هيئة قطر للأسواق المالية
Qatar Financial Markets Authority
State of Qatar • دولة قطر

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

"ضوابط الامتثال لمعيار تأمين المعلومات الوطنية للمشاركين في الأسواق المالية"

[IAS-FIN-NFMP]

◆

المعيار

مكمّل لمعيار الضمان الوطني لأمن المعلومات الإصدار 2.1 – الضوابط المعيارية الخاصة بالمشاركين في الأسواق المالية

هيئة قطر للأسواق المالية

الوكالة الوطنية للأمن السيبراني

مارس 2026

النسخة 1.0

إخلاء المسؤولية / الحقوق القانونية

قامت هيئة قطر للأسواق المالية والوكالة الوطنية للأمن السيبراني بتصميم وإعداد هذه الوثيقة بعنوان: «ضوابط الامتثال لمعيار تأمين المعلومات الوطنية للمشاركين في الأسواق المالية" – الإصدار 1.0 – عام، وذلك بهدف مساعدة المشاركين في الأسواق المالية على فهم مخاطر الأمن السيبراني في البيئة الرقمية، والتخفيف من هذه المخاطر من خلال تطبيق المتطلبات الأمنية المحددة في هذه الوثيقة إلى جانب سياسة تصنيف البيانات الوطنية ومعيار الضمان الوطني لأمن المعلومات.

تتحمل هيئة قطر للأسواق المالية والوكالة الوطنية للأمن السيبراني مسؤولية مراجعة هذه الوثيقة وصيانتها.

يُعد الحصول على موافقة هيئة قطر للأسواق المالية والوكالة الوطنية للأمن السيبراني إلزامياً عند أي إعادة نسخ لهذه الوثيقة سواء جزئيًا أو كليًا وبغض النظر عن وسيلة الاستنساخ، باعتبارهما المصدر والمالك لوثيقة: " ضوابط الامتثال لمعيار تأمين المعلومات الوطنية للمشاركين في الأسواق المالية ".

كما تُعتبر الموافقة الخطية من هيئة قطر للأسواق المالية والوكالة الوطنية للأمن السيبراني إلزامية عند أي إعادة إصدار هذه الوثيقة بقصد الاستخدام التجاري، وتحتفظ هيئة قطر للأسواق المالية والوكالة الوطنية للأمن السيبراني بحق تقييم وظيفة وقابلية تطبيق جميع عمليات إعادة الإصدار التي يتم تطويرها لأغراض تجارية.

ولا يجوز تفسير الحصول على موافقة هيئة قطر للأسواق المالية والوكالة الوطنية للأمن السيبراني على أنه اعتماد لإعادة الإصدار المطوّرة، كما لا يجوز للمطور بأي حال من الأحوال الترويج لذلك أو إساءة تفسيره بأي وسيلة إعلامية أو في المناقشات الشخصية أو عبر وسائل التواصل الاجتماعي.

تفاصيل الوثيقة

تفاصيل الوثيقة	
رمز الوثيقة	IAS-FIN-NFMP
النسخة	1.0
التصنيف والنوع	عام
الملخص	ضوابط أمنية معيارية خاصة بالمشاركين في الأسواق المالية، وهي ملحق لمعيار الضمان الوطني لأمن المعلومات الإصدار 2.1.

المراجعة والاعتماد

الاسم/ الدور	القسم	تمت المراجعة والاعتماد	النسخة	التاريخ
المسؤول	شؤون السياسات، الوكالة الوطنية للأمن السيبراني		1.0	
	هيئة قطر للأسواق المالية		1.0	

تفاصيل التعديلات

النسخة	المؤلف	وصف التعديل	التاريخ
1.0	هيئة قطر للأسواق المالية والوكالة الوطنية للأمن السيبراني	الوثيقة المنشورة النسخة 1.0	

السند القانوني

الوكالة الوطنية للأمن السيبراني

استنادًا إلى المرسوم الأميري رقم (1) لسنة 2021 بشأن إنشاء الوكالة الوطنية للأمن السيبراني، والذي يهدف إلى المحافظة على الأمن السيبراني الوطني وتنظيمه وتعزيز وحماية المصالح الحيوية للدولة في مواجهة التهديدات السيبرانية، ووفقًا للمادة رقم (3) من المرسوم، فإن الوكالة تختص بوضع وتطوير وتحديث السياسات وآليات الحوكمة والمعايير والضوابط والإرشادات اللازمة لتعزيز الأمن السيبراني بالتنسيق مع الجهات المعنية، وتعميمها على الجهات ذات العلاقة ومتابعة الالتزام بها.

كما تعزز الاستراتيجية الوطنية للأمن السيبراني 2.0، الركيزة الثانية – التشريعات والتنظيم وإنفاذ القانون من أجل فضاء سيبراني آمن، الهدف الاستراتيجي 1 – تطوير الأطر القانونية والتنظيمية المناسبة، المبادرة 4 – تطوير الأطر التنظيمية للأمن السيبراني للتقنيات الناشئة الحديثة، صلاحيات الوكالة الوطنية للأمن السيبراني باعتبارها الجهة المختصة بإصدار السياسات والمعايير والأطر والإرشادات ذات الصلة بالأمن السيبراني.

