الهيئة الوطنية للأمن السيبـراني
National Cybersecurity Authority

ملحق المنهجية والمواءمة
لضوابط الأمن السيبراني للحوسبة السحابية

CCC Methodology and Mapping Annex

مسودة

إشـــارة المـــشـــاركـــة: أبـيـض
تـصـنـيـف الـوثـيـقـة: مـتـــاح

بســـم اللّه الرحمـــن الرحيـــم

بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل او خارج المنشأة خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

حيث يمكنك مشاركتها مع آخرين من منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

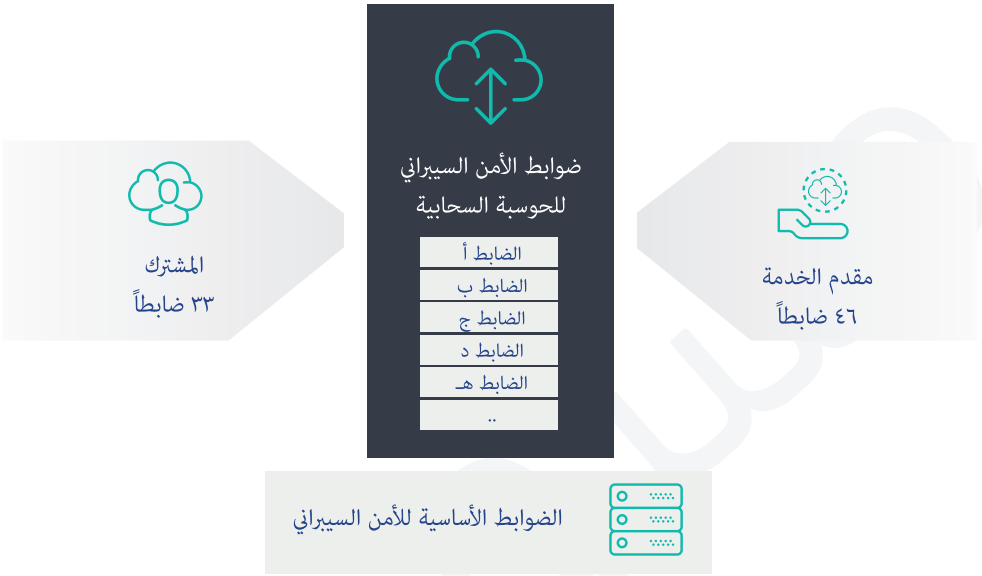
قائمة المحتويات

قائمة الأشكال والرسوم التوضيحية

قائمة الجداول

مبادئ تصميم ضوابط الأمن السيبراني للحوسبة السحابية

طورت ضوابط الأمن السيبراني للحوسبة السحابية لتكون امتداداً للضوابط الأساسية للأمن السيبراني؛ لتوفير ضوابط لكل من مقدمي الخدمات والمشتركين. ويجب أن يلتزم كل من مقدمي الخدمات والمشتركين بالضوابط الأساسية للأمن السيبراني أولًا، ثم الضوابط الإضافية المنصوص عليها في هذه الوثيقة "ضوابط الأمن السيبراني للحوسبة السحابية"، وبتعبير آخر، **يُعَدّ تحقيق الالتزام بالضوابط الأساسية للأمن السيبراني شرطًا مسبقًا لتحقيق الالتزام بضوابط الأمن السيبراني للحوسبة السحابية.**



شكل ١: ضوابط الأمن السيبراني للحوسبة السحابية كامتداد للضوابط الأساسية للأمن السيبراني

بالنسبة إلى مقدمي الخدمات، فقد تم تطبيق المبادئ التالية:

- أن يكون مستوى الأمن السيبراني مماثلًا لنظيره من معايير أمن الخدمات السحابية في البلدان الأخرى (مثل، المعيار الأمريكي الفيدرالي (FedRAMP)، الأمن السحابي في سنغافورة (MTCS)، معيار الحكومة الألمانية (C5) أو معيار (Cloud Controls Matrix (CCM)، ومعايـير (ISO/IEC 27000).

- أن يكون هناك إشارة إلى مدى التوافق مع المعايير العالمية ذات العلاقة، بحيث يمكن لمقدمي الخدمات الاستفادة من شهاداتهم التي سبق إصدارها في بلدان أخرى. كما هو مذكور في قسم "مواءمة المكونات الفرعية مع الأطر الدولية" و قسم "مواءمة الضوابط مع الأطر الدولية".

بالنسبة إلى المشتركين، فقد تم تطبيق المبادئ التالية:

- أن تكون المتطلبات الأمنية في هذه الضوابط امتدادًا للضوابط الأساسية للأمن السيبراني.

