5.6
B.1.8			6.3 para 1 7.4 para 1, 1a, 1b, 1c, 1d 9.3.1 para 1 9.3.2 para 1a, 1b, 1c, 1d1, 1d2, 1d3, 1d4, 2e, 2f, 2g
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	

[2] "A" prefix refers to Annex A Clauses (Information security controls reference) of ISO/IEC 27001:2022.

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Cyber Trust			ISO/IEC 27001:2022 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.2.3	Promoter		5.2 para 1b, 2f, 2g 7.3 para 1a, 1b A6.3
B.2.4	Performer		5.2 para 1a, 1b, 1c, 1d, 2e A5.1
B.2.5			A5.1
B.2.6			5.2 para 1b, 2f, 2g 7.4 para 1, 1a, 1b, 1c, 1d
B.2.7	Advocate		6.3 para 1 7.5.2 para 1c 9.3.1 para 1 9.3.2 para 1a, 1b, 1c, 1d1, 1d4, 2e, 2f, 2g 10.1 para 1 10.2 para 1a1, 1a2, 1b1, 1b2, 1b3, 1c, 1d, 1e, 2, 3f, 3g A5.36
B.2.8			5.2 para 1a, 1b, 1c, 1d, 2e 9.1 para 1a, 1b, 3 9.2.1 para 1, 1a1, 1a2, 1b A5.36
B.2.9			10.2 para 1a1, 1a2, 1b1, 1c, 1d, 1e A5.36
B.3	Domain: Risk management		
B.3.1	Supporter		6.1.2 para 1c1
B.3.2			6.1.2 para 1d1, 1d2, 1d3, 1e1, 1e2
B.3.3	Practitioner		6.1.1 para 1a, 1b, 2d, 2e1 8.3 para 1, 2
B.3.4			6.1.2 para 1c1, 2 8.2 para 1, 2
B.3.5	Promoter		6.1.2 para 1c1, 1d1, 1d2, 1d3, 1e1
B.3.6			6.1.3 para 1f 6.2 para 2f, 4h, 4j, 4k 6.3 para 1 8.3 para 1, 2
B.3.7	Performer		5.2 para 1a, 1b, 1c, 1d, 2e 6.1.2 para 1c1, 1d1, 1d2, 1d3, 1e1

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Cyber Trust			ISO/IEC 27001:2022 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.3.8			5.3 para 1, 2a A5.2
B.3.9			6.1.2 para 1a1
B.3.10	Advocate		5.1 para 1a, 1b
B.3.11			5.3 para 1, 2b 6.2 para 2d, 2e 7.4 para 1, 1a, 1b, 1c, 1d
B.3.12			8.2 para 1, 2 10.2 para 1a1, 1a2, 1b1, 1c, 1e
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		4.1 para 1 4.2 para 1a, 1b, 1c 4.3 para 2a, 2b, 2c 8.1 para 1, 2, 3, 4
B.4.6			4.4 para 1 8.1 para 1, 2, 3, 4
B.4.7			7.1 para 1
B.4.8			5.3 para 1, 2b 6.3 para 1 9.1 para 1a, 1b, 1c, 1d, 1e, 1f, 3
B.4.9			5.1 para 1a, 1b, 1e 6.3 para 1 7.5.2 para 1c 9.1 para 1a, 1b, 1c, 1d, 1e, 1f, 3 9.3.1 para 1 9.3.2 para 1a, 1b, 1c, 1d1, 1d2, 1d3, 1d4, 2e, 2f, 2g
B.5	Domain: Compliance		
B.5.1	Supporter		4.2 para 1a, 1b, 1c A5.31, A5.34
B.5.2	Practitioner		6.1.1 para 1a, 1b, 2d, 2e1 6.1.3 para 1a, 1b, 1e A5.35, A5.36, A8.8
B.5.3	Promoter		7.4 para 1, 1a, 1c A5.4, A6.3

