



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

ملحق المنهجية والمواءمة لضوابط الأمن السيبراني للحوسبة السحابية

Cloud Cybersecurity Controls Methodology and Mapping Annex

(CCC - 1 : 2020)

إشارة المشاركة: أبيض
تصنيف الوثيقة: متاح

بسم الله الرحمن الرحيم

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 أو 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

جدول المحتويات

٦	مبادئ تصميم ضوابط الأمن السيبراني للحوسبة السحابية
٧	العلاقة بالمعايير الدولية الأخرى
٨	منهجية تصميم ضوابط الأمن السيبراني للحوسبة السحابية
٩	مكونات وهيكلية ضوابط الأمن السيبراني للحوسبة السحابية
١١	مواءمة المكونات الفرعية مع المعايير الدولية
١٣	مواءمة الضوابط مع المعايير الدولية
٢٠	مواءمة المكونات الفرعية للضوابط الأساسية للأمن السيبراني مع ضوابط الأمن السيبراني للحوسبة السحابية
٢٣	قابلية تطبيق ضوابط الأمن السيبراني للحوسبة السحابية على النماذج الثلاثة

قائمة الأشكال والرسوم التوضيحية

٦	شكل ١: ضوابط الأمن السيبراني للحوسبة السحابية كامتداد للضوابط الأساسية للأمن السيبراني
٨	شكل ٢: المعايير الدولية المتعلقة بالحوسبة السحابية التي تم المواءمة معها
٩	شكل ٣: علاقة المكونات الأساسية والفرعية لضوابط الأمن السيبراني للحوسبة السحابية مع الضوابط الأساسية للأمن السيبراني
١٠	شكل ٤: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للحوسبة السحابية

قائمة الجداول

١٢	جدول ١. مواءمة المكونات الفرعية مع المعايير الدولية
١٩	جدول ٢. مواءمة الضوابط مع المعايير الدولية
٢٢	جدول ٣. مواءمة المكونات الفرعية للضوابط الأساسية مع ضوابط الأمن السيبراني للحوسبة السحابية
٣١	جدول ٤. قابلية تطبيق ضوابط مقدم الخدمة على النماذج الثلاثة
٣٣	جدول ٥. قابلية تطبيق ضوابط المشترك على النماذج الثلاثة

مبادئ تصميم ضوابط الأمن السيبراني للحوسبة السحابية

طورت ضوابط الأمن السيبراني للحوسبة السحابية لتكون امتداداً للضوابط الأساسية للأمن السيبراني (ECC – 1: 2018)؛ لتوفير ضوابط لكل من مقدمي الخدمات والمستخدمين. ويجب أن يلتزم كل من مقدمي الخدمات والمستخدمين بالضوابط الأساسية للأمن السيبراني أولاً، ثم الضوابط الإضافية المنصوص عليها في وثيقة ”ضوابط الأمن السيبراني للحوسبة السحابية“، وبتعبير آخر، يُعدّ تحقيق الالتزام بالضوابط الأساسية للأمن السيبراني شرطاً مسبقاً 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 تكون المتطلبات الأمنية في هذه الوثيقة امتداداً للضوابط الأساسية للأمن السيبراني.
- أن يكون مستوى الأمن السيبراني مقارباً لنظيره من المعايير الدولية ذات العلاقة بالحوسبة السحابية (مثل المعيار الأمريكي (FedRAMP)، ومعيار الأمن السحابي في سنغافورة (MTCS SS)، ومعيار Cloud Controls Matrix (CCM)، ومعيار (ISO/IEC 27001).
- أن يكون هناك إشارة إلى مدى التوافق مع المعايير العالمية ذات العلاقة.
- بالنسبة إلى المستخدمين، فقد تم تطبيق المبادئ التالية:
- أن تكون المتطلبات الأمنية في هذه الوثيقة امتداداً للضوابط الأساسية للأمن السيبراني.

العلاقة بالمعايير الدولية الأخرى

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

- معايير ISO/IEC 27001.
- المعيار الأمريكي FedRAMP (FR).
- ضوابط Cloud Controls Matrix (CCM) الصادرة من تحالف أمن الحوسبة السحابية Cloud Security Alliance (CSA).
- المعيار الألماني Cloud Computing Compliance Control Catalogue (C5).
- معايير الأمن السحابي في سنغافورة (Multi-Tier Cloud Security Standard for Singapore (MTCS SS)).

منهجية تصميم ضوابط الأمن السيبراني للحوسبة السحابية

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

وخلال تطوير ضوابط الأمن السيبراني للحوسبة السحابية، تم إعداد قائمة موحدة من المتطلبات الأمنية في المجالات ذات الصلة من خمسة معايير مرجعية في مجال الأمن السيبراني للحوسبة السحابية (المذكورة في قسم "العلاقة بالمعايير الدولية الأخرى") لتشكيل مجموعة مدمجة من ضوابط الحوسبة السحابية.