العلاقة بالمعايير الدولية الأخرى

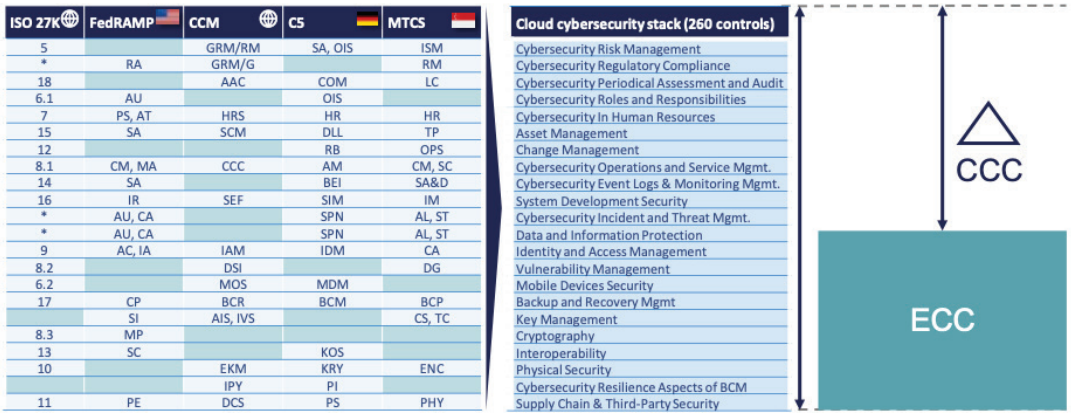
خلال تطوير هذه الضوابط، تم استخدام عدة معايير دولية ذات العلاقة بالأمن السيبراني والحوسبة السحابية. وتمثلت المعايير الرئيسية الخمسة التي استخدمت في تطوير هذه الضوابط فيما يلي:

- معايير ISO/IEC 27000.
- المعيار الأمريكي الفيدرالي FedRAMP (FR).
- معيار Cloud Controls Matrix (CCM) الصادر من تحالف أمن الحوسبة السحابية Cloud Security Alliance (CSA).
- معيار الحكومة الألمانية (C5).
- معايير الأمن السحابي في سنغافورة (MTCS).

منهجية تصميم ضوابط الأمن السيبراني للحوسبة السحابية

في سبيل تحقيق أهداف ضوابط الأمن السيبراني للحوسبة السحابية، فقد تبنت منهجية التصميم المتبعة مراجعة التشريعات المعنية بخصوصية البيانات وحمايتها وكذلك المتعلقة بالحوسبة السحابية. واستنادًا إلى هذه المراجع، طورت الهيئة ضوابط الأمن السيبراني للحوسبة السحابية لتكون امتدادًا مكمِّلًا للضوابط الأساسية للأمن السيبراني من حيث العمق والشمول في قطاع الحوسبة السحابية.

وخلال تطوير ضوابط الأمن السيبراني للحوسبة السحابية، تم استنباط قائمة موّحدة من المتطلبات الأمنية في المجالات ذات الصلة من خمسة معايير مرجعية في مجال الأمن السحابي (المذكورة في قسم "العلاقة بالمعايير الدولية") لتشكيل مجموعة مدمجة من ضوابط الحوسبة السحابية. وقد وفرت المقارنة مع الضوابط الحالية الأساسية للأمن السيبراني المنهجية التي سوف تحدد النطاق، حيث يضمن هذا النهج توفير ضوابط الأمن السيبراني للحوسبة السحابية المستوى الأمني الملائم للمعايير الأمنية المرجعية الخمسة (5) مجتمعة.