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Cyber Trust			ISO/IEC 27001:2022 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.5.4			A5.31, A5.32, A5.33, A5.34
B.5.5	Performer		A5.31, A5.32, A5.33, A5.34
B.5.6			5.3 para 1, 2a A5.2
B.5.7	Advocate		A5.35, A5.36, A8.8
B.5.8			10.2 para 1a1, 1a2, 1b1, 1c, 1d, 1e, 2, 3f, 3g
B.5.9			5.3 para 1, 2b
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		9.2.2 para 1, 2, 3a A5.2, A8.34
B.6.5			9.2.2 para 3b A8.34
B.6.6			10.2 para 1a1 A8.34
B.6.7	Advocate		9.3.1 para 1 9.3.2 para 1d3 A8.34
B.6.8			9.2.2 para 3c 10.2 para 1a1, 1a2, 1b1, 1c, 1d, 1e, 2, 3f, 3g
B.7	Domain: Training and awareness		
B.7.1	Supporter		7.3 para 1a A5.37, A6.3
B.7.2	Practitioner		7.3 para 1a, 1b A5.10, A5.17, A6.3, A6.7, A6.8, A7.6, A8.7
B.7.3			A6.3
B.7.4	Promoter		A6.3
B.7.5			7.1 para 1
B.7.6	Performer		A6.3
B.7.7			A6.3

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Cyber Trust			ISO/IEC 27001:2022 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.7.8			7.2 para 1a, 1b, 1c
B.7.9	Advocate		A6.3
B.7.10			7.2 para 1c
B.7.11			7.1 para 1 A6.3
B.8	Domain: Asset management		
B.8.1	Supporter		A5.9, A5.10, A5.23, A 7.10, A7.13, A7.14, A8.10
B.8.2	Practitioner		A5.9, A7.10, A7.13, A8.10
B.8.3	Promoter		5.2 para 1a, 1b, 1c A5.10, A7.10
B.8.4			A5.10, A5.12, A5.13
B.8.5			5.3 para 1, 2a, 2b A5.2
B.8.6	Performer		A5.9
B.8.7			A5.10, A7.10
B.8.8	Advocate		5.2 para 1a, 1b, 1c A5.9
B.8.9			A5.9
B.8.10			6.1.1 para 2e1
B.9	Domain: Data protection and privacy		
B.9.1	Supporter		A5.10, A5.13, A7.10, A7.14, A8.12, A8.26
B.9.2			A5.5, A5.24, A6.8
B.9.3			A5.2, A5.10, A5.20, A5.23, A8.12
B.9.4	Practitioner		A5.13
B.9.5	Promoter		5.2 para 1a, 1b, 1c A5.10, A5.12, A8.26
B.9.6			A5.14, A5.33, A8.12, A8.26
B.9.7			5.2 para 1a, 1b, 1c A5.33, A8.26
B.9.8	Performer		5.2 para 1a, 1b, 1c A5.14, A5.33, A8.12, A8.26

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Cyber Trust			ISO/IEC 27001:2022 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.9.9			5.3 para 1, 2a, 2b A5.2, A8.12
B.9.10			A8.12, A8.24, A8.26
B.9.11	Advocate		5.2 para 1a, 1b, 1c A8.12, A8.24, A8.26
B.9.12			5.2 para 1a, 1b, 1c A5.14, A8.12, A8.26
B.9.13			5.2 para 1a, 1b, 1c 7.4 para 1, 1a, 1b, 1c, 1d A8.26
B.10	Domain: Backups		
B.10.1	Supporter		A5.23, A8.13
B.10.2	Practitioner		A8.13
B.10.3			A8.13
B.10.4	Promoter		A8.13
B.10.5			A8.13
B.10.6	Performer		5.2 para 1a, 1b, 1c A8.13
B.10.7			5.3 para 1, 2a, 2b A5.2, A8.13
B.10.8	Advocate		A8.13
B.10.9			5.2 para 1a, 1b, 1c 7.4 para 1, 1a, 1b, 1c, 1d
B.10.10			5.2 para 1a, 1b, 1c A8.13
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		5.2 para 1a, 1b, 1c A8.1
B.11.5	Advocate		A8.1
B.11.6			A5.36, A8.1
B.11.7			5.2 para 1a, 1b, 1c

