CSA CYBERSECURITY CERTIFICATION

Cross-mapping between Cyber Trust and ISO/IEC 27001

Date of Publication: 18-05-2022 (First edition, revised)

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 27001:2013 and the Cyber Trust mark developed by the Cyber Security Agency of Singapore (CSA).

ISO/IEC 27001:2013 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 200 ISO/IEC 27001: 2013 certificates issued to Singapore[1].

Organisations that are certified in ISO/IEC 27001:2013 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 27001:2013 to the cybersecurity preparedness domains in Cyber Trust mark; and

b) Annex II maps the Annex A control clauses in ISO/IEC 27001:2013 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 27001:2013 may refer to the mapping in Annex III, which maps the cybersecurity preparedness statements in Cyber Trust mark to ISO/IEC 27001:2013.

[1] Source – ISO Survey 2020

Cross-mapping between Cyber Trust and ISO/IEC 27001

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 27001:2013.

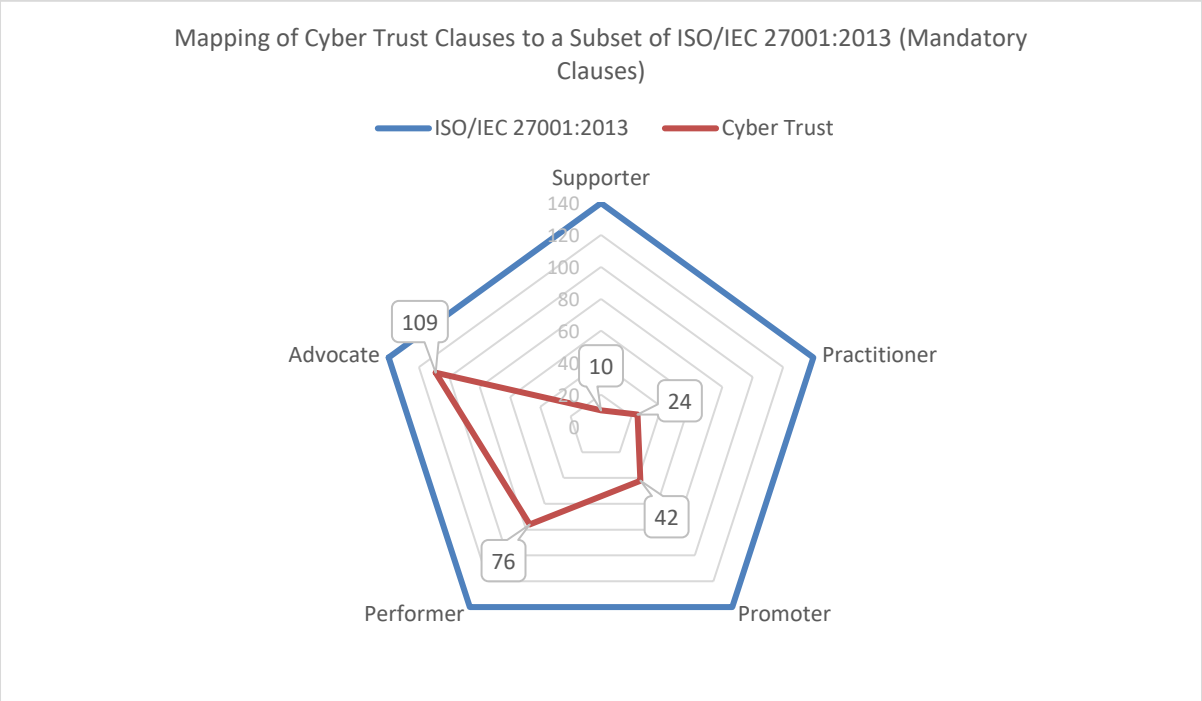

Figure 1 – Mapping of Cyber Trust clauses to subset of ISO/IEC 27001:2013 (Mandatory Clauses)

	ISO/IEC 27001:2013 (Mandatory Clauses)	Cyber Trust Clauses Mapped to ISO/IEC 27001:2013				
		Supporter	Practitioner	Promoter	Performer	Advocate
# of clauses	140	10	24	42	76	109
Percentage	100%	7.1%	17.1%	30%	54.3%	77.9%

Table 1 – Mapping of Cyber Trust clauses to subset of ISO/IEC 27001:2013 (Mandatory Clauses)

There are a total of 140 requirements in the mandatory clauses (i.e. clauses 4 – 10) of ISO/IEC 27001:2013.

The clauses in the “Advocate” tier of Cyber Trust mark map to 109 of these 140 requirements in the mandatory clauses of ISO/IEC 27001:2013. 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 109 clauses would include those in the lower tiers, i.e. “Performer”, “Promoter”, “Practitioner” and “Supporter”.

Cross-mapping between Cyber Trust and ISO/IEC 27001

Figure 2 and Table 2 show the mapping of clauses in Cyber Trust to a subset of the Annex A clauses in ISO/IEC 27001:2013.