شكل ٢: المعايير الدولية المتعلقة بالحوسبة السحابية التي تم المواءمة معها

مكونات وهيكلية ضوابط الأمن السيبراني للحوسبة السحابية

العلاقة مع الضوابط الأساسية للأمن السيبراني

تتماشى المكونات الأساسية والفرعية لضوابط الأمن السيبراني للحوسبة السحابية في وثيقة ضوابط الأمن السيبراني للحوسبة السحابية مع المكونات الأساسية والفرعية للضوابط الأساسية للأمن السيبراني. وضوابط الأمن السيبراني للحوسبة السحابية متضمنة في أربعة مكونات أساسية وتضيف أربعة 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) بسبب عدم انطباقه على الحوسبة السحابية في الوقت الحالي. كما ثمة ثمانية مكونات فرعية للضوابط الأساسية للأمن السيبراني لا تضم ضوابط محددة تخص الحوسبة السحابية، ولا تمثل جزءاً من ضوابط الأمن السيبراني للحوسبة السحابية (كما يتضح باللون الرمادي في الشكل ٣).

حوكمة الأمن السيبراني	استراتيجية الأمن السيبراني	إدارة الأمن السيبراني	سياسات وإجراءات الأمن السيبراني	أدوار ومسؤوليات الأمن السيبراني	إدارة مخاطر الأمن السيبراني
	الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني	المراجعة والتدقيق الدوري للأمن السيبراني	الأمن السيبراني المتعلق بالموارد البشرية	برنامج التوعية والتدريب بالأمن السيبراني
تعزيز الأمن السيبراني	إدارة الأصول	إدارة هويات الدخول والصلاحيات	حماية الأنظمة وأجهزة معالجة المعلومات	حماية البريد الإلكتروني	إدارة أمن الشبكات
	أمن الأجهزة المحمولة	حماية البيانات والمعلومات	التشفير	إدارة النسخ الاحتياطية	إدارة الثغرات
	اختيار الاختراق	إدارة سجلات الأحداث ومراقبة الأمن السيبراني	إدارة حوادث وتهديدات الأمن السيبراني	الأمن المادي	
	حماية تطبيقات الويب	إدارة المفاتيح	أمن تطوير الأنظمة		
أمن وسائط التخزين					
صمود الأمن السيبراني	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال				
الأمن السيبراني المتعلق بالأطراف الخارجية	الأمن السيبراني المتعلق بالأطراف الخارجية				
	الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة				
	مكونات فرعية أضيف لها ضوابط خاصة بالحوسبة السحابية	مكونات فرعية لم يصف لها ضوابط خاصة بالحوسبة السحابية	مكونات فرعية خاصة بضوابط الأمن السيبراني للحوسبة السحابية		

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:

حوكمة الأمن السيبراني		أدوار ومسؤوليات الأمن السيبراني		إدارة مخاطر الأمن السيبراني	
الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني		الأمن السيبراني المتعلق بالموارد البشرية		إدارة التغيير	
إدارة الأصول	إدارة هويات الدخول والصلاحيات	حماية الأنظمة وأجهزة معالجة المعلومات	إدارة أمن الشبكات		
أمن الأجهزة المحمولة		حماية البيانات والمعلومات	التشفير	إدارة النسخ الاحتياطية	
إدارة الثغرات	اختبار الاختراق	إدارة سجلات الأحداث ومراقبة الأمن السيبراني	إدارة حوادث وتهديدات الأمن السيبراني		
الأمن المادي		حماية تطبيقات الويب	إدارة المفاتيح		
أمن تطوير الأنظمة		أمن وسائط التخزين			
جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال					
صمود الأمن السيبراني					
الأمن السيبراني المتعلق بالأطراف الخارجية					
الأمن السيبراني المتعلق بسلسلة الإمداد والأطراف الخارجية					

شكل ٤: المكونات الأساسية والفرعية لضوابط الأمن السيبراني للحوسبة السحابية

مواءمة المكونات الفرعية مع المعايير الدولية

عند وجود أي اختلافات ما بين مكونات ضوابط الأمن السيبراني للحوسبة السحابية مع المعايير العالمية الخمسة، فإن ما هو مذكور في وثيقة ضوابط الأمن السيبراني للحوسبة السحابية هو المعتمد به.