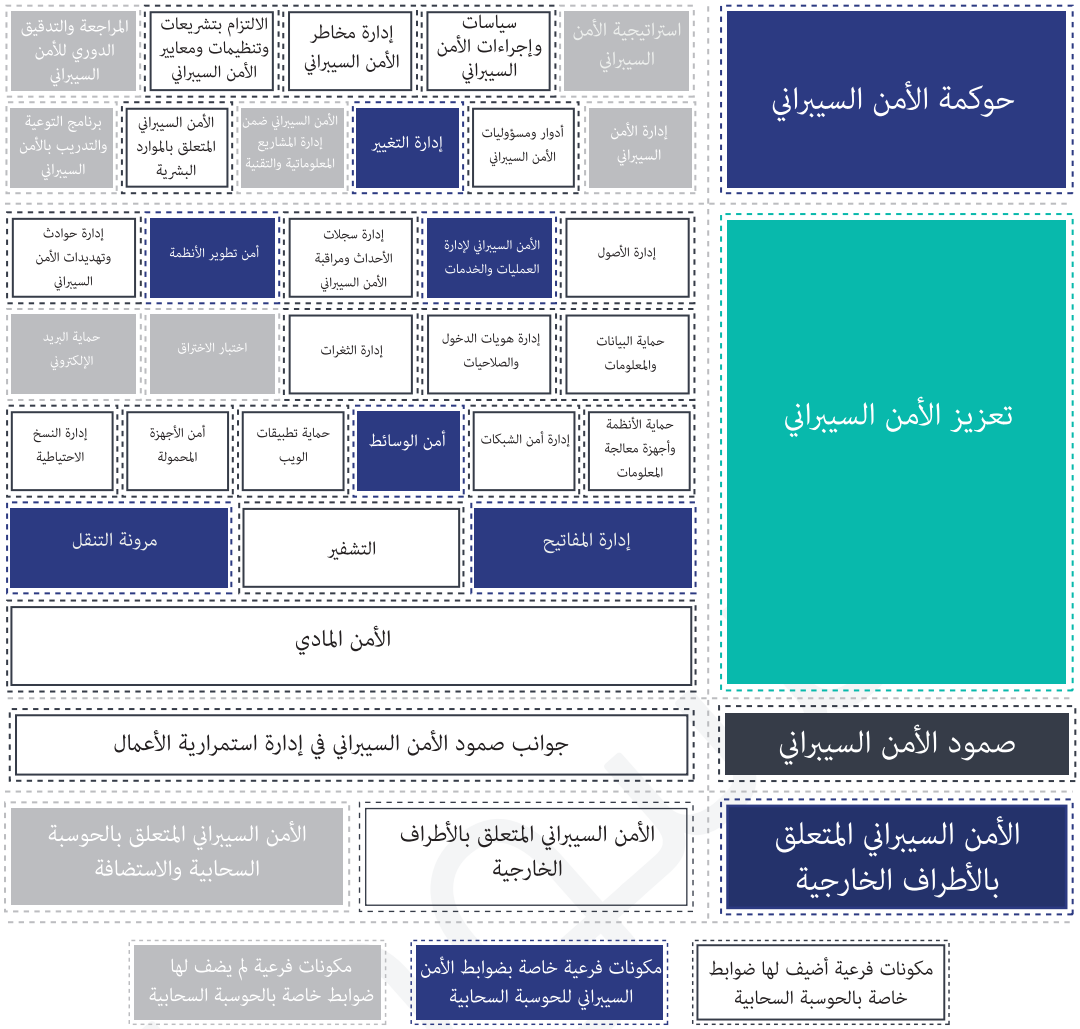
ISO 27K	FedRAMP	CCM	C5	MTCS
5		GRM/RM	SA, OIS	ISM
*	RA	GRM/G		RM
18		AAC	COM	LC
6.1	AU		OIS	
7	PS, AT	HRS	HR	HR
15	SA	SCM	DLL	TP
12			RB	OPS
8.1	CM, MA	CCC	AM	CM, SC
14	SA		BEI	SA&D
16	IR	SEF	SIM	IM
*	AU, CA		SPN	AL, ST
*	AU, CA		SPN	AL, ST
9	AC, IA	IAM	IDM	CA
8.2		DSI		DG
6.2		MOS	MDM	
17	CP	BCR	BCM	BCP
	SI	AIS, IVS		CS, TC
8.3	MP			
13	SC		KOS	
10		EKM	KRY	ENC
		IPY	PI	
11	PE	DCS	PS	PHY

شكل ٢: المعايير الدولية المعنية بالحوسبة السحابية التي تم استنباطها في قائمة الضوابط الموّحدة

مكونات وهيكلية ضوابط الأمن السيبراني للحوسبة السحابية

العلاقة مع الضوابط الأساسية للأمن السيبراني:

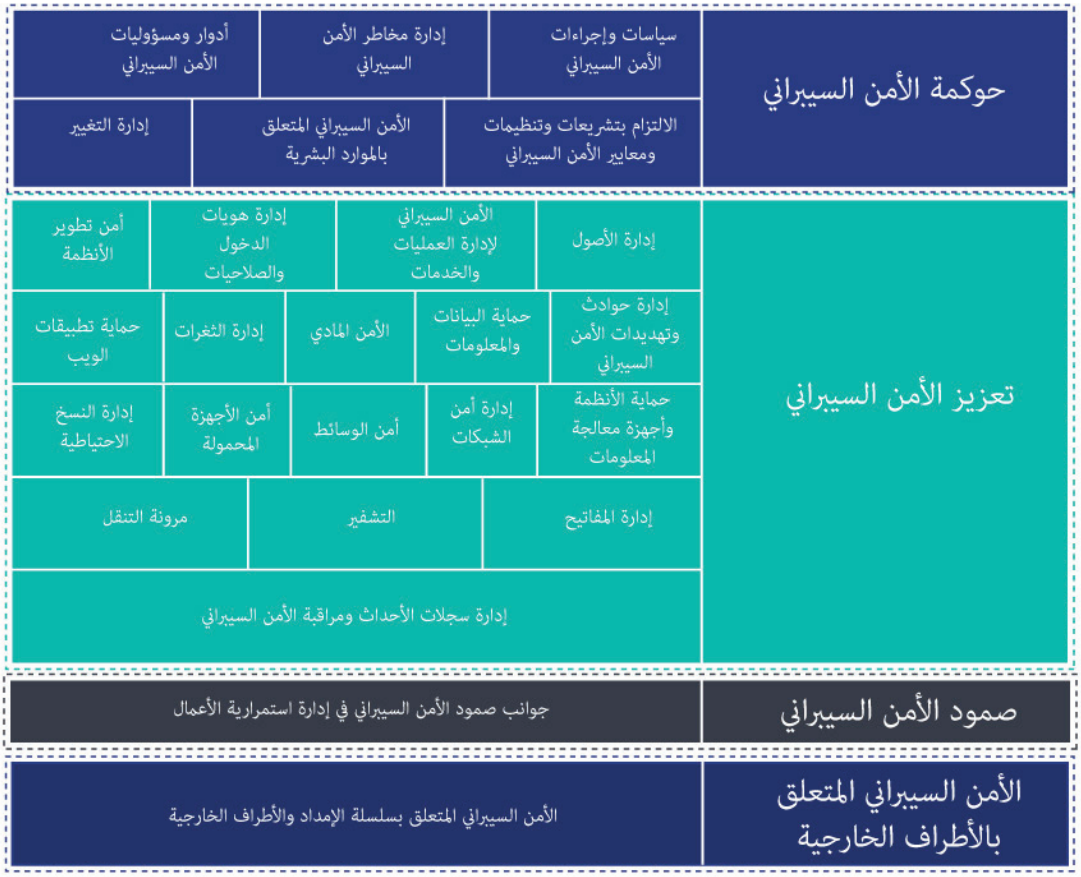
تتماشى المكونات الأساسية والفرعية لضوابط الأمن السيبراني للحوسبة السحابية مع المكونات الأساسية والفرعية للضوابط الأساسية للأمن السيبراني. وضوابط الأمن السيبراني للحوسبة السحابية متضمنة في أربعة مكونات أساسية وتضيف ستة مكونات فرعية إضافية للمجالات ذات الصلة بخدمات الحوسبة السحابية (كما يتضح باللون الأزرق الغامق في الشكل ٣)، بالإضافة إلى عشرين مكون فرعي في الضوابط الأساسية للأمن السيبراني تم إضافة لها ضوابط خاصة بالحوسبة السحابية (كما يتضح باللون الأبيض في الشكل ٣). وتم حذف المكون الأساسي الخامس (الأمن السيبراني لأنظمة التحكم الصناعي "ICS") بسبب عدم انطباقه على الحوسبة السحابية في الوقت الحالي. كما ثمة ثمانية مكونات فرعية للضوابط الأساسية للأمن السيبراني لا تضم ضوابط محدَّدة تخص الحوسبة السحابية، ولا تمثل جزءًا من ضوابط الأمن السيبراني للحوسبة السحابية (كما يتضح باللون الرمادي في الشكل ٣).