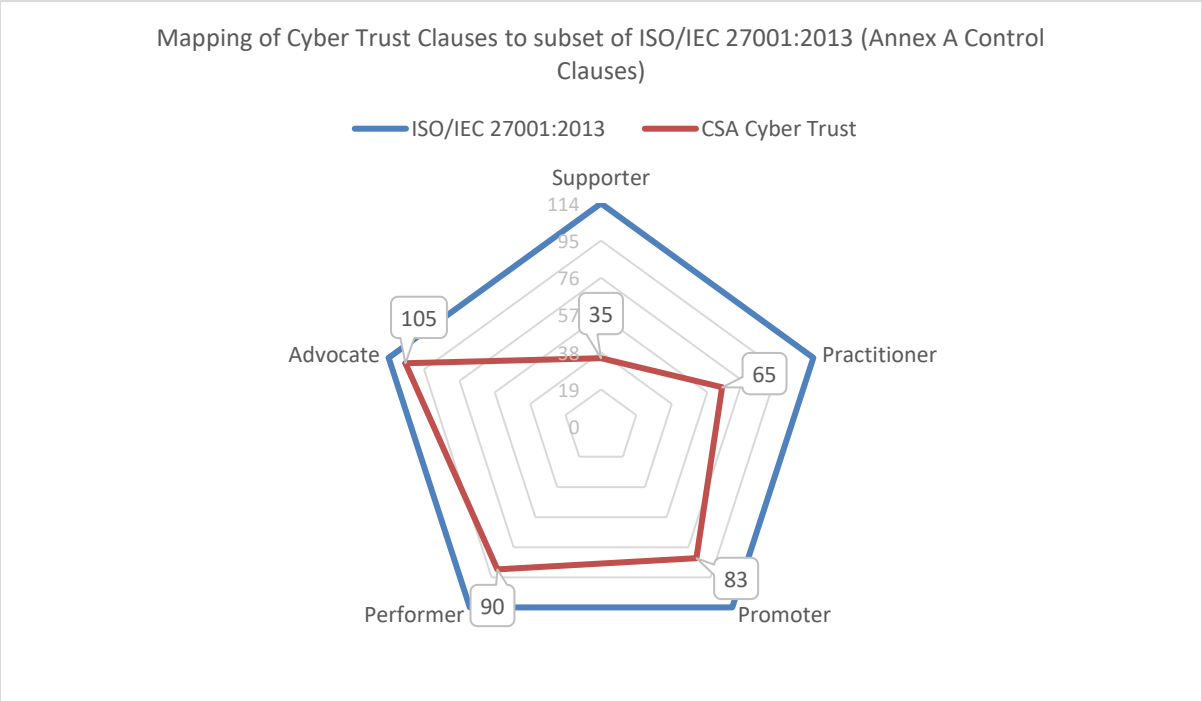

Figure 2 – Mapping of Cyber Trust clauses to subset of ISO/IEC 27001:2013 (Annex A Clauses)

	ISO/IEC 27001:2013 (Annex A Control Clauses)	Cyber Trust Clauses Mapped to ISO/IEC 27001:2013				
		Supporter	Practitioner	Promoter	Performer	Advocate
# of clauses	114	35	65	83	90	105
Percentage	100%	30.7%	57.0%	72.8%	78.9%	92.1%

Table 2 – Mapping of Cyber Trust clauses to subset of ISO/IEC 27001:2013 (Annex A Clauses)

There are a total of 114 control clauses in Annex A of ISO/IEC 27001:2013. 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 105 of these 114 control clauses in Annex A of ISO/IEC 27001:2013. 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 105 clauses would include those in the lower tiers, i.e. “Performer”, “Promoter”, “Practitioner” and “Supporter”.

Annex I

Mapping of ISO/IEC 27001:2013 (Mandatory Clauses) to Cyber Trust mark

Clause	ISO/IEC 27001:2013 (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
4.3	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

Clause	ISO/IEC 27001:2013 (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.9.5 B.9.7	B.2.4 B.3.7 B.8.3 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.9.5 B.9.7	B.2.4 B.2.6 B.3.7 B.8.3 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

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (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**
5.2 para 1c				B.9.5 B.9.7	B.2.4 B.3.7 B.8.3 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 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.1.4 B.3.8 B.5.6 B.8.5 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.1.4 B.3.8 B.5.6 B.8.5 B.9.9 B.10.7 B.12.7 B.13.7 B.19.9 B.20.8	

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (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**
5.3 para 2b					B.1.4 B.8.5 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					
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

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (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**
6.1.2 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
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.3.11
6.2 para 2e				B.3.6	B.1.6	
6.2 para 3						
6.2 para 4f				B.3.6	B.1.6	
6.2 para 4g					B.1.6	

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (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**
6.2 para 4h				B.3.6	B.1.6	
6.2 para 4i				B.3.6	B.1.6	
6.2 para 4j						
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		B.7.1	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

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (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**
7.4 para 1b					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 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.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 1e				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
7.5	Documented information					
7.5.1	General					
7.5.1 para 1a						
7.5.1 para 1b						

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (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**
7.5.2	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						
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		

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (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**
8.3 para 2			B.3.3	B.3.6		
9	Performance evaluation					
9.1	Monitoring, measurement, analysis and evaluation					
9.1 para 1						B.2.8 B.4.8 B.4.9 B.16.10
9.1 para 2a						B.2.8 B.4.8 B.4.9 B.16.10
9.1 para 2b						B.2.8 B.4.8 B.4.9 B.16.10
9.1 para 2c						B.4.8 B.4.9 B.16.10
9.1 para 2d						B.4.8 B.4.9 B.16.10
9.1 para 2e						B.4.8 B.4.9 B.16.10
9.1 para 2f						B.4.8 B.4.9 B.16.10
9.1 para 3						
9.2	Internal audit					
9.2 para 1					B.6.4* B.6.5*	B.2.8* B.6.8*
9.2 para 1a1						B.2.8
9.2 para 1a2						B.2.8
9.2 para 1b						B.2.8
9.2 para 2c					B.6.4	