المكونات الأساسية	المكونات الفرعية		مقارنة مكونات المعايير				
			معيار ISO27001	المعيار الأمريكي FedRAMP (FR)	معيار CCM	معيار C5	معايير الأمن السحابي في سنغافورة MTCS SS
حوكمة الأمن السيبراني	١-١	أدوار ومسؤوليات الأمن السيبراني	A.6.1	AU		OIS - 1	
	٢-١	إدارة مخاطر الأمن السيبراني	6.1	RA	GRM/G		8
	٣-١	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني	A.18		AAC	16 - COM	10
	٤-١	الأمن السيبراني المتعلق بالموارد البشرية	A.7	PS AT	HRS	3 - HR	7
	٥-١	الأمن السيبراني ضمن إدارة التغيير	A.12			6 - RB	19
	١-٢	إدارة الأصول	A.8.1	CM MA		4 - AM	20 14
تعزيز الأمن السيبراني	٢-٢	إدارة هويات الدخول والصلاحيات	A.9	AC IA	IAM	7 - IDM	23
	٣-٢	حماية الأنظمة وأجهزة معالجة المعلومات		SC SI	AIS IVS		22 4
	٤-٢	إدارة أمن الشبكات	A.13	SC		9 - KOS	
	٥-٢	أمن الأجهزة المحمولة	A.6.2		MOS	17 - MDM	
	٦-٢	حماية البيانات والمعلومات	A.8.2		DSI		12
	٧-٢	التشفير	A.10		EKM	8 - KRY	17
	٨-٢	إدارة النسخ الاحتياطية					
	٩-٢	إدارة الثغرات			TVM		
	١٠-٢	اختبار الاختراق		CA		18 - RB	15
	١١-٢	إدارة سجلات الأحداث ومراقبة الأمن السيبراني	A.12.4	AU CA		15 - SPN	13 15
	١٢-٢	إدارة حوادث وتهديدات الأمن السيبراني	A.16	IR	SEF	13 - SIM	11
	١٣-٢	الأمن المادي	A.11	PE	DCS	5 - PS	18
	١٤-٢	حماية تطبيقات الويب					
	١٥-٢	إدارة المفاتيح	A.10		EKM	8 - KRY	17
	١٦-٢	أمن تطوير الأنظمة	A.14	SA		11 - BEI	16
	١٧-٢	أمن وسائط التخزين	A.8.3	MP			

المكونات الأساسية	المكونات الفرعية		مقارنة مكونات المعايير				
			معايير الأمن السحابي في سنغافورة MTCS SS	معايير C5	معايير CCM	المعايير الأمريكي FedRAMP (FR)	معايير ISO27001
صمود الأمن السيبراني	١-٣	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال	21	14 - BCM	BCR	CP	A.17
الأمن السيبراني المتعلق بالأطراف الخارجية	١-٤	الأمن المتعلق بسلسلة الإمداد والأطراف الخارجية	9	12 - DLL	SCM	SA	A.15

جدول ١. مواءمة المكونات الفرعية مع المعايير الدولية

مواءمة الضوابط مع المعايير الدولية

عند وجود أي اختلافات ما بين ضوابط الأمن السيبراني للحوسبة السحابية مع المعايير العالمية الخمسة، فإن ما هو مذكور في وثيقة ضوابط الأمن السيبراني للحوسبة السحابية هو المعتبر به.

يرجى ملاحظة أن "خاص" في خانة المعايير تعني أن الضابط ليس مذكورًا في أي من المعايير العالمية الخمسة، وتم تطويره من قبل الهيئة.

حوكمة الأمن السيبراني (Cybersecurity Governance)



المعيار الأخرى	المعايير	رقم الضابط للمشترك	رقم الضابط لمقدم الخدمات	المكون الفرعي	رقم المكون الفرعي
ISO27001 - A.6.1.1	C5-OIS-02, C5- OIS-03	١-١-ش-١-١	١-١-م-١-١	أدوار ومسؤوليات الأمن السيبراني	١-١
	CCM GRM-11	١-١-ش-٢-١	١-١-م-٢-١	إدارة مخاطر الأمن السيبراني	٢-١
	CCM GRM-02	٢-١-ش-٢-١	٢-١-م-٢-١		
	MTCS SS 8.4	٣-١-ش-٢-١	٣-١-م-٢-١		
MTCS SS 10.1, C5 COM-01, CCM- BCR-11, CCM- AAC-03	ISO27001 A.18.1.1		١-١-م-٣-١	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني	٣-١
	MTCS SS 10.6	١-١-ش-٣-١			
	خاص		١-١-م-٤-١	الأمن السيبراني المتعلق بالموارد البشرية	٤-١
	MTCS SS 7.2	١-١-ش-٤-١	٢-١-م-٤-١		
	FR PS-6		٣-١-م-٤-١		
CCM HRS-01	MTCS SS 7.5		١-٢-م-٤-١		
CCM- CCC-05	FR-CM-3		١-٣-م-٥-١	الأمن السيبراني ضمن إدارة التغيير	٥-١
	C5- BEI-10		٢-٣-م-٥-١		

تعزيز الأمن السيبراني (Cybersecurity Defense)



المعيار الأخرى	المعيار	رقم الضابط للمشترك	رقم الضابط لمقدم الخدمات	المكون الفرعي	رقم المكون الفرعي
	ISO27001 A.8.1.1	١-١-ش-١-٢	١-١-م-١-٢	إدارة الأصول	١-٢
	ISO27001 A.8.1.2		٢-١-م-١-٢		
	C5 - IDM-08		١-١-م-٢-٢	إدارة هويات الدخول والصلاحيات	٢-٢
	CCM - IAM-12	١-١-ش-٢-٢			
	C5 - IDM-07	٢-١-ش-٢-٢			
	C5 - IDM- 08	٣-١-ش-٢-٢	٢-١-م-٢-٢		
	FR IA-2 (1)	٤-١-ش-٢-٢	٣-١-م-٢-٢		
FR-AC-7	MTCS SS-23.4	٥-١-ش-٢-٢	٤-١-م-٢-٢		
FR-IA-5 (1)	C5 - IDM-11		٥-١-م-٢-٢		
	CCM - IAM-07		٦-١-م-٢-٢		
	C5 - IAM-12		٧-١-م-٢-٢		
	FR IA - 06		٨-١-م-٢-٢		
	C5 - IDM-03		٩-١-م-٢-٢		
	FR AC - 17 (9)		١٠-١-م-٢-٢		
	FR IA - 2 (1)		١١-١-م-٢-٢		
	MTCS SS - 24.5		١٢-١-م-٢-٢		