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Cyber Trust			ISO/IEC 27001:2022 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
			A8.1, A8.12, A8.22
B.12	Domain: System security		
B.12.1	Supporter		A5.8, A8.8, A8.9, A8.26
B.12.2	Practitioner		A5.8, A5.23, A8.1, A8.8, A8.9, A8.12, A8.15, A8.16, A8.22, A8.32
B.12.3			A8.8, A8.32
B.12.4	Promoter		A5.36, A8.8, A8.9, A8.20
B.12.5			A8.15
B.12.6			A8.8, A8.29, A8.32
B.12.7	Performer		5.3 para 1, 2a, 2b A5.2, A8.9
B.12.8			5.2 para 1a, 1b, 1c A5.36, A8.9
B.12.9			5.2 para 1a, 1b, 1c A8.15
B.12.10			5.2 para 1a, 1b, 1c A8.8
B.12.11	Advocate		A5.36, A8.8, A8.9, A8.19, A8.32
B.12.12			5.2 para 1a, 1b, 1c A5.36, A8.9
B.12.13			5.2 para 1a, 1b, 1c 10.2 para 1a1, 1a2, 1b1, 1c, 1d, 1e A5.36, A8.8, A8.9
B.13	Domain: Anti-virus/Anti-malware		
B.13.1	Supporter		A6.8, A8.1, A8.7, A8.19, A8.20, A8.26
B.13.2	Practitioner		A5.1, A5.23, A8.1, A8.7, A8.20, A8.23
B.13.3			A8.7
B.13.4			A8.7, A8.23

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Cyber Trust			ISO/IEC 27001:2022 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.13.5			A5.24, A5.26, A8.7
B.13.6	Promoter		A8.7, A8.31
B.13.7	Performer		5.3 para 1, 2a, 2b A5.2, A8.7
B.13.8	Advocate		A5.6, A5.7
B.13.9			7.4 para 1, 1a, 1b, 1c, 1d A5.36, A6.8, A8.7, A8.8
B.13.10			A5.25, A5.28, A8.7, A8.16
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	
B.14.5	Advocate		A8.5, A8.25, A8.27, A8.28
B.14.6			A8.26, A8.27, A8.28, A8.31, A8.32
B.14.7			A8.29, A8.32
B.14.8			A8.26, A8.29, A8.32
B.15	Domain: Access control		
B.15.1	Supporter		A5.15, A5.16, A5.17, A5.18, A5.19, A6.4, A6.6, A7.2, A7.3, A8.2, A8.3, A8.12, A8.18
B.15.2	Practitioner		A5.17, A5.18, A8.5, A8.12
B.15.3			A5.2, A5.16, A5.18
B.15.4	Promoter		A5.15, A5.16, A5.18
B.15.5			A5.2, A5.3, A5.16, A5.18, A8.3, A8.12
B.15.6			A5.15, A5.17, A8.2, A8.5, A8.12
B.15.7	Performer		A5.17
B.15.8			A5.15, A5.18, A8.12
B.15.9			A5.15, A6.7, A8.1, A8.3, A8.12
B.15.10	Advocate		A5.18, A6.8, A8.3
B.15.11			A5.2, A5.17, A8.2, A8.3, A8.5, A8.12

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Cyber Trust			ISO/IEC 27001:2022 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
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		A5.7, A8.15
B.16.5			A5.2, A5.5, A5.24, A6.8
B.16.6			A5.7, A5.28, A8.15, A8.16
B.16.7			A5.7, A8.15, A8.16
B.16.8			A6.8
B.16.9	Advocate		A5.7, A5.25
B.16.10			5.3 para 1, 2b 7.4 para 1, 1a, 1b, 1c, 1d 9.1 para 1a, 1b, 1c, 1d, 1e, 1f, 3 A6.8
B.16.11			A5.6, A5.7, A5.25
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		A5.19, A5.20, A5.22, A5.23, A8.30
B.17.6			A5.19, A5.20, A5.23
B.17.7			A5.19, A5.20, A5.23
B.17.8			A5.19, A5.22, A5.23, A8.30
B.17.9			7.4 para 1, 1a, 1b, 1c, 1d A5.19, A5.21, A5.23
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		A8.8
B.18.4			A5.36, A8.8
B.18.5	Performer		A5.2, A8.8