وفي هذا السياق، تم تطوير هذه الإرشادات الخاصة بالضمان الوطني لأمن المعلومات للمشاركين في الأسواق المالية بهدف تنظيم وحوكمة متطلبات الأمن السيبراني للمشاركين في الأسواق المالية في دولة قطر والخاضعين لتنظيم هيئة قطر للأسواق المالية.

ويعد هذا معيارًا تكميليًا يجب استخدامه جنبًا إلى جنب مع سياسة تصنيف البيانات الوطنية ومعيار الضمان الوطني لأمن المعلومات.

وقد تم تطوير هذا المعيار استنادًا إلى المسؤوليات الموكلة إلى الوكالة الوطنية للأمن السيبراني بموجب المرسوم الأميري رقم (1) لسنة 2021، وفي حال نشوء تعارض بين هذه الوثيقة (أي حكم أو بند محدد) وقوانين دولة قطر، فإن الأولوية لقانون الدولة، ويُعتبر أي حكم أو بند محدد في هذه الحالة ملغى من هذه الوثيقة بالقدر الذي يتعارض فيه مع القانون، دون التأثير على باقي أحكام الوثيقة، وفي هذه الحالة، يلزم إجراء تعديلات لضمان الامتثال للقوانين المعمول بها في دولة قطر.

هيئة قطر للأسواق المالية

أُنشئت هيئة قطر للأسواق المالية بموجب القانون رقم (33) لسنة 2005، والمعدّل بالمرسوم بقانون أميري رقم (14) لسنة 2007 والقانون رقم (10) لسنة 2009، باعتبارها هيئة مستقلة للإشراف والرقابة والتنظيم على الأسواق المالية في دولة قطر، وتتمتع الهيئة بالصلاحيات اللازمة لتنظيم الأسواق المالية ومراقبتها والإشراف عليها.

كما يؤكد القانون رقم (8) لسنة 2012 بشأن هيئة قطر للأسواق المالية، والمعدّل بالمرسوم بقانون رقم (22) لسنة 2018، استقلالية الهيئة وتمتعها بجميع الصلاحيات المطلوبة لممارسة مهامها التنظيمية والرقابية والإشرافية بصورة أكثر فاعلية، وذلك بما يتوافق مع أحكام القانون رقم (33) لسنة 2005 وتعديلاته.

وتحديدًا، تنص المادة (29) من القانون رقم (8) لسنة 2012 على أنه لا يجوز لأي شخص ممارسة أنشطة الأسواق المالية إلا بعد الحصول على ترخيص من الهيئة يحدد النشاط أو الأنشطة المصرح بها، كما يقرر مجلس الإدارة، وفقًا لأحكام هذا القانون، المتطلبات والضوابط والإجراءات الخاصة بمنح التراخيص، وكذلك المعايير المنظمة لمزاولة النشاط، كما تنص المادة (31) على أنه يجوز للهيئة، بموجب إخطار خطي، إصدار تعليمات إلى الأسواق المالية وغيرها من الأشخاص الخاضعين لاختصاصها، وعلى الأسواق المالية والأشخاص المعنيين تضمين هذه التعليمات ضمن قواعدهم المعمول بها والالتزام بتطبيقها، ويجوز للهيئة أن تطلب من تلك الأسواق والأشخاص إعداد أو تعديل قواعد محددة ضمن نطاق أعمالهم خلال مدة زمنية محددة، وفي حال عدم الالتزام بالطلب أو بالمواعيد المحددة فيه، يجوز للهيئة إعداد هذه القواعد أو تعديلها نيابةً عنهم وإلزامهم بتحمل تكلفتها.

ويقع اعتماد هذا المعيار وتنفيذه تحت المسؤولية الكاملة للجهات المعنية، ولا تتحمل الوكالة الوطنية للأمن السيبراني وهيئة قطر للأسواق المالية أي مسؤولية عن أي أضرار ناتجة عن اتخاذ قرار غير مدروس بشأن اعتماد هذا المعيار وتنفيذه.

مستويات المتطلبات

تُفسر المصطلحات المفتاحية التالية (يجب، لا يجب، إلزامي، مقترح، ربما، اختياري) الواردة في هذه الوثيقة على النحو التالي:

- يجب/ إلزامي: هذه المصطلحات تُشير إلى أن البند يُعد متطلبًا إلزاميًا أساسيًا مطلقًا ضمن المعايير.
- لا يجب: تعني هذه العبارة أن البند يُعد حظرًا مطلقًا ضمن المعايير.
- مقترح: تعني هذه الكلمة أن البند ليس متطلبًا إلزاميًا أو أساسيًا، ومع ذلك، ينبغي على الجهات اعتباره ضابطًا إضافيًا للأصول التي تم تصنيفها ضمن مستوى متوسط أو عالٍ ضمن عملية تصنيف الأصول المعلوماتية.
- ربما/ اختياري: مصطلحات تُشير إلى أن البند اختياري بالكامل.

جدول المحتويات

1. المقدمة

1.1. السياق

نعيش اليوم في عالم مترابط، فإن معظم الخدمات التي نستخدمها أصبحت متاحة عبر الإنترنت، وعلى الرغم من أن ذلك قد وفر لنا العديد من الفوائد وسهّل أسلوب الحياة، إلا أنه فتح أيضًا مساحة جديدة واسعة للهجمات، وشكل ذلك أكبر تهديد في الخدمات المالية عبر الانترنت.