المعايير الأخرى	المعايير	رقم الضابط للمشترك	رقم الضابط لمقدم الخدمات	المكون الفرعي	رقم المكون الفرعي
	MTCS SS-14.9		١-١-م-٣-٢	حماية الأنظمة وأجهزة معالجة المعلومات	٣-٢
	MTCS SS-24.6		٢-١-م-٣-٢		
	FR-CM-7		٣-١-م-٣-٢		
	FR SC-24, FR- SI-10, FR- SI-11, FR- SI-16		٤-١-م-٣-٢		
	FR SC-03		٥-١-م-٣-٢		
	خاص		٦-١-م-٣-٢		
	FR- SI-7		٧-١-م-٣-٢		
	MTCS SS-24.1		٨-١-م-٣-٢		
	خاص	١-١-ش-٣-٢	٩-١-م-٣-٢		
	خاص		١٠-١-م-٣-٢		
	خاص		١١-١-م-٣-٢		
	خاص		١٢-١-م-٣-٢		
	FR SI-4 (11) (18) (22)		١-١-م-٤-٢	إدارة أمن الشبكات	٤-٢
	FR SC-07		٢-١-م-٤-٢		
	FR SC-05		٣-١-م-٤-٢		
	FR SC-08 (1)		٤-١-م-٤-٢		
	C5 KOS-03		٥-١-م-٤-٢		
C5-KOS-04	MTCS SS-24.2		٦-١-م-٤-٢		
	FR SC-08	١-١-ش-٤-٢			
	CCM, MOS-09		١-١-م-٥-٢	أمن الأجهزة المحمولة	٥-٢
	CCM, MOS-10		٢-١-م-٥-٢		
	CCM, MOS-16		٣-١-م-٥-٢		
	خاص	١-١-ش-٥-٢	٤-١-م-٥-٢		
	CCM-DSI-05		١-١-م-٦-٢	حماية البيانات والمعلومات	٦-٢
	MTCS SS-12.6		٢-١-م-٦-٢		
	MTCS SS-12.6		٣-١-م-٦-٢		
	ISO27001 A.18.1.4	١-١-ش-٦-٢	٤-١-م-٦-٢		
	C5-PI-03	٢-١-ش-٦-٢	٥-١-م-٦-٢		

المكون الفرعي	رقم المكون الفرعي	المكون الفرعي	رقم الضابط لمقدم الخدمات	رقم الضابط للمشارك	المعايير	المعايير الأخرى
٧-٢	التشفير	١-١-م-٧-٢	١-١-ش-٧-٢	خاص		
		٢-١-م-٧-٢		FR SC - 17		
			٢-١-ش-٧-٢	FR - SC - 28(1)		
٨-٢	إدارة النسخ الاحتياطية	١-١-م-٨-٢		FR CP - 10 (4)	CCM BCR-11	
		٢-١-م-٨-٢		FR CP - 10 (4)	CCM BCR-11	
٩-٢	إدارة الثغرات	١-١-م-٩-٢	١-١-ش-٩-٢	MTCS SS - 24.4	CCM-IVS-05, MTCS SS-15.1	
		٢-١-م-٩-٢	٢-١-ش-٩-٢	C5 - RB - 20		
١٠-٢	اختبار الاختراق	١-١-م-١٠-٢		FR - CA - 08		
١١-٢	إدارة سجلات الأحداث ومراقبة الأمن السيبراني	١-١-م-١١-٢		MTCS SS 13.3	MTCS SS 13.4	
		٢-١-م-١١-٢	١-١-ش-١١-٢	ISO27001 A.12.4.3		
		٣-١-م-١١-٢		C5 - RB - 15		
		٤-١-م-١١-٢		ISO27001 A.18.1.3		
		٥-١-م-١١-٢		FR - SI - 04	MTCS SS 13.2	
		٦-١-م-١١-٢	٢-١-ش-١١-٢	MTCS SS 13.2		
		٧-١-م-١١-٢		FR AC - 17 (1)		
		٨-١-م-١١-٢		C5 - RB - 11		
١٢-٢	إدارة حوادث وتهديدات الأمن السيبراني	١-١-م-١٢-٢		C5 - OIS - 05	ISO27001 - A.6.1.4	
		٢-١-م-١٢-٢		FR - IR - 02		
		٣-١-م-١٢-٢		MTCS SS - 11.2		
		٤-١-م-١٢-٢		MTCS SS - 11.4		
		٥-١-م-١٢-٢		CCM - SEF - 04		
		٦-١-م-١٢-٢		MTCS SS - 11.3		
		٧-١-م-١٢-٢		FR-IR - 07		
		٨-١-م-١٢-٢		CCM - SEF-05		
١٣-٢	الأمن المادي	١-١-م-١٣-٢		FR - PE - 06		
		٢-١-م-١٣-٢		FR - PE - 05		
		٣-١-م-١٣-٢		CCM - DCS - 05		