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Cyber Trust			ISO/IEC 27001:2022 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.18.6			A8.8
B.18.7			6.1.3 para 1a, 1b, 1e A8.8
B.18.8	Advocate		6.1.3 para 1a, 1b, 1e A8.8
B.18.9			6.1.3 para 1a, 1b, 1e A5.36, A8.8
B.18.10			6.1.3 para 1a, 1b, 1e A8.8
B.18.11			6.1.3 para 1a, 1b, 1e A8.8
B.19	Domain: Physical/environmental security		
B.19.1	Supporter	Domain is not assessable for this tier	
B.19.2	Practitioner		6.1.2 para 1c1, 1c2 6.1.3 para 1a A7.1
B.19.3			A5.15, A7.1, A7.3, A7.5, A7.7, A7.8, A7.9, A7.10, A7.11, A7.12, A8.1
B.19.4			A7.1, A7.2, A7.3
B.19.5	Promoter		A7.2
B.19.6			A7.1, A7.3, A7.4
B.19.7			A5.15, A7.8, A7.10, A7.14
B.19.8	Performer		5.2 para 1a 7.4 para 1, 1a, 1b, 1c, 1d A7.2
B.19.9			5.3 para 1, 2a, 2b 6.1.2 para 1c1, 1c2 6.1.3 para 1a A5.2
B.19.10			6.1.2 para 1d1, 1d2, 1d3, 1e1, 1e2 A5.15, A7.2
B.19.11	Advocate		7.4 para 1, 1a, 1b, 1c, 1d
B.19.12			6.1.2 para 1d1, 1d2, 1d3, 1e1, 1e2 A5.15, A7.2

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Cyber Trust			ISO/IEC 27001:2022 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.20	Domain: Network security		
B.20.1	Supporter	Domain is not assessable for this tier	
B.20.2	Practitioner		A8.20, A8.21
B.20.3			A8.20, A8.21
B.20.4			A5.36, A8.8, A8.20, A8.21
B.20.5	Promoter		A8.5, A8.12, A8.20, A8.21
B.20.6			A8.12, A8.20, A8.22
B.20.7	Performer		A8.20, A8.21
B.20.8			5.3 para 1, 2a, 2b A5.2, A8.20
B.20.9			A8.16, A8.20, A8.21
B.20.10	Advocate		A8.20, A8.21
B.20.11			A8.20, A8.21
B.21	Domain: Incident response		
B.21.1	Supporter		A5.2, A5.5, A5.24
B.21.2	Practitioner		A5.1, A5.24, A5.27
B.21.3	Promoter		A5.24, A5.26
B.21.4			7.2 para 1b 7.3 para 1b A5.5, A5.24, A6.3
B.21.5	Performer		A5.26, A5.27
B.21.6			A5.25, A5.26
B.21.7	Advocate		A5.26, A5.27, A6.8
B.21.8			5.2 para 1a, 1b, 1c 7.4 para 1, 1a, 1b, 1c, 1d A5.24, A5.26, A5.28, A6.8
B.22	Domain: Business continuity/Disaster recovery		
B.22.1	Supporter	Domain is not assessable for this tier	
B.22.2	Practitioner		A5.9, A5.29, A5.30, A7.13, A8.14
B.22.3	Promoter		A5.29, A5.30
B.22.4			A5.29, A5.30, A7.13, A8.14
B.22.5	Performer		A5.2, A5.29, A5.30
B.22.6			A5.29, A5.30

Cross-mapping between Cyber Trust and ISO/IEC 27001:2022

Cyber Trust			ISO/IEC 27001:2022 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.22.7			A5.29, A5.30
B.22.8			A5.29, A5.30
B.22.9	Advocate		7.4 para 1, 1a, 1b, 1c, 1d A5.29, A5.30, A8.14
B.22.10			A5.29, A5.30, A5.35