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (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**
9.2 para 2d					B.6.4	
9.2 para 2e					B.6.5	
9.2 para 2f						B.6.8
9.2 para 2g						
9.3	Management review					
9.3 para 1					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9 B.6.7
9.3 para 2a					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9
9.3 para 2b					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9
9.3 para 2c1					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9
9.3 para 2c2					B.1.6	B.1.7 B.1.8 B.4.9
9.3 para 2c3					B.1.6	B.1.7 B.1.8 B.4.9 B.6.7
9.3 para 2c4					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9
9.3 para 2d					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9
9.3 para 2e					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (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**
9.3 para 2f					B.1.6	B.1.7 B.1.8 B.2.7 B.4.9
9.3 para 3						
9.3 para 4						
10	Improvement					
10.1	Nonconformity and corrective action					
10.1 para 1a1					B.6.6	B.2.7 B.2.9 B.3.12 B.5.8 B.6.8 B.12.13
10.1 para 1a2						B.2.7 B.2.9 B.3.12 B.5.8 B.6.8 B.12.13
10.1 para 1b1						B.2.7 B.2.9 B.3.12 B.5.8 B.6.8 B.12.13
10.1 para 1b2						B.2.7
10.1 para 1b3						B.2.7
10.1 para 1c						B.2.7 B.2.9 B.3.12 B.5.8 B.6.8 B.12.13
10.1 para 1d						B.2.7 B.2.9 B.5.8 B.6.8 B.12.13
10.1 para 1e						B.2.7 B.2.9 B.3.12

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (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.5.8 B.6.8 B.12.13
10.1 para 2						B.2.7 B.5.8 B.6.8
10.1 para 3f						B.2.7 B.5.8 B.6.8
10.1 para 3g						B.2.7 B.5.8 B.6.8
10.2	Continual Improvement					
10.2 para 1						B.2.7

Annex II

Mapping of ISO/IEC 27001:2013 (Annex A Control Clauses) to Cyber Trust mark

Clause	ISO/IEC 27001:2013 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
A.5	Information Security Policies					
A.5.1	Management direction for information security					
A.5.1.1	Policies for information security				B.1.5 B.2.4 B.2.5	
A.5.1.2	Review of the policies for information security		A.4.4 (i) A.9.4 (d) B.13.2 B.21.2		B.1.6	B.1.7
A.6	Organization of information security					
A.6.1	Internal organization					
A.6.1.1	Information security roles and responsibilities			B.1.3	B.1.4 B.8.5 B.9.9 B.10.7 B.12.7 B.13.7 B.16.5	
A.6.1.2	Segregation of duties			B.15.5		
A.6.1.3	Contact with authorities	A.9.4 (a) B.21.1 B.9.2		B.1.3 B.21.4	B.16.5	
A.6.1.4	Contact with special interest groups					B.1.7 B.13.8 B.16.11
A.6.1.5	Information security in project management					
A.6.2	Mobile devices and teleworking					
A.6.2.1	Mobile device policy		A.6.4 (h) B.12.2		B.11.4 B.15.9	B.11.5 B.11.6 B.11.7

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
A.6.2.2	Teleworking		A.1.4 (c) B.7.2		B.15.9	
A.7	Human resource security					
A.7.1	Prior to employment					
A.7.1.1	Screening					
A.7.1.2	Terms and conditions of employment					
A.7.2	During employment					
A.7.2.1	Management responsibilities			B.5.3		
A.7.2.2	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
A.7.2.3	Disciplinary process	A.5.4 (h) B.15.1				
A.7.3	Termination and change of employment					
A.7.3.1	Termination or change of employment responsibilities					
A.8	Asset management					
A.8.1	Responsibility for assets					
A.8.1.1	Inventory of assets	A.2.4 (a), (d) B.8.1	A.2.4 (b), (e), (f) B.8.2 B.22.2	B.8.6		B.8.8 B.8.9
A.8.1.2	Ownership of assets		A.2.4 (c) B.8.2			
A.8.1.3	Acceptable use of assets	A.2.4 (g), (h), (i), (j), (k) B.8.1			B.8.3 B.8.7	
A.8.1.4	Return of assets					
A.8.2	Information classification					
A.8.2.1	Classification of information			B.8.4 B.9.5		

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
A.8.2.2	Labelling of information	A.3.4 (a) B.9.1	A.3.4 (b) B.9.4	B.8.4		
A.8.2.3	Handling of assets	A.3.4 (c), (d) B.9.1 B.9.3	A.1.4 (c) B.7.2	B.8.4 B.9.5		
A.8.3	Media handling					
A.8.3.1	Management of removable media			B.19.7		
A.8.3.2	Disposal of media	A.3.4 (e) B.9.1	A.2.4 (m) B.8.2		B.8.3	
A.8.3.3	Physical media transfer			B.19.7		
A.9	Access control					
A.9.1	Business requirements of access control					
A.9.1.1	Access control policy	A.5.4 (a) B.15.1		B.15.4 B.15.6	B.15.8	
A.9.1.2	Access to networks and network services				B.15.9	
A.9.2	User access management					
A.9.2.1	User registration and deregistration	A.5.4 (b) B.15.1		B.15.5		
A.9.2.2	User access provisioning	A.5.4 (c), (e), (g) B.15.1		B.15.5		
A.9.2.3	Management of privileged access rights	A.5.4 (f) B.15.1		B.15.6		B.15.11
A.9.2.4	Management of secret authentication information of users			B.15.6		B.15.11
A.9.2.5	Review of user access rights		A.5.4 (j) B.15.2 B.15.3	B.15.4		B.15.10
A.9.2.6	Removal or adjustment of access rights	A.5.4 (e), (g) B.15.1	A.5.4 (k) B.15.2		B.15.8	
A.9.3	User responsibilities					