المعايير الأخرى	المعايير	رقم الضابط للمشترك	رقم الضابط لمقدم الخدمات	المكون الفرعي	رقم المكون الفرعي
	ISO27001 A.14.1.2, ISO27001 A.14.1.3		١-١-م-١٤-٢	حماية تطبيقات الويب	١٤-٢
	CCM - EKM - 01	١-٣-ش-١٥-٢	١-٣-م-١٥-٢	إدارة المفاتيح	١٥-٢
	CCM - EKM - 04; FR SC - 12 (1)	٢-٣-ش-١٥-٢	٢-٣-م-١٥-٢		
	ISO27001 A.12.4.3		٣-٣-م-١٥-٢		
	ISO27001 A.14.1.1		١-٣-م-١٦-٢	أمن تطوير الأنظمة	١٦-٢
	ISO27001 A.14.2.6		٢-٣-م-١٦-٢		
	FR - MP - 6		١-٣-م-١٧-٢	أمن وسائط التخزين	١٧-٢
CCM - DSI - 07	MTCS SS - 12.8		٢-٣-م-١٧-٢		
	ISO27001 A.8.3.1		٣-٣-م-١٧-٢		
	FR - MP - 3		٤-٣-م-١٧-٢		
	FR - MP - 4		٥-٣-م-١٧-٢		
	FR - MP - 7		٦-٣-م-١٧-٢		

صمود الأمن السيبراني (Cybersecurity Resilience)



٣

المعايير الأخرى	المعايير	رقم الضابط للمشترك	رقم الضابط لمقدم الخدمات	المكون الفرعي	رقم المكون الفرعي
	FR CP - 2 (4)	١-١-٣-ش-١-٣	١-١-٣-م-١-٣	جوانب صمود الأمن السيبراني في	١-٣
	C5 BCM - 02		٢-١-٣-م-١-٣	إدارة استمرارية الأعمال	

الأمن السيبراني المتعلق بالأطراف الخارجية (Third-Party Cybersecurity)



المكون الفرعي	رقم المكون الفرعي	المكون الفرعي	رقم الضابط لمقدم الخدمات	رقم الضابط للمشارك	المعايير	المعايير الأخرى
١-٤	الأمن المتعلق بسلسلة الإمداد والأطراف الخارجية	١-٤-١-١-٤	٢-١-٤-١-٤	٣-١-٤-١-٤	٤-١-٤-١-٤	خاص
					FR-SA - 05	
					MTCS SS 10.5	
					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 Cybersecurity Governance	١-١ استراتيجية الأمن السيبراني Cybersecurity Strategy	
	٢-١ إدارة الأمن السيبراني Cybersecurity Management	
	٣-١ سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	
	٤-١ أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities	١-١ أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities
	٥-١ إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	٢-١ إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management
	٦-١ الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects	
	٧-١ الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Compliance with Cybersecurity Standards, Laws and Regulations	٣-١ الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Compliance with Cybersecurity Standards, Laws and Regulations
	٨-١ المراجعة والتقييم الدوري للأمن السيبراني Periodical Cybersecurity Review and Audit	
	٩-١ الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	٤-١ الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources
	١٠-١ برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program	
		٥-١ الأمن السيبراني ضمن إدارة التغيير Cybersecurity in Change Management

المكونات الأساسية		المكونات الفرعية للضوابط الأساسية للأمن السيبراني		المكونات الفرعية لضوابط الأمن السيبراني للحوسبة السحابية	
تعزيز الأمن السيبراني Cybersecurity Defense	١-٢	إدارة الأصول Asset Management	١-٢	إدارة الأصول Asset Management	١-٢
	٢-٢	إدارة هويات الدخول والصلاحيات Identity and Access Management	٢-٢	إدارة هويات الدخول والصلاحيات Identity and Access Management	٢-٢
	٣-٢	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Information Processing Facilities Protection	٣-٢	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Information Processing Facilities Protection	٣-٢
	٤-٢	حماية البريد الإلكتروني Email Protection			
	٥-٢	إدارة أمن الشبكات Network Security Management	٤-٢	إدارة أمن الشبكات Network Security Management	٤-٢
	٦-٢	أمن الأجهزة المحمولة Mobile Device Security	٥-٢	أمن الأجهزة المحمولة Mobile Device Security	٥-٢
	٧-٢	حماية البيانات والمعلومات Data and Information Protection	٦-٢	حماية البيانات والمعلومات Data and Information Protection	٦-٢
	٨-٢	التشفير Cryptography	٧-٢	التشفير Cryptography	٧-٢
	٩-٢	إدارة النسخ الاحتياطية Backup and Recovery Management	٨-٢	إدارة النسخ الاحتياطية Backup and Recovery Management	٨-٢
	١٠-٢	إدارة الثغرات Vulnerabilities Management	٩-٢	إدارة الثغرات Vulnerabilities Management	٩-٢
	١١-٢	اختبار الاختراق Penetration Testing	١٠-٢	اختبار الاختراق Penetration Testing	١٠-٢
	١٢-٢	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	١١-٢	إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	١١-٢
	١٣-٢	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	١٢-٢	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	١٢-٢
	١٤-٢	الأمن المادي Physical Security	١٣-٢	الأمن المادي Physical Security	١٣-٢
	١٥-٢	حماية تطبيقات الويب Web Application Security	١٤-٢	حماية تطبيقات الويب Web Application Security	١٤-٢
		إدارة المفاتيح Key Management	١٥-٢	إدارة المفاتيح Key Management	١٥-٢
		أمن تطوير الأنظمة System Development Security	١٦-٢	أمن تطوير الأنظمة System Development Security	١٦-٢
		أمن وسائط التخزين Storage Media Security	١٧-٢	أمن وسائط التخزين Storage Media Security	١٧-٢