شكل ٣: علاقة المكونات الأساسية والفرعية لضوابط الأمن السيبراني للحوسبة السحابية مع الضوابط الأساسية للأمن السيبراني

هيكلية المكونات الأساسية والفرعية لضوابط الأمن السيبراني للحوسبة السحابية:

ونتيجة لما سبق، تتكون ضوابط الأمن السيبراني للحوسبة السحابية من المكونات الأساسية والفرعية التالية:



شكل ٤: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للحوسبة السحابية

مواءمة المكونات الفرعية مع المعايير الدولية

عند وجود أي اختلافات ما بين مكونات هذه الضوابط مع المعايير العالمية الخمسة، فإن ماهو مذكور في هذه الضوابط هو المعتبر به.

المكونات الأساسية	المكونات الفرعية		مقارنة مكونات الأطر				
			ISO 27K	المعيار الأمريكي الفيدرالي FedRAMP	معيار CCM	معيار الحكومة الألمانية C5 (DE)	معايير الأمن السحابي في سنغافورة MTCS (SGP)
حوكمة الأمن السيبراني	١-١	سياسات وإجراءات الأمن السيبراني	A.5		GRM/RM	2 - SA	6
	١-٢	إدارة مخاطر الأمن السيبراني	6.1	RA	GRM/G		8
	١-٣	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني	A.18		AAC	16 - COM	10
	١-٤	أدوار ومسؤوليات الأمن السيبراني	A.6.1	AU		1 - OIS	
	١-٥	الأمن السيبراني المتعلق بالموارد البشرية	A.7	PS AT	HRS	3 - HR	7
	١-٦	إدارة التغيير	A.12				19
تعزيز الأمن السيبراني	٢-١	إدارة الأصول	A.8.1	CM MA	ضوابط الأمن السيبراني للحوسبة السحابية CCC	4 -AM	20 14
	٢-٢	الأمن السيبراني لإدارة العمليات والخدمات	A.12			6 - RB	19
	٢-٣	إدارة سجلات الأحداث ومراقبة الأمن السيبراني		AU CA		15-SPN	13 15
	٢-٤	أمن تطوير الأنظمة	A.14	SA		11- BEI	16
	٢-٥	إدارة حوادث وتهديدات الأمن السيبراني	A.16	IR	SEF	13-SIM	11

تعزيز الأمن السيبراني	٢-٦	حماية البيانات والمعلومات	A.8.2		DSI		12
	٢-٧	إدارة هويات الدخول والصلاحيات	A.9	AC	IAM	7-IDM	23
				IA			
	٢-٨	إدارة الثغرات			TVM		
	٢-٩	حماية الأنظمة وأجهزة معالجة المعلومات		SC	AIS		22
				SI	IVS		4
	٢-١٠	إدارة أمن الشبكات	A.13	SC		9 -KOS	
			A.13	SC			
	٢-١١	أمن الوسائط	A.8.3	MP			
	٢-١٢	حماية تطبيقات الويب					
	٢-١٣	أمن الأجهزة المحمولة	A.6.2		MOS	17 – MDM	
	٢-١٤	إدارة النسخ الاحتياطية					
	٢-١٥	إدارة المفاتيح	A.10		EKM	8 -KRY	17
	٢-١٦	التشفير	A.10		EKM	8 -KRY	
	٢-١٧	مرونة التنقل			IPY	10 - PI	
	٢-١٨	الأمن المادي	A.11	PE	DCS	5 - PS	18
صمود الأمن السيبراني	٣-١	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال	A.17	CP	BCR	14 -BCM	21
الأمن السيبراني المتعلق بالأطراف الخارجية	٤-١	الأمن المتعلق بسلسلة الإمداد والأطراف الخارجية	A.15	SA	SCM	12-DLL	9