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
A.9.3.1	Use of secret authentication information			B.15.6		
A.9.4	System and application access control					
A.9.4.1	Information access restriction	A.5.4 (m) B.15.1		B.15.5	B.15.9	B.15.10 B.15.11
A.9.4.2	Secure log-on procedures		A.5.4 (o) B.15.2	B.15.6		
A.9.4.3	Password management system	A.5.4 (l), (n) B.15.1	A.1.4 (c) A.5.4 (p) B.7.2 B.15.2		B.15.7	
A.9.4.4	Use of privileged utility programs	A.5.4 (f) B.15.1	A.5.4 (o)			
A.9.4.5	Access control to program source code					
A.10	Cryptography					
A.10.1	Cryptographic controls					
A.10.1.1	Policy on the use of cryptographic controls				B.9.10	B.9.11
A.10.1.2	Key management					B.9.11
A.11	Physical and environmental security					
A.11.1	Secure areas					
A.11.1.1	Physical security perimeter		B.19.2 B.19.3 B.19.4	B.19.6		
A.11.1.2	Physical entry controls	A.5.4 (i) B.15.1	B.19.4	B.19.5	B.19.8 B.19.10	B.19.12
A.11.1.3	Securing offices, rooms and facilities	A.5.4 (i) B.15.1	B.19.3 B.19.4	B.19.6		
A.11.1.4	Protecting against external and environmental threats		B.19.3			
A.11.1.5	Working in secure areas		A.1.4 (c) B.7.2			
A.11.1.6	Delivery and loading areas		B.19.4			
A.11.2	Equipment					

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
A.11.2.1	Equipment siting and protection		B.19.3	B.19.7		
A.11.2.2	Supporting utilities		B.19.3			
A.11.2.3	Cabling security		B.19.3			
A.11.2.4	Equipment maintenance		B.22.2	B.22.4		
A.11.2.5	Removal of assets		B.19.3			
A.11.2.6	Security of equipment and assets off-premises		B.19.3			
A.11.2.7	Secure disposal or re-use of equipment	A.2.4 (l) A.3.4 (e) B.8.1 B.9.1		B.19.7		
A.11.2.8	Unattended user equipment		B.19.3			
A.11.2.9	Clear desk and clear screen policy		B.19.3			
A.12	Operations security					
A.12.1	Operational procedures and responsibilities					
A.12.1.1	Documented operating procedures	A.1.4 (b) B.7.1				
A.12.1.2	Change management					B.12.11
A.12.1.3	Capacity management					
A.12.1.4	Separation of development, testing and operational environments			B.13.6		
A.12.2	Protection from malware					
A.12.2.1	Controls 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
A.12.3	Backup					

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
A.12.3.1	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
A.12.4	Logging and monitoring					
A.12.4.1	Event logging		A.6.4 (f), (h) B.12.2	B.12.5	B.12.9 B.16.4 B.16.6 B.16.7	
A.12.4.2	Protection of log information			B.12.5	B.12.9 B.16.4 B.16.6	
A.12.4.3	Administrator and operator logs Control		A.6.4 (f) B.12.2	B.12.5	B.12.9 B.16.4 B.16.6	
A.12.4.4	Clock synchronisation					
A.12.5	Control of operational software					
A.12.5.1	Installation of software on operational systems					B.12.11
A.12.6	Technical vulnerability management					
A.12.6.1	Management of technical vulnerabilities	A.7.4 (a) B.12.1	A.7.4 (c), (d) B.12.2 B.12.3	B.12.6 B.18.3 B.18.4	B.12.10 B.18.5 B.18.6 B.18.7	B.18.8 B.18.9 B.18.10 B.18.11
A.12.6.2	Restrictions on software installation	A.4.4 (k) B.13.1				
A.12.7	Information systems audit considerations					
A.12.7.1	Information systems audit controls				B.6.4	
A.13	Communications security					
A.13.1	Network security management					
A.13.1.1	Network controls	A.4.4 (f), (g), (l) B.13.1	A.4.4 (h), (i), (j) B.13.2 B.20.2	B.20.5 B.20.6	B.20.7 B.20.8 B.20.9	B.20.10 B.20.11

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
			B.20.3 B.20.4			
A.13.1.2	Security of network services		B.20.2 B.20.3 B.20.4	B.20.5	B.20.9	B.20.11
A.13.1.3	Segregation in networks		A.6.4 (h) B.12.2	B.20.6		B.11.7
A.13.2	Information transfer					
A.13.2.1	Information transfer policies and procedures			B.9.6	B.9.8	B.9.12
A.13.2.2	Agreements on information transfer			B.9.6		
A.13.2.3	Electronic messaging					B.9.12
A.13.2.4	Confidentiality or non-disclosure agreements	A.5.4 (h) B.15.1				
A.14	System acquisition, development and maintenance					
A.14.1	Security requirements of information systems					
A.14.1.1	Information security requirements analysis and specification	A.6.4 (a), (b), (c), (d), (e) B.12.1	A.6.4 (g), (h) A.7.4 (d) B.12.2			
A.14.1.2	Securing application services on public networks	A.3.4 (c) A.4.4 (g), (l) A.6.4 (c) B.9.1 B.12.1 B.13.1	B.12.2 B.13.2	B.9.5 B.9.6 B.9.7	B.9.8 B.9.10	B.9.11 B.9.12 B.9.13
A.14.1.3	Protecting application services transactions	A.3.4 (c) A.4.4 (g), (l) A.6.4 (c) B.9.1 B.12.1 B.13.1	B.12.2 B.13.2	B.9.5 B.9.6 B.9.7	B.9.8 B.9.10	B.9.11 B.9.12 B.9.13
A.14.2	Security in development and support processes					