المكونات الأساسية		المكونات الفرعية للضوابط الأساسية للأمن السيبراني		المكونات الفرعية لضوابط الأمن السيبراني للحوسبة السحابية	
صمود الأمن السيبراني Cybersecurity Resilience		جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	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 Third-Party Cybersecurity		الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	١-٤	الأمن المتعلق بسلسلة الإمداد والأطراف الخارجية Third-Party and Supply Chain Cybersecurity	١-٤

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

قابلية تطبيق ضوابط الأمن السيبراني للحوسبة السحابية على النماذج الثلاثة

في هذا القسم تم عرض نموذج لقابلية تطبيق ضوابط الأمن السيبراني للحوسبة السحابية (لكل من مقدمي الخدمات والمستخدمين) على نماذج الحوسبة السحابية الثلاثة (البرمجيات كخدمة "SaaS"، المنصة كخدمة "PaaS"، البنية التحتية كخدمة "IaaS"). وتجدر الإشارة إلى أن قابلية التطبيق الفعلية لكل ضابط قد تختلف عن ما هو موضح في هذا القسم حيث تعتمد على نوعية الخدمة والعلاقة ما بين مقدم الخدمة والمستخدم.

ضوابط مقدم الخدمة:

يوضح الجدول أدناه قابلية تطبيق ضوابط مقدمي الخدمة على النماذج الثلاثة (البرمجيات كخدمة "SaaS"، المنصة كخدمة "PaaS"، البنية التحتية كخدمة "IaaS"). ويرجى ملاحظة الآتي:

- X: تعني أن الضابط قد لا ينطبق.
- ✓: تعني أن الضابط قد ينطبق.
- الموارد (Resources): تعني أن الضابط قد ينطبق على مقدم الخدمة، وبشكل خاص على الموارد الخاصة بمقدم الخدمة.
- الأنظمة التقنية السحابية (CTS): تعني أن الضابط قد ينطبق على مقدم الخدمة، وبشكل خاص على الأنظمة التقنية السحابية (CTS) الخاصة بمقدم الخدمة.
- تطوير الأنظمة (System Development): تعني أن الضابط قد ينطبق على مقدم الخدمة، وبشكل خاص على تطوير الأنظمة لدى مقدم الخدمة.
- الأمن المادي (Physical Security): تعني أن الضابط قد ينطبق على مقدم الخدمة، وبشكل خاص على الأمن المادي لدى مقدم الخدمة.
- إدارة استمرارية الأعمال (Management Continuity Business): تعني أن الضابط قد ينطبق على مقدم الخدمة، وبشكل خاص على إدارة استمرارية الأعمال لدى مقدم الخدمة.
- العروض (Offering): تعني أن الضابط قد ينطبق على مقدم الخدمة، وبشكل خاص على العروض الخاصة بمقدم الخدمة.

الضابط الأساسي	الضابط الفرعي	IaaS	PaaS	SaaS
١-١-١-١				
	١-١-١-١-١	✓	✓	✓
١-٢-١				
	١-١-٢-١	✓	✓	✓
	٢-١-٢-١	✓	✓	✓
	٣-١-٢-١	✓	✓	✓
١-٣-١				
	١-١-٣-١	✓	✓	✓
١-٤-١				
	١-١-٤-١	✓	✓	✓
	٢-١-٤-١	✓	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))
	٣-١-٤-١	✓	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))
٢-٤-١				
	١-٢-٤-١	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))
١-٥-١		✓	✓	✓
٢-٥-١		✓	✓	✓
٣-٥-١				
	١-٣-٥-١	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))
	٢-٣-٥-١	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))
٤-٥-١		✓	✓	✓

الضابط الأساسي	الضابط الفرعي	IaaS	PaaS	SaaS
١-٢-١-٢				
	١-١-٢-٢	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))
	٢-١-٢-٢	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))
١-٢-٢				
	١-١-٢-٢	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))
	٢-١-٢-٢	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))
	٣-١-٢-٢	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))
	٤-١-٢-٢	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))
	٥-١-٢-٢	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))
	٦-١-٢-٢	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))
	٧-١-٢-٢	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))
	٨-١-٢-٢	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))