جدول ١. مواءمة المكونات الفرعية مع المعايير الدولية

مواءمة الضوابط مع المعايير الدولية

عند وجود أي اختلافات ما بين هذه ضوابط مع المعايير العالمية الخمسة، فإن ما هو مذكور في هذه الضوابط هو المعتبر به.

يرجى ملاحظة أن "خاص" في خانة المعايير تعني أن الضابط ليس مذكورًا في أي من المعايير العالمية الخمسة.

١ حوكمة الأمن السيبراني

رقم المكون الفرعي	المكون الفرعي	رقم الضابط لمقدم الخدمات	رقم الضابط للمشترك	المعايير	المعايير الأخرى
CCC-1-1	سياسات وإجراءات الأمن السيبراني	١-١-م-١-١		C5 SA-03	
CCC-1-2	إدارة مخاطر الأمن السيبراني	١-٢-م-١-١	١-٢-ش-١-١	CCM GRM-11	
		١-٢-م-١-٢	١-٢-ش-١-٢	CCM GRM-02	
		١-٢-م-١-٣	١-٢-ش-١-٣	MTCS 8.4	
		١-٢-م-١-٤	١-٢-ش-١-٤	CCM GRM-08	
CCC-1-3	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني	١-٣-م-١-١		ISO27K A.18.1.1	ISO27K, A.18.1.1, MTCS 10.1, C5 COM-01, CCM-BCR-11, CCM-AAC-03
			١-٣-ش-١-١	ISO27K A.18.1.2	
		١-٣-م-١-٢		ISO27K A.18.1.3	
		١-٣-م-١-٣		ISO27K A.18.1.4	
		١-٣-م-١-٤		MTCS 10.4	ISO27K A.18.1.5
		١-٣-م-١-٥		MTCS 10.5	
			١-٣-ش-١-٢	MTCS 10.6	

CCC-1-4	أدوار ومسؤوليات الأمن السيبراني	١-٤-م-١-١	١-٤-ش-١-١	C5-OIS-02, C5-OIS-03	ISO27K - A.6.1.1
		١-٤-م-١-٢		C5-OIS-05	ISO27K - A.6.1.4
		١-٤-م-٢-٢		ISO27K - A.6.1.3	
CCC-1-5	الأمن السيبراني المتعلق بالموارد البشرية	١-٥-م-١-١		FR PS-2	
		١-٥-م-١-٢	١-٥-ش-١-١	MTCS 7.2	
		١-٥-م-١-٣		MTCS 7.4	C5 HR-04; ISO27K A.7.1.5; FR PS-8;
		١-٥-م-١-٤		FR PS-6	
		١-٥-م-٢-١		FR PS-4	
		١-٥-م-٢-٢		MTCS 7.5	CCM HRS-01
CCC-1-6	إدارة التغيير	١-٦-م-٣-١		FR-CM-3	CCM- CCC-05
		١-٦-م-٣-٢		C5- BEI-07, C5-BEI-08, C5-BEI-09	
		١-٦-م-٣-٣		C5- BEI-10	
		١-٦-م-٣-٤	١-٦-ش-٣-١	FR-CM-4	
		١-٦-م-٣-٥		FR-CM-7	
		١-٦-م-٣-٦		CCM- CCC-04	

٢ تعزيز الأمن السيبراني

رقم المكون الفرعي	المكون الفرعي	رقم الضابط لمقدم الخدمات	رقم الضابط للمشترك	المرجع المعياري	المعايير الأخرى
CCC-2-1	إدارة الأصول	٢-١-م-١-١		ISO27K A.8.1.1	
		٢-١-م-١-٢		ISO27K A.8.1.2	
CCC-2-2	الأمن السيبراني لإدارة العمليات والخدمات	٢-٢-م-١		MTCS-19.3	
		٢-٢-م-٣-١		MTCS-19.3	
		٢-٢-م-٣-٢	٢-٢-ش-٣-١	MTCS-19.1, MTCS-19.2	
		٢-٢-م-٣-٣		FR-CM-2	
		٢-٢-م-٣-٤		MTCS-19.4	
		٢-٢-م-٣-٥		FR-PL-8	
CCC-2-3	إدارة سجلات الأحداث ومراقبة الأمن السيبراني	٢-٣-م-١-١		MTCS 13.3	
		٢-٣-م-١-٢		MTCS 13.4	
		٢-٣-م-١-٣		C5-RB-15	
		٢-٣-م-١-٤		MTCS 13.4	
		٢-٣-م-١-٥		FR- SI-04	MTCS 13.2
		٢-٣-م-١-٦		MTCS 13.2	
		٢-٣-م-١-٧		C5-RB-16	
		٢-٣-م-١-٨		C5-RB-11	
		٢-٣-م-١-٩		FR AC-17 (1)	
		٢-٣-م-١-١٠	٢-٣-ش-١-٣	ISO27K A.12.4.3	