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
A.14.2.1	Secure development policy					B.14.5
A.14.2.2	System change control procedures					B.14.7
A.14.2.3	Technical review of applications after operating platform changes		A.7.4 (b) B.12.2 B.12.3	B.12.6		B.14.8
A.14.2.4	Restrictions on changes to software packages					B.14.6
A.14.2.5	Secure system engineering principles					B.14.5 B.14.6
A.14.2.6	Secure development environment					B.14.6
A.14.2.7	Outsourced development					B.17.5
A.14.2.8	System security testing					B.14.8
A.14.2.9	System acceptance testing			B.12.6		B.14.7 B.14.8
A.14.3	Test data					
A.14.3.1	Protection of test data					
A.15	Supplier relationships					
A.15.1	Information security in supplier relationships					
A.15.1.1	Information security policy for supplier relationships	A.5.4 (h) B.15.1				B.17.7 B.17.9
A.15.1.2	Addressing security within supplier agreements	B.9.3				B.17.5 B.17.6 B.17.7
A.15.1.3	Information and communication technology supply chain					B.17.9
A.15.2	Supplier service delivery management					
A.15.2.1	Monitoring and review of supplier services					B.17.5 B.17.8

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
A.15.2.2	Managing changes to supplier services					B.17.8
A.16	Information security incident management					
A.16.1	Management of information security incidents and improvements					
A.16.1.1	Responsibilities and procedures	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.16.5	B.21.8
A.16.1.2	Reporting information security events	A.4.4 (m) 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.21.8
A.16.1.3	Reporting information security weaknesses	A.4.4 (m) B.13.1				B.21.7
A.16.1.4	Assessment of and decision on information security events				B.21.6	B.13.10 B.16.9 B.16.11
A.16.1.5	Response to information security incidents		B.13.5	B.21.3	B.21.5 B.21.6	B.21.7 B.21.8
A.16.1.6	Learning from information security incidents		A.9.4 (c) B.21.2		B.21.5	B.21.7
A.16.1.7	Collection of evidence				B.16.6	B.13.10 B.21.8
A.17	Information security aspects of business continuity management					
A.17.1	Information security continuity					
A.17.1.1	Planning information security continuity		B.22.2	B.22.3 B.22.4		
A.17.1.2	Implementing information security continuity			B.22.4	B.22.5 B.22.6	
A.17.1.3	Verify, review and evaluate information security continuity				B.22.7 B.22.8	B.22.9 B.22.10

Cross-mapping between Cyber Trust and ISO/IEC 27001

Clause	ISO/IEC 27001:2013 (Annex A Control Clauses)	Cyber Trust				
		Supporter	Practitioner	Promoter	Performer	Advocate
A.17.2	Redundancies					
A.17.2.1	Availability of information processing facilities		B.22.2	B.22.4		B.22.9
A.18	Compliance					
A.18.1	Compliance with legal and contractual requirements					
A.18.1.1	Identification of applicable legislation and contractual requirements	B.5.1				
A.18.1.2	Intellectual property rights			B.5.4	B.5.5	
A.18.1.3	Protection of records			B.5.4 B.9.6 B.9.7	B.5.5 B.9.8	
A.18.1.4	Privacy and protection of personally identifiable information			B.5.4	B.5.5	
A.18.1.5	Regulation of cryptographic controls			B.5.4	B.5.5	
A.18.2	Information security reviews					
A.18.2.1	Independent review of information security		B.5.2			B.5.7 B.22.10
A.18.2.2	Compliance with security policies and standards		B.5.2		B.12.8	B.2.7 B.2.8 B.2.9 B.5.7 B.11.6 B.12.12
A.18.2.3	Technical compliance review		B.5.2 B.20.4	B.12.4 B.18.4		B.5.7 B.12.11 B.12.13 B.13.9 B.18.9

Annex III

Mapping of Cyber Trust mark to ISO/IEC 27001:2013

Cyber Trust			ISO/IEC 27001:2013 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 (a), (b) 5.1 (d) 7.4 (a), (c), (e) A.6.1.1
B.1.4	Performer		5.3 (a), (b) A.6.1.1
B.1.5			5.1 (a), (b), (c), (f), (h) A.5.1.1
B.1.6			5.1 (e), (g) 6.2 (a), (e), (f), (g), (h), (i) 9.3 (a), (b), (c), (d), (e), (f) A.5.1.2
B.1.7	Advocate		5.1 (a), (b), (c), (d), (e), (f), (g), (h) 9.1 (a), (d), (f) 9.3 (a), (b), (c1), (c2), (c3), (c4), (d), (e), (f) A.5.1.2 A.6.1.4
B.1.8			7.4 (a), (b), (c), (d), (e) 9.1 (a), (d), (f) 9.3 (a), (b), (c1), (c2), (c3), (c4), (d), (e), (f)
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		5.2 (b), (f), (g) 7.3 (a), (b) A.7.2.2
B.2.4	Performer		5.2 (a), (b), (c), (d), (e) A.5.1.1
B.2.5			A.5.1.1