الضابط الأساسي	الضابط الفرعي	IaaS	PaaS	SaaS
	٩-١-٢-٢	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))
	١٠-١-٢-٢	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))
	١١-١-٢-٢	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))
	١٢-١-٢-٢	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))	✓ (العروض والأنظمة التقنية السحابية ((CTS))
١-٣-٢				
	١-١-٣-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٢-١-٣-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٣-١-٣-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٤-١-٣-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٥-١-٣-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٦-١-٣-٢	✓	✓	✓
	٧-١-٣-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٨-١-٣-٢	✓ (الأنظمة التقنية السحابية ((CTS))	×	×
	٩-١-٣-٢	✓	✓	✓
	١٠-١-٣-٢	✓	✓	✓

الضابط الأساسي	الضابط الفرعي	IaaS	PaaS	SaaS
	١١-١-م-٣-٢	✓	✓	✓
	١٢-١-م-٣-٢	✓	✓	✓
١-م-٤-٢				
	١-١-م-٤-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٢-١-م-٤-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٣-١-م-٤-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٤-١-م-٤-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٥-١-م-٤-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٦-١-م-٤-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
١-م-٥-٢				
	١-١-م-٥-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٢-١-م-٥-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٣-١-م-٥-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٤-١-م-٥-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
١-م-٦-٢				
	١-١-م-٦-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٢-١-م-٦-٢	✓	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))

الضابط الأساسي	الضابط الفرعي	IaaS	PaaS	SaaS
	٣-١-٦-٢	✓	✓	✓
	٤-١-٦-٢	✓	✓	✓
	٥-١-٦-٢	✓	✓	✓
١-٧-٢				
	١-١-٧-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٢-١-٧-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
١-٨-٢				
	١-١-٨-٢	×	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٢-١-٨-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
١-٩-٢				
	١-١-٩-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٢-١-٩-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
١-١٠-٢				
	١-١-١٠-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
١-١١-٢				
	١-١-١١-٢	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))
	٢-١-١١-٢	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))
	٣-١-١١-٢	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))

الضابط الأساسي	الضابط الفرعي	IaaS	PaaS	SaaS
	٤-١-١١-٢	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد، والأنظمة التقنية السحابية (CTS)، وبيانات المشارك التي تتم إدارتها من قبل مقدم الخدمة)
	٥-١-١١-٢	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))
	٦-١-١١-٢	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))
	٧-١-١١-٢	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))
	٨-١-١١-٢	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))	✓ (الموارد والأنظمة التقنية السحابية ((CTS))
١-١٢-٢				
	١-١-١٢-٢	✓	✓	✓
	٢-١-١٢-٢	✓	✓	✓
	٣-١-١٢-٢	✓	✓	✓
	٤-١-١٢-٢	✓	✓	✓
	٥-١-١٢-٢	✓	✓	✓
	٦-١-١٢-٢	✓	✓	✓
	٧-١-١٢-٢	✓	✓	✓
	٨-١-١٢-٢	✓	✓	✓
١-١٣-٢				
	١-١-١٣-٢	✓ (الأمن المادي)	✓ (الأمن المادي)	✓ (الأمن المادي)
	٢-١-١٣-٢	✓ (الأمن المادي)	✓ (الأمن المادي)	✓ (الأمن المادي)
	٣-١-١٣-٢	✓ (الأمن المادي)	✓ (الأمن المادي)	✓ (الأمن المادي)
١-١٤-٢				

الضابط الأساسي	الضابط الفرعي	IaaS	PaaS	SaaS
	١-١-١٤-٢	✓ (الأنظمة التقنية السحابية ((CTS)	✓ (الأنظمة التقنية السحابية ((CTS)	✓ (الأنظمة التقنية السحابية ((CTS)
١-١٥-٢		✓	✓	✓
٢-١٥-٢		✓	✓	✓
٣-١٥-٢				
	١-٣-١٥-٢	✓ (الأنظمة التقنية السحابية ((CTS)	✓ (الأنظمة التقنية السحابية ((CTS)	✓ (الأنظمة التقنية السحابية ((CTS)
	٢-٣-١٥-٢	✓ (الأنظمة التقنية السحابية ((CTS)	✓ (الأنظمة التقنية السحابية ((CTS)	✓ (الأنظمة التقنية السحابية ((CTS)
	٣-٣-١٥-٢	✓ (الأنظمة التقنية السحابية ((CTS)	✓ (الأنظمة التقنية السحابية ((CTS)	✓ (الأنظمة التقنية السحابية ((CTS)
٤-١٥-٢		✓	✓	✓
١-١٦-٢		✓	✓	✓
٢-١٦-٢		✓	✓	✓
٣-١٦-٢				
	١-٣-١٦-٢	✓ (تطوير الأنظمة، والأنظمة التقنية السحابية ((CTS)	✓ (تطوير الأنظمة، والأنظمة التقنية السحابية ((CTS)	✓ (تطوير الأنظمة، والأنظمة التقنية السحابية ((CTS)
	٢-٣-١٦-٢	✓ (تطوير الأنظمة، والأنظمة التقنية السحابية ((CTS)	✓ (تطوير الأنظمة، والأنظمة التقنية السحابية ((CTS)	✓ (الموارد والأنظمة التقنية السحابية ((CTS)
٤-١٦-٢		✓	✓	✓
١-١٧-٢		✓	✓	✓
٢-١٧-٢		✓	✓	✓
٣-١٧-٢				
	١-٣-١٧-٢	✓ (الأنظمة التقنية السحابية ((CTS)	✓ (الأنظمة التقنية السحابية ((CTS)	✓ (الأنظمة التقنية السحابية ((CTS)
	٢-٣-١٧-٢	✓ (الأنظمة التقنية السحابية ((CTS)	✓ (الأنظمة التقنية السحابية ((CTS)	✓ (الأنظمة التقنية السحابية ((CTS)