لقد باتت مخاطر الأمن السيبراني اليوم معترفاً بها بوصفها من بين أبرز خمسة تهديدات عالمية، وذلك وفقاً لتقديرات الهيئات العالمية الرائدة مثل البنك الدولي والمنتدى الاقتصادي العالمي وغيرها.

وتُعد الأنظمة المالية من بين الأنظمة الأكثر عرضةً لهذه المخاطر، ويرجع ذلك في المقام الأول إلى المكاسب المالية التي توفّرها للمجرمين، فضلاً عن حجم التغيير المباشر الذي قد تتركه الهجمات السيبرانية على الجمهور وثقة المتعاملين، ومن هذا المنطلق، تبرز أهمية إدراك هذه المخاطر والعمل على اتخاذ الإجراءات المناسبة للحد منها والتخفيف من آثارها.

ولهذه الغاية، تقترح هيئة قطر للأسواق المالية اعتماد سياسة التصنيف الوطنية للبيانات والمعيار الوطني لضمان المعلومات، إلى جانب هذا المعيار التكميلي لتعزيز نضج الأمن السيبراني لدى المشاركين العاملين ضمن الأسواق المالية في دولة قطر.

2. الغرض والنطاق والاستخدام والصلاحيات

2.1. الغرض

الغرض من هذه الوثيقة هو تقديم نظرة عامة على أبرز مخاطر الأمن السيبراني المرتبطة بتداول الأسواق المالية وتحديد الضوابط والتدابير الوقائية المناسبة، ويُعد هذا المعيار مكمّلًا لمعيار تأمين المعلومات الوطنية الإصدار 2.1، ويتماشى مع المعيار الدولي (IOSCO)، كما يُقصد استخدام هذا المعيار لأغراض اعتماد الجهات العاملة في الأسواق المالية.

2.2. النطاق

يشمل نطاق هذا المعيار المشاركين في الأسواق المالية في دولة قطر الخاضعين لتنظيم هيئة قطر للأسواق المالية، كما ينطبق هذا المعيار على الأفراد والعمليات والأنظمة المرتبطة بتداول الأسواق ومراقبتها وتطبيقات العملاء.

2.3. الاستخدام

يجب على الجهات العاملة في الأسواق المالية في دولة قطر والخاضعة لتنظيم هيئة قطر للأسواق المالية تنفيذ هذا المعيار والحصول على الاعتماد وفقًا له لإثبات امتثالها لمتطلبات الأمن السيبراني أمام الهيئة وتقديم ضمانات لعملائها.

ويجب على المشاركين ملاحظة أنه لا يجوز النظر إلى هذه الوثيقة بشكل منفصل، بل يجب تحقيق الامتثال من خلال الالتزام المتكامل بكل من هذه الوثيقة وسياسة تصنيف البيانات الوطنية ومعيار الضمان الوطني لأمن المعلومات.

وتُعد المتطلبات المذكورة في هذا المعيار (القسم 5)، إلى جانب المتطلبات المذكورة في الملحق 7.2 متطلبات إلزامية.

كما أنه في الحالات التي ينص فيها هذا المعيار على أن أحد ضوابط معيار تأمين المعلومات الوطنية الإصدار 2.1 "يجب توسيعه"، فإن هذا التوسيع ينطبق فقط ضمن نطاق المشاركين في الأسواق المالية ولا يعدّل النص الأساسي لمعيار تأمين المعلومات الوطنية الإصدار 2.1.

وأخيرًا، فإن هذا الامتثال لا يُعد ضمانًا لأي نماذج ذكاء اصطناعي أو أنظمة مدعومة أو مستخدمه بالذكاء الاصطناعي، وفي حال الحاجة إلى ضمان نماذج أو أنظمة الذكاء الاصطناعي، يمكن استخدام الاعتماد وفق معيار (ISO/IEC 42001) وذلك إلى حين إصدار معيار ذي صلة من قبل هيئة قطر للأسواق المالية أو الوكالة الوطنية للأمن السيبراني.

3. المصطلحات الأساسية

الجهة	تشير إلى أي جهة تجارية / غير تجارية تعمل في دولة قطر وتخضع لتنظيم هيئة قطر للأسواق المالية.

4. المخاطر والتحديات

4.1. المخاطر

يتناول القسم التالي نظرة شاملة على مشهد المخاطر من منظور الأسواق المالية.

أ. عدم توفر أنظمة البورصة والبنية التحتية للسوق

تُعد البورصة والبنية التحتية للسوق حساسة للغاية تجاه تأخيرات الحوسبة، والتي قد تؤدي إلى عدم تنفيذ الصفقات أو عدم إتمامها، وقد يؤثر عدم توفر المنصة على أسعار المؤشرات، وصناديق المؤشرات المتداولة (ETFs)، والمشتقات، وجميع الأدوات المرتبطة بهذه الأسواق، مما يؤدي إلى حدوث مخاطر متتابعة في عمليات احتساب الهوامش ونماذج المخاطر، وبالتالي التسبب في خسائر مالية كبيرة، وقد تؤدي الهجمات السيبرانية إلى إبطاء أنظمة التداول أو جعلها غير متاحة، مثل هجمات حجب الخدمة على بوابات البورصة، أو بيانات السوق، أو البنية التحتية لتوجيه الأوامر.