Cross-mapping between Cyber Trust and ISO/IEC 27001

Cyber Trust			ISO/IEC 27001:2013 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.2.6			5.2 (b), (f), (g) 7.4 (a), (b), (c), (e)
B.2.7	Advocate		7.5.2 (c) 9.3 (a), (b), (c1), (c4), (d), (e), (f) 10.1 (a1), (a2), (b1), (b2), (b3), (c), (d), (e), (f), (g) 10.2 para 1 A.18.2.2
B.2.8			5.2 (a), (b), (c), (d), (e) 9.1 (a), (b) 9.2 (a1), (a2), (b) A.18.2.2
B.2.9			10.1 (a1), (a2), (b1), (c), (d), (e) A.18.2.2
B.3	Domain: Risk management		
B.3.1	Supporter		6.1.2 (c1)
B.3.2			6.1.2 (d1), (d2), (d3), (e1), (e2)
B.3.3	Practitioner		6.1.1 (a), (b), (d), (e1) 6.1.3 (a), (b), (e) 8.3 para 1, para 2
B.3.4			6.1.2 (c1), para 2 8.2 para 1, para 2
B.3.5	Promoter		6.1.2 (c1), (d1), (d2), (d3), (e1)
B.3.6			6.1.3 (f) 6.2 (e), (f), (h), (i) 8.3 para 1, para 2
B.3.7	Performer		5.2 (a), (b), (c), (d), (e) 6.1.2 (c1), (d1), (d2), (d3), (e1)
B.3.8			5.3 (a)
B.3.9			6.1.2 (a1)
B.3.10	Advocate		5.1 (a), (b)
B.3.11			5.3 (b) 6.2 (d) 7.4 (a), (b), (c), (d), (e)
B.3.12			8.2 para 1, para 2 10.1 (a1), (a2), (b1), (c), (d), (e)
B.4	Domain: Cyber strategy		
B.4.1	Supporter	Domain is not assessable for this tier	

Cross-mapping between Cyber Trust and ISO/IEC 27001

Cyber Trust			ISO/IEC 27001:2013 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
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 (a), (b) 4.3 (a), (b), (c) 8.1 para 1, para 2, para 3, para 4
B.4.6			4.4 para 1 8.1 para 1, para 2, para 3, para 4
B.4.7			7.1 para 1
B.4.8			5.3 (b) 9.1 (a), (b) (c), (d), (e), (f)
B.4.9			5.1 (a), (b), (e) 7.5.2 (c) 9.1 (a), (b), (c), (d), (e), (f) 9.3 (a), (b), (c1), (c2), (c3), (c4), (d), (e), (f)
B.5	Domain: Compliance		
B.5.1	Supporter		4.2 (a), (b) A.18.1.1
B.5.2	Practitioner		6.1.1 (a), (b), (d), (e1) 6.1.3 (a), (b), (e) A.18.2.1 A.18.2.2 A.18.2.3
B.5.3	Promoter		7.4 (a), (c), (e) A.7.2.1 A.7.2.2
B.5.4			A.18.1.2 A.18.1.3 A.18.1.4 A.18.1.5
B.5.5	Performer		A.18.1.2 A.18.1.3 A.18.1.4 A.18.1.5
B.5.6			5.3 (a)
B.5.7	Advocate		A.18.2.1 A.18.2.2 A.18.2.3

Cross-mapping between Cyber Trust and ISO/IEC 27001

Cyber Trust			ISO/IEC 27001:2013 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.5.8			10.1 (a1), (a2), (b1), (c), (d), (e), (f), (g)
B.5.9			5.3 (b)
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 (c), (d) A.12.7.1
B.6.5			9.2 (e)
B.6.6			10.1 (a1)
B.6.7	Advocate		9.3 (c3)
B.6.8			9.2 (f) 10.1 (a1), (a2), (b1), (c), (d), (e), (f), (g)
B.7	Domain: Training and awareness		
B.7.1	Supporter		7.3 para 1a, para 1b A.7.2.2 A.12.1.1
B.7.2	Practitioner		7.3 para 1a, para 1b A.6.2.2 A.7.2.2 A.8.2.3 A.9.4.3 A.11.1.5 A.12.2.1 A.16.1.2
B.7.3			A.7.2.2
B.7.4	Promoter		A.7.2.2
B.7.5			7.1 para 1 7.2 (a), (b)
B.7.6	Performer		A.7.2.2
B.7.7			A.7.2.2
B.7.8			7.2 (a), (b), (c)
B.7.9	Advocate		7.2 (c) A.7.2.2
B.7.10			7.2 (a), (b), (c)

Cross-mapping between Cyber Trust and ISO/IEC 27001

Cyber Trust			ISO/IEC 27001:2013 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.7.11			7.1 para 1 A.7.2.2
B.8	Domain: Asset management		
B.8.1	Supporter		A.8.1.1 A.8.1.3 A.11.2.7
B.8.2	Practitioner		A.8.1.1 A.8.1.2 A.8.3.2
B.8.3	Promoter		A.8.1.1
B.8.4			A.8.2.1 A.8.2.2 A.8.2.3
B.8.5			5.3 (a), (b) A.6.1.1
B.8.6	Performer		A.8.1.1
B.8.7			A.8.1.3
B.8.8	Advocate		5.2 (a), (b), (c) A.8.1.1
B.8.9			A.8.1.1
B.8.10			6.1.1 para 2e1
B.9	Domain: Data protection and privacy		
B.9.1	Supporter		A.8.2.2 A.8.2.3 A.8.3.2 A.11.2.7 A.14.1.2 A.14.1.3
B.9.2			A.6.1.3 A.16.1.1 A.16.1.2
B.9.3			A.8.2.3 A.15.1.2
B.9.4	Practitioner		A.8.2.2
B.9.5	Promoter		5.2 (a), (b), (c) A.8.2.1 A.8.2.3 A.14.1.2 A.14.1.3