الضابط الأساسي	الضابط الفرعي	IaaS	PaaS	SaaS
	٣-٣-م-١٧-٢	✓	✓	✓
	٤-٣-م-١٧-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٥-٣-م-١٧-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
	٦-٣-م-١٧-٢	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))	✓ (الأنظمة التقنية السحابية ((CTS))
٤-م-١٧-٢		✓	✓	✓
١-م-١-٣				
	١-١-م-١-٣	✓ (الأنظمة التقنية السحابية ((CTS))، وإدارة استمرارية الأعمال)	✓ (الأنظمة التقنية السحابية ((CTS))، وإدارة استمرارية الأعمال)	✓ (الأنظمة التقنية السحابية ((CTS))، وإدارة استمرارية الأعمال)
	٢-١-م-١-٣	✓ (الأنظمة التقنية السحابية ((CTS))، وإدارة استمرارية الأعمال)	✓ (الأنظمة التقنية السحابية ((CTS))، وإدارة استمرارية الأعمال)	✓ (الأنظمة التقنية السحابية ((CTS))، وإدارة استمرارية الأعمال)
١-م-١-٤				
	١-١-م-١-٤	✓	✓	✓
	٢-١-م-١-٤	✓	✓	✓
	٣-١-م-١-٤	✓	✓	✓
	٤-١-م-١-٤	✓	✓	✓

جدول ٤. قابلية تطبيق ضوابط مقدم الخدمة على النماذج الثلاثة

ضوابط المشترك:

يوضح الجدول ٥ أدناه قابلية تطبيق ضوابط المشتركين على نماذج الحوسبة السحابية الثلاثة (البرمجيات كخدمة "SaaS"، المنصة كخدمة "PaaS"، البنية التحتية كخدمة "IaaS"). ويرجى ملاحظة الآتي:

- × : تعني أن الضابط قد لا ينطبق.
- ✓ : تعني أن الضابط قد ينطبق.
- مفاتيح التشفير (Cryptographic Keys): تعني أن الضابط قد ينطبق على المشترك، وبشكل خاص على مفاتيح التشفير الخاصة بالمشارك.

الضابط الأساسي	الضابط الفرعي	IaaS	PaaS	SaaS
١-١-١-ش-١				
	١-١-١-ش-١	✓	✓	✓
١-٢-٢-ش-١				
	١-٢-٢-ش-١	✓	✓	✓
	٢-١-٢-ش-١	✓	✓	✓
	٣-١-٢-ش-١	✓	✓	✓
١-٣-٣-ش-١				
	١-٣-٣-ش-١	✓	✓	✓
١-٤-٤-ش-١				
	١-٤-٤-ش-١	✓	✓	✓
١-١-٢-ش-١				
	١-١-٢-ش-١	✓	✓	✓
١-٢-٢-ش-١				
	١-٢-٢-ش-١	✓	✓	✓
	٢-١-٢-ش-١	✓	✓	✓
	٣-١-٢-ش-١	✓	✓	✓
	٤-١-٢-ش-١	✓	✓	✓
	٥-١-٢-ش-١	✓	✓	✓
١-٣-٣-ش-١				
	١-٣-٣-ش-١	✓	✓	✓
١-٤-٤-ش-١				

الضابط الأساسي	الضابط الفرعي	IaaS	PaaS	SaaS
	١-٢-٤-ش-١	✓	✓	✓
١-٢-٥-ش-١				
	١-٢-٥-ش-١	✓	✓	✓
١-٢-٦-ش-١				
	١-٢-٦-ش-١	✓	✓	✓
	١-٢-٦-ش-٢	✓	✓	✓
١-٢-٧-ش-١				
	١-٢-٧-ش-١	✓	✓	×
	١-٢-٧-ش-٢	✓	✓	✓
١-٢-٩-ش-١				
	١-٢-٩-ش-١	✓	✓	×
	١-٢-٩-ش-٢	✓	✓	×
١-٢-١١-ش-١				
	١-٢-١١-ش-١	✓	✓	✓
	١-٢-١١-ش-٢	✓	✓	✓
١-٢-١٥-ش-١		✓	✓	✓
١-٢-١٥-ش-٢		✓	✓	✓
١-٢-١٥-ش-٣				
	١-٢-١٥-ش-٣	(مفاتيح التشفير)	(مفاتيح التشفير)	(مفاتيح التشفير)
	١-٢-١٥-ش-٣	(مفاتيح التشفير)	(مفاتيح التشفير)	(مفاتيح التشفير)
١-٢-١٥-ش-٤		✓	✓	✓
١-٣-١-ش-١				
	١-٣-١-ش-١	✓	✓	✓

جدول ٥. قابلية تطبيق ضوابط المشترك على النماذج الثلاثة



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