CCC-2-4	أمن تطوير الأنظمة	٢-٤-م-٣-١		FR-SA-03	
		٢-٤-م-٣-٢		C5-BEI-01	
		٢-٤-م-٣-٣	٢-٤-ش-٣-١	ISO27K A.14.1.1	
		٢-٤-م-٣-٤	٢-٤-ش-٣-٢	ISO27K A.14.2.8	
		٢-٤-م-٣-٥		FR-SA-05	
		٢-٤-م-٣-٦		ISO27K A.14.2.6	
		٢-٤-م-٣-٧		MTCS 16.4	
		٢-٤-م-٣-٨		CCM-CCC-02	
		٢-٤-م-٣-٩		MTCS-16.5	
		٢-٤-م-٣-١٠		ISO27K A.14.3.1	
CCC-2-5	إدارة حوادث وتهديدات الأمن السيبراني		٢-٥-ش-١-١	FR-IR-06	MTCS-11.3
		٢-٥-م-١-١		MTCS-11.1	FR-IR-08
		٢-٥-م-١-٢		FR-IR-02	
		٢-٥-م-١-٣		FR-IR-09	
		٢-٥-م-١-٤		MTCS-11.4	
		٢-٥-م-١-٥		CCM-SEF-04	
		٢-٥-م-١-٦	٢-٥-ش-١-٤	C5-SIM-06	
		٢-٥-م-١-٧	٢-٥-ش-١-٢	FR-IR-07	
		٢-٥-م-١-٨	٢-٥-ش-١-٣	CCM-SEF-05	
		٢-٥-م-١-٩	٢-٥-ش-١-٥	MTCS-11.2	
CCC-2-6	حماية البيانات والمعلومات	٢-٦-م-١-١	٢-٦-ش-١-١	CCM-DSI-02	
		٢-٦-م-١-٢	٢-٦-ش-١-٢	MTCS-12.10	
		٢-٦-م-١-٣		CCM-DSI-05	
		٢-٦-م-١-٤		MTCS-12.6	
		٢-٦-م-١-٥		خاص	
		٢-٦-م-١-٦	٢-٦-ش-١-٣	خاص	
		٢-٦-م-١-٧		FR SA-09 (5)	

CCC-2-7	إدارة هويات الدخول والصلاحيات	٢-٧-م-١-١		C5-IDM-08	
		٢-٧-م-١-٢	٢-٧-ش-١-١	CCM- IAM-12	
		٢-٧-م-١-٣	٢-٧-ش-١-٢	C5- IDM-07	
		٢-٧-م-١-٤	٢-٧-ش-١-٣	C5-IDM- 08	
		٢-٧-م-١-٥	٢-٧-ش-١-٤	FR IA-2 (1)	
		٢-٧-م-١-٦	٢-٧-ش-١-٥	MTCS-23.4	FR-AC-7
		٢-٧-م-١-٧		FR-AC-18	
		٢-٧-م-١-٨		CCM-IAM-07	
		٢-٧-م-١-٩		CCM-DCS-03	
		٢-٧-م-١-١٠		C5-IAM-12	
		٢-٧-م-١-١١		FR IA-06	
		٢-٧-م-١-١٢		FR AC-08	
		٢-٧-م-١-١٣		FR AC-17 (9)	
		٢-٧-م-١-١٤		FR IA-05 (2)	
CCC-2-8	إدارة الثغرات	٢-٨-م-١-٣		MTCS-24.4	CCM-IVS-05
		٢-٨-م-١-٤	٢-٨-ش-١-١	MTCS-15.1	
		٢-٨-م-١-٥	٢-٨-ش-١-٢	C5-RB-20	
CCC-2-9	حماية الأنظمة وأجهزة معالجة المعلومات	٢-٩-م-١-١		FR- SI-01, FR-SC-01	
		٢-٩-م-١-٢		CCM-IVS-02	
		٢-٩-م-١-٣		MTCS-14.9	
		٢-٩-م-١-٤		FR-SC-02	
		٢-٩-م-١-٥		FR-SI-02	CCM-IVS-09
		٢-٩-م-١-٦		FR SC-24, FR-SI-10, FR- SI-11, FR- SI-16	
		٢-٩-م-١-٧		CCM IVS-04	
		٢-٩-م-١-٨		MTCS-19.5	ISO27K A.17.2.1
		٢-٩-م-١-٩		FR-SC-06	
		٢-٩-م-١-١٠		FR SC-03	
		٢-٩-م-١-١١		FR-SI-06	
		٢-٩-م-١-١٢		FC- SC-18	CCM-TVM-03
		٢-٩-م-١-١٣		FR- SI-7	
		٢-٩-م-١-١٤		MTCS-24.1	
		٢-٩-م-١-١٥		FR- SC-39	C5-KOS-05
		٢-٩-م-١-١٦		FR- SC-6 (لأنظمة الحوسبة فقط)	
		٢-٩-م-١-١٧		MTCS-24.6	
		٢-٩-م-١-١٨		MTCS-24.5	