Cross-mapping between Cyber Trust and ISO/IEC 27001

Cyber Trust			ISO/IEC 27001:2013 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.9.6			A.13.2.1 A.13.2.2 A.14.1.2 A.14.1.3 A.18.1.3
B.9.7			5.2 (a), (b), (c) A.14.1.2 A.14.1.3 A.18.1.3
B.9.8	Performer		5.2 (a), (b), (c) A.13.2.1 A.14.1.2 A.14.1.3 A.18.1.3
B.9.9			5.3 (a), (b) A.6.1.1
B.9.10			A.10.1.1 A.14.1.2 A.14.1.3
B.9.11	Advocate		5.2 (a), (b), (c) A.10.1.1 A.10.1.2 A.14.1.2 A.14.1.3
B.9.12			5.2 (a), (b), (c) A.13.2.1 A.13.2.3 A.14.1.2 A.14.1.3
B.9.13			5.2 (a), (b), (c) 7.4 (a), (b), (c), (d), (e) A.14.1.2 A.14.1.3
B.10	Domain: Backups		
B.10.1	Supporter		A.12.3.1
B.10.2	Practitioner		A.12.3.1
B.10.3			A.12.3.1
B.10.4	Promoter		A.12.3.1
B.10.5			A.12.3.1
B.10.6	Performer		5.2 (a), (b), (c) A.12.3.1

Cross-mapping between Cyber Trust and ISO/IEC 27001

Cyber Trust			ISO/IEC 27001:2013 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.10.7			5.3 (a), (b) A.6.1.1 A.12.3.1
B.10.8	Advocate		A.12.3.1
B.10.9			5.2 (a), (b), (c) 7.4 (a), (b), (c), (d), (e)
B.10.10			5.2 (a), (b), (c) A.12.3.1
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 (a), (b), (c) A.6.2.1
B.11.5	Advocate		A.6.2.1
B.11.6			A.6.2.1 A.18.2.2
B.11.7			5.2 (a), (b), (c) A.6.2.1 A.13.1.3
B.12	Domain: System security		
B.12.1	Supporter		A.12.6.1 A.14.1.1 A.14.1.2 A.14.1.3
B.12.2	Practitioner		A.6.2.1 A.12.4.1 A.12.4.3 A.12.6.1 A.13.1.3 A.14.1.1 A.14.1.2 A.14.1.3 A.14.2.3
B.12.3			A.12.6.1 A.14.2.3
B.12.4	Promoter		A.18.2.3
B.12.5			A.12.4.1 A.12.4.2 A.12.4.3

Cross-mapping between Cyber Trust and ISO/IEC 27001

Cyber Trust			ISO/IEC 27001:2013 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.12.6			A.12.6.1 A.14.2.3 A.14.2.9
B.12.7	Performer		5.3 (a), (b) A.6.1.1
B.12.8			5.2 (a), (b), (c) A.18.2.2
B.12.9			5.2 (a), (b), (c) A.12.4.1 A.12.4.2 A.12.4.3
B.12.10			5.2 (a), (b), (c) A.12.6.1
B.12.11	Advocate		A.12.1.2 A.12.5.1 A.18.2.3
B.12.12			5.2 (a), (b), (c) A.18.2.2
B.12.13			5.2 (a), (b), (c) 10.1 (a1), (a2), (b1), (c), (d), (e) A.18.2.3
B.13	Domain: Anti-virus/Anti-malware		
B.13.1	Supporter		A.12.2.1 A.12.6.2 A.13.1.1 A.14.1.2 A.14.1.3 A.16.1.2 A.16.1.3
B.13.2	Practitioner		A.5.1.2 A.12.2.1 A.13.1.1 A.14.1.2 A.14.1.3
B.13.3			A.12.2.1
B.13.4			A.12.2.1
B.13.5			A.12.2.1 A.16.1.1 A.16.1.5
B.13.6	Promoter		A.12.1.4 A.12.2.1

Cross-mapping between Cyber Trust and ISO/IEC 27001

Cyber Trust			ISO/IEC 27001:2013 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.13.7	Performer		5.3 (a), (b) A.6.1.1 A.12.2.1
B.13.8	Advocate		A.6.1.4
B.13.9			7.4 (a), (b), (c), (d), (e) A.12.2.1 A.16.1.2 A.18.2.3
B.13.10			A.12.2.1 A.16.1.4 A.16.1.7
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		A.14.2.1 A.14.2.5
B.14.6			A.14.2.4 A.14.2.5 A.14.2.6
B.14.7			A.14.2.2 A.14.2.9
B.14.8			A.14.2.3 A.14.2.8 A.14.2.9
B.15	Domain: Access control		
B.15.1	Supporter		A.7.2.3 A.9.1.1 A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.6 A.9.4.1 A.9.4.3 A.9.4.4 A.11.1.2 A.11.1.3 A.13.2.4 A.15.1.1
B.15.2	Practitioner		A.9.2.5 A.9.2.6

Cross-mapping between Cyber Trust and ISO/IEC 27001

Cyber Trust			ISO/IEC 27001:2013 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
			A.9.4.2 A.9.4.3
B.15.3			A.9.2.5
B.15.4	Promoter		A.9.1.1 A.9.2.5
B.15.5			A.6.1.2 A.9.2.1 A.9.2.2 A.9.4.1
B.15.6			A.9.1.1 A.9.2.3 A.9.2.4 A.9.3.1 A.9.4.2
B.15.7	Performer		A.9.4.3
B.15.8			A.9.1.1 A.9.2.6
B.15.9			A.6.2.1 A.6.2.2 A.9.1.2 A.9.4.1
B.15.10	Advocate		A.9.2.5 A.9.4.1 A.16.1.2
B.15.11			A.9.2.3 A.9.2.4 A.9.4.1
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		A.12.4.1 A.12.4.2 A.12.4.3
B.16.5			A.6.1.1 A.6.1.3 A.16.1.2
B.16.6			A.12.4.1 A.12.4.2 A.12.4.3 A.16.1.7

Cross-mapping between Cyber Trust and ISO/IEC 27001

Cyber Trust			ISO/IEC 27001:2013 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.16.7			A.12.4.1
B.16.8			A.16.1.2
B.16.9	Advocate		A.16.1.4
B.16.10			5.3 (b) 7.4 (a), (b), (c), (d), (e) 9.1 (a), (b), (c), (d), (e), (f) A.16.1.2
B.16.11			A.6.1.4 A.16.1.4
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		A.14.2.7 A.15.1.2 A.15.2.1
B.17.6			A.15.1.2
B.17.7			A.15.1.1 A.15.1.2
B.17.8			A.15.2.1 A.15.2.2
B.17.9			7.4 (a), (b), (c), (d), (e) A.15.1.1 A.15.1.3
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		A.12.6.1
B.18.4			A.12.6.1 A.18.2.3
B.18.5	Performer		A.12.6.1
B.18.6			A.12.6.1
B.18.7			6.1.3 (a), (b), (e) A.12.6.1
B.18.8	Advocate		6.1.3 (a), (b), (e) A.12.6.1

Cross-mapping between Cyber Trust and ISO/IEC 27001

Cyber Trust			ISO/IEC 27001:2013 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.18.9			6.1.3 (a), (b), (e) A.12.6.1 A.18.2.3
B.18.10			6.1.3 (a), (b), (e) A.12.6.1
B.18.11			6.1.3 (a), (b), (e) A.12.6.1
B.19	Domain: Physical/environmental security		
B.19.1	Supporter	Domain is not assessable for this tier	
B.19.2	Practitioner		6.1.2 (c1), (c2) 6.1.3 (a) A.11.1.1
B.19.3			A.11.1.1 A.11.1.3 A.11.2.1 A.11.2.2 A.11.2.3 A.11.2.5 A.11.2.6 A.11.2.8 A.11.2.9
B.19.4			A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.6
B.19.5	Promoter		A.11.1.2
B.19.6			A.11.1.1 A.11.1.3
B.19.7			A.11.2.1 A.11.2.7 A.8.3.1 A.8.3.3
B.19.8	Performer		5.2 (a) 7.4 (a), (b), (c), (d), (e) A.11.1.2
B.19.9			5.3 (a), (b) 6.1.2 (c1), (c2) 6.1.3 (a)
B.19.10			6.1.2 (d1), (d2), (d3), (e1), (e2) A.11.1.2
B.19.11	Advocate		7.4 (a), (b), (c), (d), (e)

Cross-mapping between Cyber Trust and ISO/IEC 27001

Cyber Trust			ISO/IEC 27001:2013 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.19.12			6.1.2 (d1), (d2), (d3), (e1), (e2) A.11.1.2
B.20	Domain: Network security		
B.20.1	Supporter	Domain is not assessable for this tier	
B.20.2	Practitioner		A.13.1.1 A.13.1.2
B.20.3			A.13.1.1 A.13.1.2
B.20.4			A.13.1.1 A.13.1.2 A.18.2.3
B.20.5	Promoter		A.13.1.1 A.13.1.2
B.20.6			A.13.1.1 A.13.1.3
B.20.7	Performer		A.13.1.1
B.20.8			5.3 (a), (b) A.13.1.1
B.20.9			A.13.1.1 A.13.1.2
B.20.10	Advocate		A.13.1.1
B.20.11			A.13.1.1 A.13.1.2
B.21	Domain: Incident response		
B.21.1	Supporter		A.6.1.3 A.16.1.1
B.21.2	Practitioner		A.5.1.2 A.16.1.1 A.16.1.6
B.21.3	Promoter		A.16.1.1 A.16.1.5
B.21.4			7.2 (b) 7.3 (b) A.6.1.3 A.7.2.2
B.21.5	Performer		A.16.1.5 A.16.1.6

Cross-mapping between Cyber Trust and ISO/IEC 27001

Cyber Trust			ISO/IEC 27001:2013 Clauses
Clause	**Cybersecurity Preparedness Tier**	**Description**	
B.21.6			A.16.1.4 A.16.1.5 A.16.1.7
B.21.7	Advocate		A.16.1.3 A.16.1.5 A.16.1.6
B.21.8			5.2 (a), (b), (c) 7.4 (a), (b), (c), (d), (e) A.16.1.1 A.16.1.2 A.16.1.5 A.16.1.7
B.22	Domain: Business continuity/Disaster recovery		
B.22.1	Supporter	Domain is not assessable for this tier	
B.22.2	Practitioner		A.8.1.1 A.11.2.4 A.17.1.1 A.17.2.1
B.22.3	Promoter		A.17.1.1
B.22.4			A.11.2.4 A.17.1.1 A.17.1.2 A.17.2.1
B.22.5	Performer		A.17.1.2
B.22.6			A.17.1.2
B.22.7			A.17.1.3
B.22.8			A.17.1.3
B.22.9	Advocate		7.4 (a), (b), (c), (d), (e) A.17.1.3 A.17.2.1
B.22.10			A.17.1.3 A.18.2.1