ب. إلحاق الضرر بالأنظمة

تُعد منصات السوق والتداول حساسة للغاية لأنها تتعامل مع الأموال والمعلومات المالية الخاصة بالمشاركين، وهم الوسطاء والعملاء الذين يتداولون على المنصة، كما أن لها تأثيرًا أيضًا على الشركات المتداولة في السوق، فمن المهم جدًا الحفاظ على سلامة الأنظمة، وأي هجوم يضر بسلامة الأنظمة من خلال التلاعب ببيانات الأسعار أو أحجام التداول أو دفاتر الأوامر أو تأكيدات الصفقات دون تعطيل الأنظمة بالضرورة قد يؤثر على سلامة السوق ويفتح المجال أمام إساءة استخدام السوق دون اكتشافها.

وقد تحدث مثل هذه الهجمات أيضًا نتيجة لاختراق خوارزميات التداول وأنظمة توجيه الأوامر الذكية أو من خلال التلاعب بخوارزميات التداول عالي التردد (HFT)، أو خوارزميات التنفيذ، أو محركات التحقق من المخاطر.

ج. مخاطر سلسلة التوريد (الموردون، الخدمات السحابية، والأطراف الثالثة)

إن اعتمادنا على مزودي الخدمات الرقمية يعني أنه في حال تعرض أحد الموردين للاختراق، فإن المشكلة تصبح أكثر خطورة خاصة في حال وجود تركّز في عدد محدود من مزودي بيانات السوق أو مزودي التكنولوجيا، مما قد يؤدي إلى حدوث انقطاعات على مستوى القطاع بأكمله.

د. المخاطر الناتجة عن التقنيات الناشئة مثل الذكاء الاصطناعي

إن الاستخدام غير المنضبط وغير المنظم للتقنيات الناشئة مثل الذكاء الاصطناعي قد يشكل خطرًا يتمثل في فقدان الثقة، مما يؤدي إلى آثار مالية، وقد تظهر هذه المخاطر من خلال قدرة تقنيات مثل الذكاء الاصطناعي على التلاعب بالسوق عبر ممارسات (spoofing وlayering وpump and dump)، وكذلك من خلال السلوك الجماعي الخوارزمي (Algorithmic herding) استجابةً لإشارات مُتلاعب بها، مما يؤدي إلى تضخيم تقلبات الأسعار.

4.2. التحديات

من أبرز التحديات التي تواجه الأسواق المالية الحاجة إلى الحفاظ على سلامة الأنظمة وثقة العملاء، مع حماية أنظمة تقنية المعلومات المعقدة ومتعددة الأطراف المعنية من مختلف توجهات التهديدات السيبرانية.

5. عبارات التحكم

حوكمة الأمن المعلوماتي

استيفاءً لمتطلبات هذا المجال، يجب على الجهات:

CCMP-IG 01:

إنشاء لجنة توجيهية للأمن السيبراني (CSC) تكون مسؤولة عن الإشراف على استراتيجية الأمن السيبراني والحوكمة وإدارة المخاطر داخل الجهة.

أ. ضمان أن يرأس اللجنة أحد كبار التنفيذيين وأن تضم ممثلين من تقنية المعلومات وإدارة المخاطر والشؤون القانونية والامتثال ووحدات الأعمال لضمان إشراف مشترك بين الإدارات.

ب. تحديد وتوثيق نطاق عمل اللجنة، بما يشمل الأدوار والمسؤوليات والصلاحيات وآليات اتخاذ القرار لضمان وضوح المساءلة وفعالية الحوكمة.

ج. إجراء تقييمات دورية لمخاطر الأمن السيبراني ومراجعات استراتيجية، مع رفع نتائجها إلى الإدارة العليا ومجلس الإدارة (حيثما ينطبق).
د. الاجتماع مرة واحدة على الأقل كل ربع سنة مع الإدارة العليا ومجلس الإدارة لمراجعة حوادث الأمن السيبراني وحالة الامتثال ومعلومات التهديدات والوضع العام للأمن السيبراني.

CCMP-IG 02:

تحديد وقياس مؤشرات ذات الصلة عبر مختلف مجالات الضوابط لتقييم مستوى نضج أمن المعلومات لدى الجهة ومتابعة تطورها سنوياً.

CCMP-IG 03:

رفع تقارير تقدم مستوى نضج أمن المعلومات إلى القيادة من خلال اللجنة التوجيهية للأمن السيبراني، ويمكن للجهات استخدام أدوات مثل بطاقات قياس المرونة السيبرانية (Cyber Resilience Scorecards) لإعداد التقارير.

إدارة المخاطر

استيفاءً لمتطلبات هذا المجال، يجب على الجهات:

CCMP-RM 01:

توسيع الضابط RM 5 الوارد في الفصل 4 القسم 2 إدارة المخاطر ليشمل إجراء تقييم مخاطر مرة واحدة سنويًا على الأقل لجميع الأنظمة المرتبطة في تداول الأسواق والمراقبة وواجهات برمجة التطبيقات الخاصة بالعملاء.

CCMP-RM 02:

ضمان تقييم أي تقنية يتم اعتمادها داخل الجهة (خصوصًا في تداول الأسواق والمراقبة وواجهات برمجة التطبيقات الخاصة بالعملاء) من حيث المخاطر الأمنية المحتملة، ويجب تنفيذ أي تقنية جديدة وفق منهجية الأمن حسب التصميم (Security by Design) مع دمج الضوابط اللازمة للتخفيف من المخاطر المحتملة على الأنظمة.

إدارة أمن الأطراف الثالثة

استيفاءً لمتطلبات هذا المجال، يجب على الجهات:

CCMP-TM 01:

توسيع الضابط TM 5 الوارد في الفصل 4 القسم 3 إدارة أمن الأطراف الثالثة ليشمل إجراء تدقيق أمني سنوي على الأقل لجميع الأنظمة المرتبطة في تداول الأسواق والمراقبة وواجهات برمجة التطبيقات الخاصة بالعملاء.

CCMP-TM 02:

مراقبة أداء الأطراف الثالثة وتدفقات البيانات لاكتشاف أي سلوك غير طبيعي.

CCMP-TM 03:

ضمان امتثال الموردين من الأطراف الثالثة للمتطلبات التعاقدية والتنظيمية بما يشمل، على سبيل المثال لا الحصر، نقل البيانات، ويجب مراقبة هذا الامتثال باستخدام أدوات مثل لوحات المتابعة الآلية.

التوعية الأمنية

استيفاءً لمتطلبات هذا المجال، يجب على الجهات:

CCMP-SA 01:

تقديم برامج تدريب قائمة على المهارات حسب الحاجة لتزويد فرق تقنية المعلومات وأمن المعلومات بالمهارات اللازمة بما يتماشى مع الأدوار الوظيفية والمسؤوليات ويجب تحديث هذه البرامج التدريبية لمواكبة تغيرات التكنولوجيا ومشهد التهديدات وغيرها من العوامل.

إدارة الحوادث

استيفاءً لمتطلبات هذا المجال، يجب على الجهات:

CCMP-IM 01:

إعداد أدلة إجراءات تفصيلية (Playbooks) للتعامل مع التهديدات الحرجة مثل، على سبيل المثال لا الحصر، التلاعب بالخوارزميات وانقطاعات الخدمة لدى المشاركين واختراقات البيانات ضمن الأنظمة المرتبطة ببيئات تداول الأسواق.

CCMP-IM 02:

توسيع الضابط IM 8 الوارد في الفصل 4 القسم 8 إدارة الحوادث لينص على: «الإبلاغ عن جميع الحوادث الحرجة إلى هيئة قطر للأسواق المالية والوكالة الوطنية للأمن السيبراني خلال ساعتين (2) من تحديد الحادث."

CCMP-IM 03:

دمج الدروس المستفادة من الحوادث السابقة لتعزيز الإطار العام للأمن عبر الأفراد والعمليات والتقنيات.

إدارة استمرارية الأعمال

استيفاءً لمتطلبات هذا المجال، يجب على الجهات:

CCMP-BC 01:

يجب توسيع نطاق الضابط BC 2 في الفصل الرابع، القسم 9 إدارة استمرارية الأعمال، ليشمل النص التالي: «يجب تنفيذ تكوين (Active-Active) مع قدرات التحويل التلقائي عند التعطل لجميع الأنظمة المرتبطة بتداول السوق، والمراقبة، وواجهات برمجة التطبيقات الخاصة بالعملاء."

CCMP-BC-02:

يجب توسيع نطاق الضابط BC 8 في الفصل الرابع، القسم 9 إدارة استمرارية الأعمال، ليشمل النص التالي: "إجراء ما لا يقل عن تمرينين غير معلنين مسبقًا (سيتم إخطار مجموعة محدودة فقط من الأفراد بالتمرين) لإدارة استمرارية الأعمال (BCM) سنويًا، بحيث يكون أحدهما على الأقل اختبار محاكاة كامل، يتم خلاله نقل جميع الأنشطة من الموقع الأصلي إلى موقع التحويل الاحتياطي (Failover Site)، مع مشاركة كاملة من جميع أصحاب المصلحة المعنيين (الموظفين، والموظفين المتعاقدين من الباطن، والمورّدين، والمدققين، وغيرهم). أما التمرين الآخر فيمكن أن يكون تمرينًا مكتبيًا (Tabletop Drill) أو تمرينًا جزئيًا من التمرين الكامل، حيث يتم اختبار مكونات محددة من خطة استمرارية الأعمال (BCP) بناءً على درجة الأهمية أو نتائج اختبار المحاكاة الكامل."

تسجيل الأحداث ومراقبة الأمن

استيفاءً لمتطلبات هذا المجال، يجب على الجهات:

CCMP-SM 01:

مراقبة وتأمين بيئات تداول السوق من خلال إجراء عمليات فحص للثغرات الأمنية بشكل استباقي.

أ. يجب إجراء عمليات فحص الثغرات الأمنية مرة واحدة على الأقل شهريًا كحد أدنى.

ب. يجب تقييم الثغرات الأمنية التي يتم تحديدها، ووضع وتنفيذ خطة للمعالجة بناءً على تقييم المخاطر.

ج. يجب تطبيق أي تصحيحات أو تحديثات وفقًا لخطة إدارة التغيير المعتمدة.

د. يجب معالجة الثغرات الحرجة ضمن إطار زمني محدد بناءً على المخاطر، بحيث يكون الهدف 72 ساعة لمعالجة الثغرات التي تواجه الإنترنت أو التي يتم استغلالها بشكل نشط.

CCMP-SM 02:

تطوير عمليات أو أدوات أو آليات مناسبة لاكتشاف الخوارزميات أو البرامج غير المصرح بها (rogue algorithms) التي قد تقوم بالتلاعب بالسوق، وتقع مسؤولية اكتشاف هذه الخوارزميات وإيقافها على دور المشارك، حيث يجب على البورصات ضمان وجود ضوابط على مستوى السوق، بينما يجب على الوسطاء ضمان وجود ضوابط ضمن الأنظمة الواقعة تحت نطاق مسؤوليتهم التشغيلية.

CCMP-SM-03:

تطوير ودمج وظيفة مفتاح الإيقاف الآلي (Kill-Switch) لإيقاف مثل هذه التطبيقات غير المصرح بها فورًا.

CCMP-SM 04:

المشاركة في الهيئات الصناعية / القطاعية مثل:

FS-ISAC (Global) ودمج مصادر معلومات التهديدات السيبرانية الخارجية ضمن أنظمة مراقبة التهديدات المؤسسية.

CCMP-SM-05:

استخدام المعلومات المتاحة لتعزيز الوعي الظرفي والتدابير الدفاعية من أجل دعم الدفاعات الاستباقية.

CCMP-SM 06:

التعاون مع الجهات النظيرة داخل القطاع ومع الجهة التنظيمية للقطاع لتبادل معلومات التهديدات والرؤى وأفضل الممارسات المتعلقة بأمن المعلومات بهدف تعزيز وتطوير مستوى النضج السيبراني للقطاع.

التدقيق والاعتماد

استيفاءً لمتطلبات هذا المجال، يجب على الجهات:

CCMP-AC-01:

تطوير إطار موحد للامتثال يشمل اللوائح المعمول بها مثل سياسة تصنيف البيانات الوطنية ومعيار الضمان الوطني لأمن المعلومات وقانون حماية خصوصية البيانات الشخصية واللوائح القطاعية وأي لوائح عالمية أخرى قابلة للتطبيق لضمان المراقبة وإعداد التقارير بشكل متسق عبر مختلف الاختصاصات القضائية.

أمن البرمجيات

استيفاءً لمتطلبات هذا المجال، يجب على الجهات:

CCMP-SS 01:

توسيع الضابط SS 5 الوارد في الفصل 5 القسم 6 أمن البرمجيات [SS] لينص على أن الخوارزميات المستخدمة ضمن الأنظمة المرتبطة في تداول الأسواق والمراقبة، ويجب تصميم وتنفيذ وتشغيل وواجهات برمجة التطبيقات الخاصة بالعملاء بطريقة تضمن سلامة السوق والمرونة في مواجهة الهجمات السيبرانية، كما يجب أن تطبق هذه الخوارزميات ضوابط موثقة تشمل ضوابط ما قبل التداول ومراقبة ما بعد التداول وضوابط الطوارئ (بما في ذلك وظيفة Kill-Switch) وذلك لمنع التداول غير المنظم أو التلاعب بالسوق أو السلوك غير المقصود.

CCMP-SS 02:

توسيع الضابط SS 5 الوارد في الفصل 5 القسم 6 أمن البرمجيات [SS] لينص على أن الأنظمة المرتبطة في تداول الأسواق والمراقبة وواجهات برمجة التطبيقات الخاصة بالعملاء والتي يجب أن تخضع لاختبارات ضغط مناسبة، وبناءً عليه، يجب على الجهات ذات الأهمية الكبيرة مثل البورصات والوسطاء المرتبطين إجراء اختبارات ضغط للبنية التحتية الحرجة للأسواق حتى 8 – 10 أضعاف أحجام التداول القصوى، بينما يمكن للوسطاء الآخرين إجراء اختبارات ضغط حتى 2 – 3 أضعاف الحمل الأقصى الموثق لديهم.

أمن التحكم في الوصول

استيفاءً لمتطلبات هذا المجال، يجب على الجهات:

CCMP-AM-01:

مراقبة سلوك المستخدمين، مع التركيز على أنماط الوصول غير المعتادة ومحاولات تسريب البيانات وغيرها من المؤشرات أثناء استخدام الأنظمة المرتبطة في تداول الأسواق والمراقبة وواجهات برمجة التطبيقات الخاصة بالعملاء.

6. الامتثال والتنفيذ

6.1. الامتثال والتنفيذ

يوفر هذا المعيار التكميلي متطلبات وضوابط أمنية إضافية ضرورية لتنفيذ نظام إدارة أمن المعلومات لدى المشاركين في الأسواق المالية الخاضعين لتنظيم هيئة قطر للأسواق المالية، وتُعد هذه الضوابط إضافية إلى الضوابط الواردة في معيار الضمان الوطني لأمن المعلومات الإصدار 2.1.

6.1.1. عمليات الامتثال

يجب على الجهات الخاضعة لتنظيم هيئة قطر للأسواق المالية ملاحظة أنه لا يجوز النظر إلى هذه الوثيقة بشكل منفصل، ويجب الامتثال لهذا المعيار التكميلي إلى جانب سياسة تصنيف البيانات الوطنية ومعيار الضمان الوطني لأمن المعلومات ويتم إثبات الامتثال من خلال الحصول على شهادة الاعتماد وفق معيار الضمان الوطني لأمن المعلومات إلى جانب هذا المعيار.

6.1.2. الأدوار والمسؤوليات

تتحمل الوكالة الوطنية للأمن السيبراني وهيئة قطر للأسواق المالية مسؤولية تنفيذ ومتابعة الالتزام بهذا المعيار، وسيتم تطوير أي تغييرات أو تحديثات على هذا المعيار بشكل مشترك بين الجهتين، كما ستكون هيئة قطر للأسواق المالية مسؤولة عن تنفيذ هذا المعيار على الجهات الخاضعة لتنظيمها، ويجب على الجهات الخاضعة لتنظيم الهيئة إثبات امتثالها للمعيار من خلال الحصول على شهادة اعتماد والمحافظة عليها وسيتم تطوير وتنفيذ نظام الشهادات من قبل الوكالة الوطنية للأمن السيبراني.

وتعد هيئة قطر للأسواق المالية الجهة المختصة بالإجابة عن أي استفسارات تتعلق بهذا المعيار التكميلي.

6.2. الانتقال وتاريخ النفاذ

6.2.1. تاريخ النفاذ

يصبح هذا المعيار ساري المفعول اعتبارًا من تاريخ النشر الرسمي للمعيار.

6.2.2. فترة الانتقال

ستُمنح الجهات العاملة في الأسواق المالية في دولة قطر والخاضعة لتنظيم هيئة قطر للأسواق المالية فترة انتقال مدتها اثنا عشر (12) شهرًا من تاريخ نشر المعيار لإثبات خارطة طريق امتثالها لهذا المعيار.

6.3. الاستثناءات والانحرافات

6.3.1. الاستثناءات من متطلبات المعيار

جميع المتطلبات المذكورة في هذا المعيار (القسم 5)، إلى جانب الملحق 7.2 هي متطلبات إلزامية، ومع ذلك، قد تضطر الجهات إلى الاستثناء عن بعض المتطلبات الأمنية المحددة في هذا المعيار لعدة أسباب مثل اعتبارات السلامة وقابلية التشغيل، وتعني أي حالة قد يؤدي فيها تطبيق أحد المتطلبات الأمنية إلى تعريض الأرواح للخطر أو التأثير بشكل سلبي كبير على عمليات الجهة وأنظمتها.

وكذلك اعتبارات قيود الأعمال، وتعني عندما لا تسمح التقنيات الحالية (الأنظمة القديمة Legacy) أو متطلبات العمليات التجارية بتطبيق المتطلبات الأمنية المحددة، أو عندما يتطلب تطبيقها تكاليف مالية كبيرة أو موارد غير متناسبة أو غير مقبولة أو عندما يكون النظام قيد الترقية أو الاستبدال.

6.3.2. عمليات الاستثناء عن متطلبات المعيار

في الحالات المذكورة أعلاه يجب توثيق الاستثناء ويجب إجراء تقييم مخاطر لتحديد المخاطر الناتجة عن عدم تطبيق المتطلب المحدد، كما يجب على الجهة تحديد وتنفيذ ضوابط بديلة أو ضوابط تعويضية وفي حال تعذر تنفيذها أيضًا يجب تسجيل هذا الاستثناء باعتباره مخاطر متبقية غير مُخففة.

ويجب رفع هذا الاستثناء والمخاطر المرتبطة به إلى الإدارة العليا في الجهة، واعتماده من قِبل رئيس الجهة، أو الشخص المفوض من قِبله، أو رئيس إدارة المخاطر، أو رئيس التدقيق الداخلي.

وأخيراً يجب إرسال هذا الاستثناء مع خطة المعالجة إلى هيئة قطر للأسواق المالية من خلال القنوات الرسمية للمراسلات، وبناءً على هذه المعلومات، ستقوم الهيئة بمراجعة طلب الاستثناء وإصدار الموافقة أو الرفض.

وفي حال كانت هذه الاستثناءات مرتبطة في سياسة تصنيف البيانات الوطنية أو معيار الضمان الوطني لأمن المعلومات، فسيتم اتباع نفس العملية، على أن يتم اتخاذ القرار من قبل هيئة قطر للأسواق المالية بالتنسيق مع الوكالة الوطنية للأمن السيبراني.

7. الملحق

7.1. الاختصارات

IOSCO	المنظمة الدولية لهيئة الأسواق المالية

7.2. معيار التداول الخوارزمي (RTS 6/7) مترجم إلى أهداف ضوابط واضحة وقابلة للتدقيق ومربوطة مباشرةً بمعيار الضمان الوطني لأمن المعلومات (الإصدار 2.1)

الغرض

يحدد هذا الملحق أهداف ضوابط محددة وقابلة للتدقيق تنطبق على أنظمة التداول الخوارزمي ومنصات مراقبة السوق وواجهات برمجة تطبيقات التداول الخاصة بالعملاء.

وذلك بهدف ضمان سلامة السوق والمرونة التشغيلية وضمان الأمن السيبراني بما يتماشى مع معيار الضمان الوطني لأمن المعلومات الإصدار 2.1، مع الحفاظ على مبدأ التناسب وفقًا لدور الجهة وتأثيرها النظامي.

نطاق التطبيق

تنطبق أهداف الضوابط هذه على:

- الخوارزميات المستخدمة في إنشاء الأوامر أو توجيهها أو تنفيذها أو تحسينها
- المكونات الآلية للتداول المدمجة ضمن (OMS) و (EMS) أو منصات واجهات برمجة التطبيقات
- أنظمة المراقبة الخاصة بأنشطة التداول الخوارزمي أو التداول عالي التردد، وتشمل الجهات المعنية:
  - البورصات ومشغلي الأسواق الوسطاء
  - المرخصين وأعضاء التداول
  - مزودي منصات التداول الخوارزمي من الأطراف الثالثة (حيثما ينطبق)

مجالات الضوابط	الأهداف	المتطلبات	الضبط مع معيار الضمان الوطني لأمن المعلومات الإصدار 2.!
الحوكمة والمسؤولية	يجب تشغيل أنظمة التداول الخوارزمي ضمن هياكل حوكمة واضحة وملكية محددة ومساءلة واضحة	• تحديد مالك رسمي لكل خوارزمية تداول • تحديد جهة اعتماد نشر وتعديل الخوارزميات • إشراف مجلس الإدارة أو الإدارة العليا على مخاطر التداول الخوارزمي	• حوكمة أمن المعلومات • إدارة أمن المخاطر
التصميم الآمن وإدارة التغيير	يجب تصميم واختبار ونشر خوارزميات التداول بشكل آمن باستخدام عمليات خاضعة للرقابة وقابلة للتدقيق	• تطبيق دورة حياة تطوير آمنة لتسلسل الخوارزميات • اختبارات ما قبل النشر ضمن بيئات خاضعة للرقابة • إدارة تغيير رسمية لتسلسل الخوارزميات والمدخلات والإعدادات • الفصل بين بيئات التطوير والاختبارات والإنتاج	• أمن البرمجيات • أمن التطبيقات والبرمجيات • أمن العمليات وإدارة التغيير • ضوابط تقوية الأنظمة
ضوابط المخاطر قبل التداول	يجب أن تتضمن الخوارزميات ضوابط وقائية لمنع التداول غير المنظم والتأثير المفرط على السوق	• تحديد حدود حجم الأوامر والأسعار والكميات • تطبيق آليات: تحديد المعدل (Rate-limiting) والتحكم في التدفق (Throttling) • منع التداول الذاتي والتنفيذ غير المنضبط	• أمن البرمجيات • التحكم في الوصول
المراقبة واكتشاف السلوكيات المشبوهة	يجب مراقبة النشاط الخوارزمي بشكل مستمر لاكتشاف السلوك غير الطبيعي أو غير المقصود أو التلاعب المحتمل	• المراقبة اللحظية لأداء الخوارزميات وأنماط التداول • اكتشاف الانحراف عن السلوك المتوقع • تسجيل شامل لأغراض التحليل الجنائي والرقابة الإشرافية	• التسجيل والمراقبة
ضوابط الطوارئ (قدرات مفتاح الإيقاف الذاتي) (Kill-Switch)	يجب أن تكون الجهات قادرة على إيقاف أو تقييد التداول الخوارزمي فورًا في حال حدوث خلل أو اختراق أو اضطراب في السوق	• آليات تعليق يدوية و/أو آلية • إجراءات تصعيد وتفويض محددة • اختبار إجراءات الاستجابة ودمجها مع إدارة الحوادث	• إدارة الحوادث • استمرارية الأعمال
اختبارات الضغط والمرونة الاستيعابية	يجب أن تثبت أنظمة التداول الخوارزمي مرونتها تحت ظروف التشغيل القصوى وظروف الضغط	• اختبارات ضغط تتماشى مع ملف المخاطر وأحجام التداول • اختبار سيناريوهات الفشل وحساسية التأخير وتشبع الأنظمة • توثيق نتائج الاختبارات وإجراءات المعالجة	• استمرارية الأعمال • إدارة المخاطر
اعتماديات الأطراف الثالثة والموردين	عندما تكون هذه الأنظمة مقدمة أو مدعومة من قِبل أطراف ثالثة يجب تطبيق ضوابط أمنية عليها.	• تقييم أمني للموردين الذين يقدمون منصات التداول الخوارزمي • فرض أهداف الضوابط تعاقدياً • المراقبة المستمرة لأداء الموردين ومخاطرهم	• التسجيل والمراقبة

الجدول 1 ربط مبادئ RTS 6/7 الخوارزمية بمعيار الضمان الوطني لأمن المعلومات

7.3. المراجع

إرشادات المرونة السيبرانية للبنية التحتية للأسواق المالية (IOSCO)، يونيو 2016

7.4. قائمة الأشكال

لا توجد أشكال.

7.5. قائمة الجداول

نهاية الوثيقة