CCC-2-10	إدارة أمن الشبكات	٢-١٠-م-١-١		CCM IVS-13	C5 KOS-06
		٢-١٠-م-١-٢		FR SC-07	
		٢-١٠-م-١-٣		FR SC-05	
		٢-١٠-م-١-٤		FR SC-08	
		٢-١٠-م-١-٥		C5 KOS-03	
		٢-١٠-م-١-٦		FR SC-06 (التواصل فقط)	
		٢-١٠-م-١-٧		خاص	خاص
		٢-١٠-م-١-٨		C5-KOS-05	ISO27K A.13.1.3
		٢-١٠-م-١-٩		MTCS-24.2	C5-KOS-04
		٢-١٠-م-١-١٠			FR SI-4 (11) (18) (22)
		٢-١٠-م-١-١١		FR-SI-04(1)	
CCC-2-11	أمن الوسائط	٢-١١-م-٣-١		FR-MP-6	
		٢-١١-م-٣-٢		MTCS-12.8	CCM-DSI-07
		٢-١١-م-٣-٣		ISO27K A.8.3.1	
		٢-١١-م-٣-٤		FR-MP-3	
		٢-١١-م-٣-٥		FR-MP-4	
		٢-١١-م-٣-٦		FR-MP-7	
CCC-2-12	حماية تطبيقات الويب	٢-١٢-م-١-١		ISO27K A.14.1.2, ISO27K A.14.1.3	
CCC-2-13	أمن الأجهزة المحمولة	٢-١٣-م-١-١		CCM, MOS-09	
		٢-١٣-م-١-٢		CCM, MOS-10	
		٢-١٣-م-١-٣		CCM, MOS-16	
		٢-١٣-م-١-٤		CCM, MOS-19	
		٢-١٣-م-١-٥		خاص	
		٢-١٣-م-١-٦	٢-١٢-ش-١-١	خاص	
		٢-١٣-م-١-٧	٢-١٢-ش-١-٢	خاص	
		٢-١٣-م-١-٨		FR SC-15	
		٢-١٣-م-١-٩		FR MA-3	
CCC-2-14	إدارة النسخ الاحتياطية	٢-١٤-م-١-١		FR CP-10 (4)	CCM BCR-11
CCC-2-15	إدارة المفاتيح	٢-١٥-م-٣-١	٢-١٥-ش-٣-١	CCM-EKM-01	
		٢-١٥-م-٣-٢	٢-١٥-ش-٣-٢	CCM-EKM-04	
		٢-١٥-م-٣-٣	٢-١٥-ش-٣-٣	خاص	
		٢-١٥-م-٣-٤	٢-١٥-ش-٣-٤	FR SC-12 (1)	

CCC-2-16	التشفير	٢-١٦-م-١-١	٢-١٦-ش-١-١	C5 KRY-02 (المتطلبات الأساسية فقط)	MTCS 17.2
		٢-١٦-م-١-٢		FR SC-17	
			٢-١٦-ش-١-٢	FC-SC-28(1)	
CCC-2-17	مرونة التنقل	٢-١٧-م-٣-١	٢-١٧-ش-٣-١	C5-PI-03	
		٢-١٧-م-٣-٢	٢-١٧-ش-٣-٢	CCM-IPY-01	C5-PI-01
		٢-١٧-م-٣-٣	٢-١٧-ش-٣-٣	CCM-IPY-04	
		٢-١٧-م-٣-٤	٢-١٧-ش-٣-٤	CCM-IPY-02	
		٢-١٧-م-٣-٥		CCM-IPY-05	
CCC-2-18	الأمن المادي	٢-١٨-م-١-١		FR-PE-06	
		٢-١٨-م-١-٢		FR-PE-08	MTCS-18,4
		٢-١٨-م-١-٣		FR-PE-04	
		٢-١٨-م-١-٤		FR-PE-05	
		٢-١٨-م-١-٥		CCM-DCS-01	
		٢-١٨-م-١-٦		FR-PE-12	
		٢-١٨-م-١-٧		FR-PE-10	
		٢-١٨-م-١-٨		FR-PE-13	
		٢-١٨-م-١-٩		C5-PS-03	
		٢-١٨-م-١-١٠		FR PE-15	
		٢-١٨-م-١-١١		C5-PS-04	
		٢-١٨-م-١-١٢		FR-PE-11 (1)	
		٢-١٨-م-١-١٣		FR CP-8	
		٢-١٨-م-١-١٤		CCM BCR-06	
		٢-١٨-م-١-١٥		CCM BCR-07	C5-PS-05
		٢-١٨-م-١-١٦		خاص	
		٢-١٨-م-١-١٧		CCM-DCS-01	
		٢-١٨-م-١-١٨		MTCS-18.2	CCM-DCS-04
		٢-١٨-م-١-١٩		ISO27K A.11.1.6	
		٢-١٨-م-١-٢٠		CCM-DCS-05	
		٢-١٨-م-١-٢١		FR-PR 14 (1) (2)	CCM BCR-03
		٢-١٨-م-١-٢٢		FR-PE-09	

٣ صمود الأمن السيبراني

رقم المكون الفرعي	المكون الفرعي	رقم الضابط لمقدم الخدمات	رقم الضابط للمشترك	المرجع المعياري	المعايير الأخرى
CCC-3-1	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال	٣-١-م-١-١	٣-١-ش-١-١	FR CP-2 (4)	
		٣-١-م-١-٢		C5 BCM-02	
		٣-١-م-١-٣	٣-١-ش-١-٢	FR CP-3	
		٣-١-م-١-٤		FR CP-4	
		٣-١-م-١-٥		FR CP-7 (1) (2) (3) (4)	
		٣-١-م-١-٦		FR PE-17	
		٣-١-م-١-٧		FR CP-6	

٤ الأمن السيبراني المتعلق بالأطراف الخارجية

رقم المكون الفرعي	المكون الفرعي	رقم الضابط لمقدم الخدمات	رقم الضابط للمشترك	المرجع المعياري	المعايير الأخرى
CCC-4-1	الأمن السيبراني المتعلق بسلسلة الإمداد والأطراف الخارجية	٤-١-م-١-١		MTCS-9.1, MTCS-9.2 CCM-STA-06, CCM-STA-08, CCM-STA-09	
		٤-١-م-١-٢		FR-SA-05	
		٤-١-م-١-٣	٤-١-ش-١-١	CCM-STA-01	
		٤-١-م-١-٤		C5-DDL-02	
		٤-١-م-١-٥		CCM-STA-06	

جدول ٢. مواءمة الضوابط مع المعايير الدولية

مواءمة المكونات الفرعية للضوابط الأساسية للأمن السيبراني مع ضوابط الأمن السيبراني للحوسبة السحابية

المكونات الأساسية	المكونات الفرعية للضوابط الأساسية للأمن السيبراني		المكونات الفرعية لضوابط الأمن السيبراني للحوسبة السحابية	
حوكمة الأمن السيبراني	١-١	إستراتيجية الأمن السيبراني Cybersecurity Strategy		
	١-٢	إدارة الأمن السيبراني Cybersecurity Management		
	١-٣	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	١-١	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures
	١-٤	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities	١-٤	أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities
	١-٥	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	١-٢	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management
	١-٦	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects		
	١-٧	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Compliance with Cybersecurity Standards, Laws and Regulations	١-٣	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Compliance with Cybersecurity Standards, Laws and Regulations
	١-٨	المراجعة والتقييم الدوري للأمن السيبراني Cybersecurity Periodical Assessment and Audit		
	١-٩	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	١-٥	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources
	١-١٠	برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program		

تعزيز الأمن السيبراني	٢-١	إدارة الأصول Asset Management	١-٢	إدارة الأصول Asset Management
			٢-٢	الأمن السيبراني لإدارة العمليات والخدمات Operations and service Management Cybersecurity
	٢-٢	إدارة هويات الدخول والصلاحيات Identity and Access Management	٧-٢	إدارة هويات الدخول والصلاحيات Identity and Access Management
	٢-٣	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Information Processing Facilities Protection	٩-٢	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Information Processing Facilities Protection
	٢-٤	حماية البريد الإلكتروني Email Protection		
	٢-٥	إدارة أمن الشبكات Network Security Management	١٠-٢	إدارة أمن الشبكات Network Security Management
	٢-٦	أمن الأجهزة المحمولة Mobile Device Security	١٣-٢	أمن الأجهزة المحمولة Mobile Device Security
			١١-٢	أمن الوسائط Media Security
	٢-٧	حماية البيانات والمعلومات Data and Information Protection	٦-٢	حماية البيانات والمعلومات Data and Information Protection
			٤-٢	أمن تطوير الأنظمة System Development Security
	٢-٨	التشفير Cryptography	١٦-٢	التشفير Cryptography
	٢-٩	إدارة النسخ الاحتياطية Backup and Recovery Management	١٤-٢	إدارة النسخ الاحتياطية Backup and Recovery Management
	٢-١٠	إدارة الثغرات Vulnerability Management	٨-٢	إدارة الثغرات Vulnerability Management
	٢-١١	اختبار الاختراق Penetration Testing		
	٢-١٢	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	٣-٢	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management
	٢-١٣	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	٥-٢	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management
	٢-١٤	الأمن المادي Physical Security	١٨-٢	الأمن المادي Physical Security
	٢-١٥	حماية تطبيقات الويب Web Application Security	١٢-٢	حماية تطبيقات الويب Web Application Security
			١٥-٢	إدارة المفاتيح Key Management
			١٧-٢	مرونة التنقل Interoperability

صمود الأمن السيبراني	١-٣	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	١-٣
الأمن السيبراني المتعلق بالأطراف الخارجية	١-٤	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	١-٤

جدول ٣. مواءمة المكونات الفرعية للضوابط الأساسية مع ضوابط الأمن السيبراني للحوسبة السحابية

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority