إطار عمل لتحسين الأمن السبراني للبنية التحتية الحساسة

النسخة 1.1

المعهد الوطني للمعايير والتكنولوجيا (NIST)

16 أبريل، 2018

ترجمة:

- علي الحسن (https://www.linkedin.com/in/ali-alhasan)
- علي الحاجي (https://www.linkedin.com/in/AliAlhajji1)

مراجعة: شركة شرايبر للترجمة. ليست ترجمة رسمية من حكومة الولايات المتحدة الأميركية

Translated by

- Ali A. AlHasan, PMP, CISSP,CISA, CGEIT, CRISC, CISM (https://www.linkedin.com/in/ali-alhasan)
- Ali AlHajji (https://www.linkedin.com/in/AliAlhajji1)

Reviewed by Schreiber Translations, INC (STI). Not an official U.S. Government translation.

ملاحظات للقُرّاء عن النسخة المحدثة

تهدف النسخة 1.1 من هذا الإطار العملي للأمن السبراني إلى تنقيح وتوضيح وإثراء النسخة 1.0 التي تم إصدارها في فبراير 2014. تدمج النسخة الحالية المُحدثة التعليقات التي تم تلقيها عن المسودتين للنسخة 1.1.

الهدف من النسخة 1.1 هو أن يتم تطبيقها من قبل المستخدمين الجدد والمستخدمين الحاليين لإطار العمل. من المفترض أن يكون المستخدمون الحاليون قادرين على تطبيق النسخة 1.1 بالحد الأدنى من الإخلال بالنسخة السابقة أو من دون أي إخلال بها، إذ أن التوافق مع النسخة 1.0 كان أحد الأهداف الصريحة للنسخة المحدثة.

الجدول أدناه يلخّص التغييرات بين النسختين 1.0 والنسخة 1.1.

جدول 1: ملخص عن التغييرات على إطار العمل بين النسخة 1.0 والنسخة 1.1

التحديث	وصف التحديث
التوضيح بأن المصطلحات مثل "التقيد" قد تكون مربكة وتحمل معان مختلفة جدًا في نظر أصحاب المصلحة المختلفين بإطار العمل.	تم إضافة توضيح بأن "الجدوى" هي بنية ولغة إطار العمل من أجل تنظيم التقيد بمتطلبات الأمن السبراني للمنظمة وللتعبير عن هذا التقيد من خلال متطلبات الأمن السبراني الخاصة بالمنظمة. ومع ذلك، فإن الطرق المختلفة التي يمكن من خلالها استخدام إطار العمل من قبل المنظمة تشير إلى أن عبارات من مثل "التقيد بإطار العمل" قد تكون مربكة.
قسم جديد عن التقييم الذاتي.	إضافة قسم 4.0 التقييم الذاتي لمخاطر الأمن السبراني باستخدام إطار العمل لشرح كيف يمكن استخدام إطار العمل من قبل المنظمات لفهم وتقييم مخاطر الأمن السبراني لديهم، بما في ذلك استخدام المقاييس.
إضافة شرح موسع لاستخدام إطار العمل في مجال إدارة المخاطر السبرانية لسلاسل الإمداد.	يساعد القسم الموسّع 3.3 إبلاغ متطلبات الأمن السبراني إلى أصحاب المصلحة المستخدمين في فهم إدارة المخاطر السبرانية لسلاسل الإمداد SCRM بشكل أفضل. كما يقوم القسم 3.4 قرارات الشراء بتسليط الضوء على استخدام إطار العمل في فهم المخاطر المتعلقة بالمنتجات والخدمات التجارية الجاهزة. أيضًا، تم إضافة معايير سبرانية جديدة تتعلق بإدارة المخاطر السبرانية لسلاسل الإمداد إلى مراحل التطبيق. وأخيرًا، تم إضافة تصنيف إدارة المخاطر السبرانية لسلاسل الإمداد إلى نواة إطار العمل، ويشمل ذلك عدة تصنيفات فرعية.
تنقيحات لأخذ مسائل المصادقة والتصريح وإثبات الهوية بمزيد من الاعتبار.	تم تنقيح اللغة المستخدمة في تصنيف التحكم في الوصول لأخذ مسائل المصادقة والتصريح وإثبات الهوية بمزيد من الاعتبار. وذلك يشمل إضافة تصنيف فرعي لكل من المصادقة وإثبات الهوية. كما تم تغيير اسم التصنيف إلى إدارة الهويات والتحكم في الوصول **(PR.AC)** من أجل تمثيل نطاق التصنيف والتصانيف الفرعية التابعة له بشكل أفضل.
شرح أفضل للعلاقة بين مراحل التطبيق وبين النماذج	شرح إضافي في القسم 3.2 تأسيس أو تطوير برنامج أمن سيبراني عن استخدام مراحل إطار العمل في تطبيق إطار العمل. شرح إضافي في مراحل إطار العمل بهدف إبراز اعتبارات إطار العمل في البرامج التنظيمية لإدارة المخاطر. كما تم تنقيح مفاهيم مرحلة إطار العمل. وأيضًا، تم تحديث الشكل 2.0 ليحتوي على الإجراءات من مراحل إطار العمل.

يمكن الحصول على نسخة مجانية من هذا المنشــور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

نظرة إلى الإفصاح المنسق عن مواطن الضعف	تم إضافة تصنيف فرعي يتعلق بدورة حياة الإفصاح عن مواطن الضعف.

وكما هو الأمر في النسخة 1.0، فإننا نشجع مستخدمي النسخة 1.1 على تكييف إطار العمل لتحقيق القيمة القصوى لكل منظمة.

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

شكر وتقدير

هذه النشرة هي ثمرة جهود تعاونية متواصلة من كل من الأوساط الصناعية والأوساط الأكاديمية والحكومة. لقد قام المعهد الوطني للمعايير والتكنولوجيا NIST بإطلاق المشروع عبر اجتماعات مع منظمات وأفراد من القطاعين الخاص والعام في عام 2013. إطار العمل لتحسين الأمن السبراني للبنية التحتية الحساسة، الذي تم نشره في 2014 وتمت مراجعته خلال العام 2017 و2018، اعتُمد فيه على 8 ورش عمل عمومية، و على عدة طلبات لإبداء التعليقات والمعلومات، وعلى آلاف التعاملات المباشرة مع أصحاب المصلحة من كافة القطاعات في الولايات المتحدة الأمريكية بالإضافة إلى عدة قطاعات حول العالم.

إن الحوافز وراء تغيير النسخة 1.1 والتغييرات الموجودة في هذه النسخة 1.1 تقوم على:

- التعليقات والأسئلة المتكررة التي تلقاها NIST منذ صدور إطار العمل نسخة 1.0
- الردود الـ105 على طلب المعلومات المنشور في ديسمبر 2015: Framework for Improving Critical Infrastructure Cybersecurity
- ما يقارب الـ85 تعليقًا على المسودة المقترحة الثانية للنسخة 1.1 والمنشورة في 5 ديسمبر 2017.
- ما يقارب الـ120 تعليقًا على المسودة المقترحة الأولى للنسخة 1.1 والمنشورة في 10 يناير 2017
- تعقيبات أكثر من 1200 شخص حضروا ورشات عمل إطار العمل في عامي 2016 و2017

بالإضافة إلى ذلك، قام المعهد القومي للمعايير والتكنولوجيا NIST مسبقًا بإصدار النسخة 1.0 من إطار عمل الأمن السبراني مع ملف مرافق له خارطة طريق **NIST** لتطوير الأمن السبراني للبنية التحتية الحساسة. في خارطة الطريق هذه يتم تسليط الضوء على "مجالات التحسين" الأساسية للمزيد من التطوير والمواءمة والعمل المشترك. بفضل القطاعين الخاص والعام، تطورت بعض مجالات التحسين بما يكفي ليتم إضافتها إلى إطار العمل هذا بنسخته 1.1.

يتقدم المعهد القومي للمعايير والتكنولوجيا NIST بالشكر والثناء إلى كل من ساهم في إعداد هذا الإطار العام

يمكن الحصول على نسخة مجانية من هذا المنشــور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

ملخص تنفيذي

تعتمد الولايات المتحدة الأمريكية على الأداء الموثوق للبنية التحتية الحساسة. أما المخاطر السبرانية فتستغل التعقيد والقدرات الاتصالية المتزايدين لأنظمة البنية التحتية الحساسة، مهددةً بذلك أمن الدولة واقتصادها، وسلامة السكّان وصحتهم. كما هو الحال في المخاطر المالية والمخاطر التي تمس بالسمعة، تؤثر المخاطر السبرانية أيضًا على رصيد الشركات، فهي بإمكانها أن ترفع من حجم التكاليف مؤثرة بذلك على الإيرادات، كما بإمكانها أن تضرّ بقدرة المنظمة على الإبداع وجذب العملاء والمحافظة عليهم. يمكن للأمن السبراني أن يكون جزءًا مهمًا وكبيرًا من الإدارة الشاملة للمخاطر في المنظمة.

للإشارة بشكل أفضل إلى هذه المخاطر، قام قانون تحسين الأمن السبراني (**Cybersecurity Enhancement Act, CEA**) في عام 2014[1] بتحديث دور المعهد القومي للمعايير والتكنولوجيا (NIST) ليشمل تحديد وتطوير أطر العمل الخاصة بمخاطر الأمن السبراني للاستخدام الاختياري من قبل ملّاك البنية التحتية الحساسة والمشغّلين فيها. وفقًا لقانون تحسين الأمن السبراني، يجب على المعهد القومي للمعايير والتكنولوجيا أن يحدّد "منهجية ذات أولويات محددة، مرنة، قابلة للتكرار، مبنية على جودة الأداء، وفعالة من حيث التكلفة، بما في ذلك مقاييس وضوابط أمن المعلومات التي يمكن اعتمادها بشكل اختياري من قبل ملّاك ومشغّلي البنية التحتية الحساسة لتساعدهم على تحديد وتقييم وإدارة المخاطر السبرانية." ساهم ذلك في إضفاء الطابع الرسمي لما قامت به NIST مسبقًا في تطوير إطار العمل بنسخته 1.0 تحت الأمر التنفيذي رقم 13636 "تطوير الأمن السبراني للبنية التحتية الحساسة" في فبراير 2013، كما قدّم الإرشادات نحو التطور المستقبلي لإطار العمل. إطار العمل الذي تم تطويره بناء على الأمر التنفيذي 12636، والذي لا يزال يتطور وفقًا لقانون تحسين الأمن السبراني، يستخدم لغة موحدة للإشارة إلى المخاطر السبرانية وإدارتها بطريقة ذات تكلفة فعالة بناءً على احتياجات المنظمات والأعمال دون الحاجة إلى فرض متطلبات تنظيمية إضافية على الأعمال.

يركز إطار العمل على استخدام الدوافع التي تسيّر الأعمال بهدف توجيه نشاطات الأمن السبراني ووضع المخاطر السبرانية في عين الاعتبار كجزء من عمليات إدارة المخاطر في المنظمة. يتكون إطار العمل من ثلاثة أجزاء: نواة إطار العمل، ومراحل التطبيق، ونماذج إطار العمل. نواة إطار العمل هو مجموعة من النشاطات والمخرجات والمراجع المعرفية الخاصة بالأمن السبراني والمشتركة بين مختلف القطاعات والبنيات التحتية الحساسة. أما نماذج إطار العمل، فقد وضعت لمساعدة المنظمة في تحديد أولوياتها فيما يتعلق بنشاطات الأمن السبراني ومواءمة هذه النشاطات مع رسالتها ومتطلبات أعمالها التجارية، ومع درجة تحملها للمخاطر، ومع مصادرها. أما المراحل فتقدم للمنظمات آليةً لاستعراض وفهم خصائص المنهجية التي تستخدمها في إدارة المخاطر السبراني، مما يساعد في تحديد أولويات الأهداف المتعلقة بالأمن السبراني وتحقيقها.

على الرغم من أن هذا المستند قد تم إعداده لتطوير إدارة المخاطر السبرانية في البنية التحتية الحساسة، إلا أنه يمكن استخدامه من قبل المنظمات الأخرى في أي قطاع أو أي مجال. يتيح الإطار للمنظمات -بغض النظر عن حجمها أو درجة المخاطر السبرانية التي تواجهها أو مستوى تعقيد الأمن السبراني لديها- يتيح لها أن تعتمد مبادئ والممارسات المثلى لإدارة المخاطر بهدف تطوير مستوى الأمن والصمود.

يقدّم الإطار هيكلية مشتركة وذات قدرة تنظيمية للعديد من منهجيات الأمن السبراني عن طريق تجميع المعايير والإرشادات والممارسات التي تعمل بشكل فعال في الوقت الحاضر. بالإضافة إلى ذلك، ولأن الإطار يرجع إلى معايير معترف بها عالميًا للأمن السبراني، فإن بإمكانه أن يكون نموذجًا للشركات العالمية لكي يساعدها في تقوية الأمن السبراني في البنيات التحتية الحساسة وفي القطاعات والمجالات الأخرى على حد سواء.

[1] انظر القانون الفيدرالي رقم 15: 15 U.S.C. § 272(e)(1)(A)(i). أقانون تحسين الأمن السبراني لعام 2014 (S.1353) والذي أصبح قانوناً عمومياً برقم 113-274 بتاريخ 18 ديسمبر 2014، ويمكن الوصول إليه عبر الرابط الإلكتروني:
https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

يقدم الإطار طريقة مرنة لمقاربة الأمن السبراني، بما في ذلك أثر الأمن السبراني على الأبعاد المادية والسبرانية والبشرية. يمكن تطبيق الإطار على المنظمات التي تعتمد على التقنية، سواء أكان تركيز الأمن السبراني لديها على تقنية المعلومات (IT) بشكل أساس، أم على أنظمة التحكم الصناعي (ICS)، أم على الأنظمة المادية-السبرانية (CPS)، أم على الأجهزة المترابطة بشكل عام مثل إنترنت الأشياء (IoT). يمكن للإطار أن يساعد المنظمات في مقاربة الأمن السبراني باعتباره مؤثرًا على خصوصية العملاء والموظفين والأطراف الأخرى. كما يمكن لمخرجات إطار العمل أن تشكّل أهدافًا لتطوير قوى العمل وللنشاطات التطويرية.

إن إطار العمل ليس منهجية وُضعت لتناسب الجميع لإدارة مخاطر الأمن السبراني في البنيات التحتية الحساسة، فكلّ منظمة ستظلّ تواجه مخاطر مختلفة عن غيرها – تهديدات مختلفة، ومواطن ضعف مختلفة، ومستويات مختلفة لتحمل المخاطر. كما أن المنظمات ستتباين في طرق تكييفها للممارسات الموصوفة في إطار العمل. يمكن لكل منظمة أن تقرّر النشاطات المهمة لتقديم خدماتها الأساسية، كما يمكنها أن تحدد أولويات الاستثمار لتعظيم المردود من كل دولار يتم إنفاقه. في النهاية، يهدف إطار العمل إلى تقليل المخاطر السبرانية ولإدارتها بشكل أفضل.

هنالك طرق متنوعة لاستخدام إطار العمل، وذلك لاستيعاب حاجات الأمن السبراني الفريدة لكل منظمة. إن القرار المتعلق بكيفية تطبيق إطار العمل متروك للمنظمة التي تريد تطبيقه. فمثلًا، قد تختار إحدى المنظمات استخدام مراحل تنفيذ إطار العمل لصياغة الممارسات التي تتصورها لإدارة المخاطر. بينما قد تختار منظمة أخرى أن تستخدم الوظائف الخمسة لإطار العمل من أجل تحليل كامل خطتها لإدارة المخاطر، هذا التحليل قد يعتمد وقد لا يعتمد على المزيد من الإرشادات المفصلة المصاحبة، مثل قوائم الضوابط. تبرز أحيانًا بعض المناقشات حول "التقيد" بإطار العمل، كما تُعتبر "الجدوى" هي هيكلية ولغة إطار العمل لتنظيم التقيد بمتطلبات الأمن السبراني للمنظمة وللتعبير عن هذا التقيد. ومع ذلك، فإن الطرق المتعددة لاستخدام إطار العمل من قبل المنظمة تشير إلى أن عبارات مثل "التقيد بإطار العمل" قد تكون مربكة وذات معنًى مختلف عند كل واحد من أصحاب المصلحة.

إن إطار العمل مستند حيّ وسيستمر تحديثه وتطويره في ظل التعقيبات والتعليقات المتلقاة من قطاع الصناعة. سيستمر المعهد القومي للمعايير والتكنولوجيا في التنسيق مع القطاع الخاص والهيئات الحكومية على كافة الأصعدة. وفي الوقت الذي يُستخدم فيه الإطار في مستويات أعلى، سيتم تضمين الدروس المستفادة الإضافية في النسخ المستقبلية. سيضمن ذلك أن إطار العمل يلبي احتياجات أصحاب ومشغّلي البنية التحتية الحساسة في بيئة ديناميكية ومليئة بالتحديات تشتمل على تهديدات ومخاطر وحلول جديدة.

إن استخدام هذه الإطار التطوعي ومشاركة الممارسات المثلى على نطاق واسع وبشكل فعّال هما الخطوة التالية لتطوير الأمن السبراني للبنية التحتية الحساسة لأمّتنا – بتقديمه التوجيهات المتطورة للمنظمات الفردية، في الوقت ذاته الذي يعزز فيه حالة الأمن السبراني للبنية التحتية الحساسة للأمة وللاقتصاد العام وللمجتمع.

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الفهرس

قائمة بالأشكال التوضيحية

قائمة بالجــداول

يمكن الحصول على نسخة مجانية من هذا المنشــور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

يمكن الحصول على نسخة مجانية من هذا المنشــور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

1.0 مقدمة إطار العمل

تعتمد الولايات المتحدة الأمريكية على الأداء الموثوق للبنية التحتية الحساسة. أما المخاطر السبرانية فتستغل التعقيد والقدرات الاتصالية المتزايدين لأنظمة البنية التحتية الحساسة، مهددةً بذلك أمن الدولة واقتصادها، وسلامة السكّان وصحتهم. كما هو الحال في المخاطر المالية والمخاطر التي تمس بالسمعة، تؤثر المخاطر السبرانية أيضًا على رصيد الشركات، فهي بإمكانها أن ترفع من حجم التكاليف مؤثرة بذلك على الإيرادات، كما بإمكانها أن تضرّ بقدرة المنظمة على الإبداع وجذب العملاء والمحافظة عليهم. يمكن للأمن السبراني أن يكون جزءًا مهمًا وكبيرًا من الإدارة الشاملة للمخاطر في المنظمة.

لتعزيز صمود هذه البنية التحتية، قام قانون تحسين الأمن السبراني (Cybersecurity Enhancement Act, CEA) في عام 2014[2] بتحديث دور المعهد القومي للمعايير والتكنولوجيا (National Institute of Standards and Technology, NIST) ليقوم ب تسهيل ودعم تطوير أطر عمل المخاطر المتعلقة بالأمن السبراني. وفقًا لقانون تحسين الأمن السبراني، يجب على المعهد القومي للمعايير والتكنولوجيا أن يحدّد "منهجية ذات أولويات محددة، مرنة، قابلة للتكرار، مبنية على الأداء، وفعالة من حيث التكلفة، بما في ذلك مقاييس وضوابط أمن المعلومات التي يمكن اعتمادها بشكل اختياري من قبل ملّاك ومشغّلي البنية التحتية الحساسة لتساعدهم على تحديد وتقييم وإدارة المخاطر السبرانية." ساهم ذلك في إضفاء الطابع الرسمي لما قامت به NIST مسبقًا في تطوير إطار العمل بنسخته 1.0 تحت الأمر التنفيذي رقم 13636 "تطوير الأمن السبراني للبنية التحتية الحساسة" في فبراير 2013[3]، كما قدّم الإرشادات نحو التطور المستقبلي لإطار العمل.

تُعرّف البنية التحتية الحساسة[4] في القانون الوطني 2001[5] للولايات المتحدة الأمريكية على أنها "الأنظمة والأصول شديدة الأهمية للولايات المتحدة الأمريكية، سواء مادية أم افتراضية، والتي يتسبب تعطلها أو تدميرها في أثر تدميري على الأمن أو على الأمن الاقتصادي القومي، أو على الصحة والسلامة العامة، أو على أي مزيج من هذه الجوانب." بسبب الضغوط المتزايدة من التهديدات الخارجية والداخلية، تحتاج المنظمات المسؤولة عن البنية التحتية الحساسة لأن يكون لديها منهجية متسقة وقابلة للتكرار لتحديد وتقييم وإدارة المخاطر السبرانية. هذه المنهجية ضرورية بصرف النظر عن حجم المنظمة أو التهديدات التي تواجهها أو درجة تعقيد الأمن السبراني في يومنا هذا.

تضمّ مجالات الأمن السبراني الملّاك والمشغّلين للقطاعين العام والخاص، كما تضم الجهات الأخرى التي تلعب دورًا في تأمين البنية التحتية للأمّة. يقوم كل واحد من أعضاء قطاعات البنية التحتية الحساسة بتأدية وظائف مدعومة بالتصنيف الشامل للتكنولوجيا، بما في ذلك تقنية المعلومات (IT)، أنظمة التحكم الصناعية (ICS)، الأنظمة السبرانية-المادية (CPS)، والأجهزة المرتبطة ببعضها بشكل عام، مثل إنترنت الأشياء (IoT). هذه الاعتمادية على التكنولوجيا والاتصالات والارتباطية قد غيرت وزادت من حجم مواطن الضعف المحتملة، كما زادت المخاطر المحتملة على

---

[2] انظر القانون الفيدرالي رقم 15: 15 U.S.C. § 272(e)(1)(A)(i). قانون تحسين الأمن السبراني لعام 2014 (S.1353) والذي أصبح قانوناً عمومياً برقم 113-274 بتاريخ 18 ديسمبر 2014، ويمكن الوصول إليه عبر الرابط الإلكتروني: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

[3] انظر الأمر التنفيذي رقم 13636، تحسين البنية التحتية الحيوية للأمن السيبراني، إدارة الشرطة بواشنطن العاصمة PCDP -201300091، بتاريخ 12 فبراير 2013. بالموقع الألكتروني: https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

[4] يقدم البنية التحتية الحساسة التابع لوزارة الأمن الوطني (DHS) قائمة بالقطاعات والوظائف الحيوية المرتبطة بها وسلاسل قيمها بالموقع الإلكتروني: http://www.dhs.gov/critical-infrastructure-sectors

[5] انظر الباب 42 من القانون § 5195 c(e)). "قانون المواطنة" الصادر عام 2001، والذي أصبح قانوناً عاماً برقم 107-56 بتاريخ 26 أكتوبر 2001 (H.R.3162) و يمكن الحصول عليه بالموقع الإلكتروني: https://www.congress.gov/bill/107th-congress/house-bill/3162

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

عمليات التشغيل. فعلى سبيل المثال، في الوقت الذي يتزايد فيه مدى استخدام التكنولوجيا والبيانات التي تنتجها وتعالجها لتقديم خدمات حسّاسة ولدعم قرارات الأعمال، يجب أن نضع في عين الاعتبار الآثار المحتملة لحوادث الأمن السبراني على المنظمات وصحة الأفراد وسلامتهم وعلى البيئة والمجتمعات والاقتصاد العام والمجتمع.

لإدارة المخاطر السبرانية، نحتاج إلى فهم واضح للعوامل التي تحرّك أعمال المنظمة والاعتبارات الأمنية المخصصة لكيفية استخدامها للتكنولوجيا. ولأن المخاطر والأولويات والأنظمة في كل منظمة تختلف عن غيرها، فإن الأدوات والطرق المستخدمة لتحقيق النتائج الواردة في إطار العمل ستختلف أيضًا.

من منطلق معرفة إطار العمل بالدور الذي تلعبه حماية الخصوصية والحرّياتِ المدنية في فرض ثقة أكبر عند الناس، فإنه يتضمن منهجًا لحماية الخصوصية الفردية والحريات المدنية أثناء قيام منظمات البنية التحتية الحساسة بنشاطات تتعلق بالأمن السبراني. تمتلك العديد من المنظمات سلفًا عمليات للتعامل مع الخصوصية والحريات المدنية. لقد تم تصميم هذا المنهج ليكون مكمّلًا لهذه العمليات وليقدم الإرشادات التي تيسّر إدارة مخاطر الخصوصية، والتي -أي الإرشادات- تتسق مع منهجية المنظمة في إدارة المخاطر السبرانية. إدخال مسألة الخصوصية في الأمن السبراني سيفيد المنظمات عبر زيادة ثقة العملاء، وإتاحة المزيد من المشاركة المعيارية للمعلومات، وتبسيط العمليات التشغيلية من الجانب القانوني.

سيبقى إطار العمل فعّالًا ويدعم الجديد من الابتكارات التكنولوجية لأنه محايد تكنولوجيًا، في الوقت ذاته الذي يرجع فيه إلى عدة معايير وإرشادات وممارسات موجودة، والتي تتطور بتطور التكنولوجيا. بالاعتماد على تلك المعايير والإرشادات والممارسات العالمية، والتي يتم تطويرها وإدارتها وتحديثها من قبل القطاع الصناعة، ستتخطى الأدوات المتاحة لتحقيق نتائج إطار العمل الحواجز، وستعترف بالطبيعة العامة للمخاطر السبرانية، وستتطور جنبًا إلى جنب مع التقدم التكنولوجي ومتطلبات الأعمال. إن استخدام المعايير الموجودة والمستجدّة سيفسح المجال لاقتصاديات الحجم، كما سيقود تطور المنتجات والخدمات والممارسات ذات الفعالية، والتي تلّبي احتياجات السوق المحددة. علاوة على ذلك، فإن المنافسة السوقية ستحثّ على انتشار أسرع لهذه التقنيات والممارسات، وعلى تحقيق العديد من الفوائد من قبل أصحاب المصلحة في هذه القطاعات.

انطلاقًا من تلك المعايير والإرشادات والممارسات، يقدّم إطار العمل للمنظمات طريقة تصنيف وآلية تنظيم موحَّدّتين من أجل:

1. وصف وضعهم الحالي فيما يخص الأمن السبراني.
2. وصف هدفهم المنشود من الأمن السبراني.
3. تحديد فرص التطور وترتيبها بحسب أولويتها ضمن سياق العمليات المستمرة والمتكررة.
4. تقييم التقدم نحو الهدف.
5. التواصل بين أصحاب المصلحة الداخليين والخارجيين فيما يخص الأمن السبراني.

إن إطار العمل ليس منهجية وُضعت لتناسب الجميع لإدارة مخاطر الأمن السبراني في البنيات التحتية الحساسة، فكلّ منظمة ستظلّ تواجه مخاطر مختلفة عن غيرها – تهديدات مختلفة، ومواطن ضعف مختلفة، ومستويات مختلفة لتحمل المخاطر. كما أن المنظمات ستتباين في طرق تكييفها للممارسات الموصوفة في إطار العمل. يمكن لكل منظمة أن تقرّر النشاطات المهمة لتقديم خدماتها الأساسية، كما يمكنها أن تحدد أولويات الاستثمار لتعظيم المردود من كل دولار يتم إنفاقه. في النهاية، يهدف إطار العمل إلى تقليل المخاطر السبرانية ولإدارتها بشكل أفضل.

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

هنالك طرق متنوعة لاستخدام إطار العمل، وذلك لاستيعاب حاجات الأمن السبراني الفريدة لكل منظمة. إن القرار المتعلق بكيفية تطبيق إطار العمل متروك للمنظمة التي تريد تطبيقه. فمثلًا، قد تختار إحدى المنظمات استخدام مراحل تنفيذ إطار العمل لصياغة الممارسات التي تتصورها لإدارة المخاطر. بينما قد تختار منظمة أخرى أن تستخدم الوظائف الخمسة لإطار العمل من أجل تحليل كامل خطتها لإدارة المخاطر، هذا التحليل قد يعتمد وقد لا يعتمد على المزيد من الإرشادات المفصلة المصاحبة، مثل قوائم الضوابط. تبرز أحيانًا بعض المناقشات حول "التقيد" بإطار العمل، كما تُعتبر "الجدوى" هي هيكلية ولغة إطار العمل لتنظيم التقيد بمتطلبات الأمن السبراني للمنظمة وللتعبير عن هذا التقيد. ومع ذلك، فإن الطرق المتعددة لاستخدام إطار العمل من قبل المنظمة تشير إلى أن عبارات مثل "التقيد بإطار العمل" قد تكون مربكة وذات معنًى مختلف عند كل واحد من أصحاب المصلحة.

هذا الإطار متمّم لعمليات إدارة المخاطر في المنظمة ولبرنامج الأمن السبراني فيها، وليس بديلًا عنهما. يمكن للمنظمة أن تستخدم عملياتها الحالية وأن تستفيد من إطار العمل لتحديد فرص تقوية إدارتها للمخاطر السبرانية وأن تعلن عنها في الوقت الذي تتماشى فيه مع قطاع الصناعة. وإلى جانب ذلك، يمكن للمنظمات التي لا تملك برنامج أمن سبراني أن تستفيد من إطار العمل كمرجعية لتأسيس برنامجها الخاص.

على الرغم من أن إطار العمل قد تم تطويره لتحسين إدارة المخاطر السبرانية فيما يخص البنية التحتية الحساسة، يمكن للمنظمات أيضًا أن تستخدمه في أي قطاع من قطاعات الاقتصاد أو المجتمع. إن الهدف من الإطار هو أن يكون مفيدًا للشركات والهيئات الحكومية والمنظمات غير الربحية، بغض النظر عن مجال تركيزهم أو حجمهم. طريقة التصنيف الموحّدة للمعايير والإرشادات والممارسات التي يقدّمها الإطار لا تختص ببلد معيّن كذلك. يمكن أيضًا للمنظمات خارج الولايات المتحدة الأمريكية أن تستعين بإطار العمل لتقوية جهودها في الأمن السبراني، كما يمكن للإطار أن يساهم في تطوير لغة مشتركة للتعاون الدولي فيما يخص الأمن السبراني للبنية التحتية الحساسة.

1.1 نظرة عامة على الإطار

هذا الإطار هو منهجية تقوم على أساس المخاطر لإدارة المخاطر السبرانية، وتتكون من ثلاثة أجزاء: نواة إطار العمل، ومراحل تنفيذ إطار العمل، ونماذج إطار العمل. كل واحد من هذه الأجزاء يعزز الرابطة ما بين الدوافع التي تقود الأعمال والمهمات، وبين نشاطات الأمن السبراني. فيما يلي شرح لهذه الأجزاء.

- نواة إطار العمل هي مجموعة من نشاطات الأمن السبراني والنتائج المنشودة والمراجع القابلة للتطبيق، والتي تشترك فيها قطاعات البنية التحتية الحساسة. تمثّل النواة معايير الصناعة وإرشاداتها وممارستها بشكل يسمح بتناقل نشاطات الأمن السبراني ونتائجه عبر المنظمة ابتداءً من مستوى الإدارة التنفيذية إلى مستوى العمليات التشغيلية أو التطبيقية. تتكون نواة إطار العمل من خمس وظائف متزامنة ومستمرة : التحديد، والحماية، والرصد، والاستجابة، والاستعادة. عندما يُنظر إليها معًا، يمكن لهذه الوظائف أن تقدم نظرة استراتيجية عامة على دورة حياة إدارة المخاطر السبرانية في المنظمة. بعدها، تقوم نواة إطار العمل بتحديد التصانيف الرئيسية والتصانيف الفرعية – وهي مخرجات منفصلة عن بعضها – لكل وظيفة، كما تقوم بربطها بأمثلة لمراجع ذات قيمة علمية، مثل المعايير والإرشادات والممارسات الموجودة لكل تصنيف فرعي.
- مراحل تنفيذ إطار العمل (المراحل) تقدّم سياقًا حول الطريقة التي تنظر بها المنظمة إلى المخاطر السبرانية والعمليات القائمة لإدارة تلك المخاطر. تصف المراحل الدرجة الذي تقوم فيه إدارة المخاطر السبرانية في المنظمة بإظهار خواصها المعرَّفة في إطار العمل (من هذه الخواص: الوعي بالمخاطر والتهديدات، القابلية للتكرار، والتكيف). تصف المراحل ممارسات المنظمة على شكل نطاق، يبدأ من الجزئي (المرحلة 1)، وينتهي

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

بالتكيف (المرحلة 4). تعكس هذه المراحل التقدم من الاستجابات غير الرسمية والقائمة على ردات الفعل إلى المنهجيات الرشيقة والواعية بالمخاطر. خلال عمليات اختيار المرحلة، ينبغي على المنظمة أن تضع في عين الحسبان ممارساتها الحالية لإدارة المخاطر، وبيئة التهديدات المحيطة بها، والمتطلبات القانونية والتنظيمية، وأهداف الأعمال، وقيودها المنظمية.

- نماذج إطار العمل (النماذج) تمثّل المخرجات المبنية على احتياجات الأعمال التي اختارتها المنظمة من تصنيفات إطار العمل الرئيسية والفرعية. يمكن أن يوصف النموذج بأنه موائمة المعايير والإرشادات والممارسات مع نواة إطار العمل في سيناريو تنفيذي معين. يمكن استخدام النماذج لتحديد فرص تطوير حالة الأمن السبراني عن طريق مقارنة نموذج حالي (بحالته كما هي الآن) مع النموذج الهدف (الحالة المنشودة). لوضع النموذج، يمكن للمنظمة أن تستعرض جميع التصنيفات الرئيسية والفرعية، لتحدد بعدها أيها أشد أهمية بناء على دوافع الأعمال وتقييم المخاطر؛ يمكنها أن تضيف تصنيفات رئيسية وفرعية بحسب حاجتها للتعامل مع المخاطر التي تواجهها. بعدها، يمكن أن يتم استخدام النموذج الحالي لدعم عملية وضع الأولويات ومقاييس التقدم نحو النموذج الهدف، مع مراعاة الاحتياجات الأخرى للأعمال مثل فعالية التكلفة والابتكار. يمكن أن تُستخدم النماذج لإجراء تقييمات ذاتية وللتواصل في داخل المنظمة أو فيما بين المنظمات.

1.2 إدارة المخاطر وإطار عمل الأمن السبراني

إدارة المخاطر هي العملية المتواصلة لتحديد وتقييم والاستجابة للمخاطر. لكي تتم إدارة المخاطر، يجب على المنظمة أن تعرف احتمالية أن يقع حدث ما والآثار المحتملة له. بهذه المعلومات يمكن للمنظمة أن تحدد المستوى المقبول من المخاطر لتحقيق أهدافها كمنظّمة، ويمكن أن تعبّر عن هذا المستوى المقبول بأنه درجة تحملها للمخاطر.

عبر معرفة درجة تحمل المخاطر، يمكن للمنظمة أن تحدد أولويات نشاطات الأمن السبراني، مما يتيح لها اتخاذ قرارات مدروسة فيما يتعلق بنفقات الأمن السبراني. تطبيق برامج إدارة المخاطر يعطي المنظمة القدرة على تحديد كمية التعديلات اللازمة على برامج الأمن السبراني ومشاركتها. يمكن للمنظمات أن تختار التعامل مع المخاطر بطرق مختلفة، مثل تخفيفها، أو تحويلها، أو تجنبها، أو قبولها، وذلك اعتمادًا على الأثر المحتمل على تقديم الخدمات الحساسة. يستخدم إطار العمل عمليات إدارة المخاطر لكي يتيح للمنظمة اتخاذ قرارات مستنيرة وترتيبها بحسب أولويتها فيما يتعلق بالأمن السبراني. كما يدعم إطار العمل عمليات تقييم المخاطر المتكررة والتحقق من صحة دوافع الأعمال، وذلك لمساعدة المنظمات في اختيار الحالات المنشودة لنشاطات الأمن السبراني والتي تعكس النتائج المرغوبة. لذلك، يعطي إطار العمل المنظمات القدرة على اختيار وتوجيه عملية تحسين إدارة المخاطر السبرانية بشكل ديناميكي في بيئات تقنية المعلومات وأنظمة التحكم الصناعي.

يمكن تكييف إطار العمل لتقديم تطبيقات مرنة وتقوم على أساس المخاطر، والتي يمكن استخدامها مع مجموعة كبيرة من عمليات إدارة المخاطر السبرانية. من الأمثلة على عمليات إدارة المخاطر السبرانية:
International Organization for Standardization (ISO) 3100:2009[6], ISO/International Electrotechnical Commission (IEC) 27005:2011[7], NIST Special Publication (SP) 800-39[8], Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline[9].

---

6 المنظمة الدولية للمعايير (أيزو)، "إدارة المخـاطر" – المبادئ والخطوط التوجيهية ISO 31000:2009, 2009
http://www.iso.org/iso/home/standards/iso31000.htm

7 المنظمة الدولية للمعايير / اللجنة الكهرو تقنية الدولية، تكنولوجيــــا المعلومات – تقنيات الأمن - إدارة مخاطر أمن المعلومات – ISO/IEC27005:2011 ، 2011 بالموقع الإلكتروني https://www.iso.org/standard/56742.html

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

1.3 نظرة عامة على المستند

ما تبقى من هذا المستند يحتوي على الأقسام والملحقات التالية:

- القسم 2 يصف مكونات إطار العمل: نواة إطار العمل، المراحل، والنماذج
- القسم 3 يطرح أمثلة لكيفية استخدام إطار العمل
- القسم 4 يصف كيفية استخدام إطار العمل في التقييم الذاتي ولإظهار الأمن السبراني من خلال المقاييس.
- ملحق (أ) يقدم نواة إطار العمل في شكل مجدول: الوظائف، والتصنيفات، والتصنيفات الفرعية، والمراجع المعرفية
- ملحق (ب) يحتوي على فهرس لبعض المصطلحات
- ملحق (ج) يحتوي على قائمة باختصارات المصطلحات المستخدمة في هذا المستند

[8] مبادرة التحول لفريق المهمات المشتركة، إدارة مخاطر أمن المعلومات: التنظيم، والمهمة، ونظرة على نظم المعلومات، المنشور الخاص الصادر عن المعهد الوطني للمعايير والتكنولوجيا NIST برقم 800-39 ، بتاريخ مارس 2011 بالموقع الإلكتروني https://doi.org/10.6028/NIST.SP.800-39

[9] وزارة الطاقة بالولايات المتحدة، لقطاع الكهرباء "العمليات إدارة مخاطر الأمن السبراني"، برقم DOE/OE-0003 بتاريخ مايو {آيار} بالموقع الإلكتروني: https://energy.gov/sites/prod/files/Cybersecurity Risk Management Process Guideline - Final - May 2012.pdf

2.0 أساسيات إطار العمل

يقدم إطار العمل لغةً مشتركة لفهم مخاطر الأمن السبراني وإدارتها والتعبير عنها أمام أصحاب المصلحة الداخليين والخارجيين. يمكن استخدام إطار العمل للمساعدة في تحديد وتحديد أولويات إجراءات تخفيف المخاطر السبرانية، كما أنه أداة لمواءمة السياسات والأعمال والمنهجيات التكنولوجية مع بعضها البعض بهدف إدارة تلك المخاطر. يمكن استخدامه لإدارة المخاطر السبرانية عبر كامل المنظمات، أو أن يتم تركيز استخدامه على جانب تقديم الخدمات الحساسة ضمن المنظمة. يمكن للأنواع المختلفة من الجهات – مثل هيئات تنسيق القطاعات والجمعيات والمنظمات – أن تستخدم إطار العمل لتحقيق أغراض مختلفة، مثل إنشاء نماذج مشتركة.

2.1 نواة إطار العمل

يقدم إطار العمل مجموعة من النشاطات لتحقيق نتائج محددة في الأمن السبراني، كما يتضمن إشارة إلى أمثلة على إرشادات تساعد في تحقيق تلك النتائج. ليست النواة قائمةً بالإجراءات التي ينبغي تأديتها، ولكنها تطرح نتائج أساسية في مجال الأمن السبراني تم تحديدها من قبل أصحاب المصلحة على أنها مفيدة في إدارة المخاطر السبرانية. تتكون النواة من أربعة عناصر: الوظائف، والتصنيفات، والتصنيفات الفرعية، والمراجع المعرفية. انظر إلى الشكل 1:

شكل 1:بنية نواة إطار العمل

تعمل عناصر نواة إطار العمل معًا على النحو التالي:

- **الوظائف:** تقوم بتنظيم نشاطات الأمن السبراني الأساسية في مستواها الأعلى. هذه الوظائف هي: التحديد، والحماية، والرصد، والاستجابة، والاستعادة. تساعد هذه الوظائف الخمس المنظمةَ في التعبير عن إدارتها للمخاطر السبرانية عن طريق تنظيم المعلومات، وتفعيل قرارات إدارة المخاطر، وتحديد التهديدات، والتحسين المبني على الاستفادة من النشاطات السابقة. كما تتواءم هذه الوظائف مع الطرق الموجودة لإدارة الحوادث، وتساعد في إظهار أثر الاستثمارات في الأمن السبراني. فعلى سبيل المثال، يعزز الاستثمار في

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

التخطيط والتدريب من القدرة على الاستجابة والاستعادة في الوقت المناسب، مما يؤدي إلى تأثير أقل على سير عملية تقديم الخدمات.

- **التصنيفات**: هي تقسيم الوظيفة الواحدة إلى مجموعات من مخرجات الأمن السبراني، والتي ترتبط بشكل وثيق باحتياجات البرامج وبأنشطة معينة. من الأمثلة على التصنيفات: "إدارة الأصول"، و"إدارة الهوية والتحكم بالوصول"، و"عمليات الرصد".

- **التصنيفات الفرعية:** هي تقسيم إضافي للتصنيف الواحد إلى مخرجات محددة من النشاطات الفنية و/أو الإدارية. تقدم التصنيفات الفرعية مجموعة من النتائج التي – ومن دون حصر – تساعد في تحقيق مخرجات كل تصنيف. من الأمثلة على التصنيفات الفرعية: "أنظمة المعلومات الخارجية مفهرسة"، و"البيانات المستقرة محمية"، و"إشعارات أنظمة الرصد يتم التحقيق فيها".

- **المراجع المعرفية**: هي أقسام مخصصة للمعايير والإرشادات والممارسات الشائعة بين قطاعات البنية التحتية الحساسة، والتي – أي المعايير – تطرح منهجية لتحقيق المخرجات المرتبطة بكل تصنيف فرعي. المراجع المعرفية المذكورة في إطار العمل تم وضعها على سبيل الإيضاح لا الحصر. هذه المراجع المعرفية مبنية على التوجيهات التي تكثر الإشارة إليها من قبل القطاعات أثناء فترة تطوير إطار العمل.

في الأسفل تعريف للوظائف الخمسة لنواة إطار العمل. ليس الهدف من هذه الوظائف الخمسة تشكيل مسار تسلسلي أو أن تقود إلى هدف نهائي ثابت، إنما ينبغي أن يتم تطبيقها بشكل متزامن ومتواصل لتشكيل ثقافة عملية يمكنها التعامل مع ديناميكية المخاطر السبرانية. انظر الملحق (أ) للاطلاع على القائمة الكاملة لنواة إطار العمل.

- **التحديد**: تطوير فهم منظّمي لإدارة المخاطر السبرانية على الأنظمة والأشخاص والأصول والبيانات والإمكانيات. النشاطات الموجودة في وظيفة التحديد هي أساس لاستخدام إطار العمل بشكل فعال. فهم سياق الأعمال والمصادر التي تدعم الوظائف الحساسة والمخاطر السبرانية المتعلقة بذلك يتيح للمنظمة تركيز جهودها وترتيبها بحسب أولويتها بما يتسق مع استراتيجيتها لإدارة المخاطر ومع احتياجات الأعمال. من الأمثلة على التصنيفات التابعة لهذه الوظيفة: إدارة الأصول، بيئة الأعمال، الحوكمة، تقييم المخاطر، استراتيجية إدارة المخاطر.

- **الحماية**: تطوير وتطبيق وسائل الحماية المناسبة للتأكد من سير عملية تقديم الخدمات الحساسة. تدعم وظيفة الحماية القدرة على الحد من أو احتواء أثر أحداث الأمن السبراني المحتملة. من الأمثلة على التصنيفات التابعة لهذه الوظيفة: إدارة الهويات والتحكم بالوصول، الوعي والتدريب، أمن البيانات، عمليات وإجراءات أمن المعلومات، الصيانة، التكنولوجيا الوقائية.

- **الرصد**: تطوير وتطبيق النشاطات المناسبة لتحديد وقوع أحداث الأمن السبراني. تتيح وظيفة الرصد اكتشاف أحداث الأمن السبراني في الوقت المناسب. من الأمثلة على التصنيفات التابعة لهذه الوظيفة: الحالات غير الطبيعية والأحداث، المراقبة الأمنية المستمرة، عمليات الرصد.

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

- **الاستجابة**: تطوير وتطبيق النشاطات المناسبة لاتخاذ الإجراءات في حال رصد حادث أمن سبراني. تدعم وظيفة الاستجابة القدرة على احتواء أثر حوادث الأمن السبراني المحتملة. من الأمثلة على التصنيفات التابعة لهذه الوظيفة: خطط الاستجابة، الاتصالات، التحليل، التخفيف، التحسين.

- **الاستعادة**: تطوير وتطبيق النشاطات المناسبة لوضع الخطط لتعزيز الصمود واستعادة أية إمكانيات أو خدمات تعطلت بسبب حادث أمن سبراني. تدعم وظيفة الاستعادة استعادة العمليات الطبيعية في الوقت المناسب للتخفيف الأثر الناجم عن حوادث الأمن السبراني. من الأمثلة على التصنيفات التابعة لهذه الوظيفة: خطط الاستعادة، التحسين، الاتصالات.

2.2 مراحل التطبيق

توفّر مراحل التطبيق "المراحل" سياقًا لكيفية نظرة المنظمة إلى المخاطر السبرانية والعمليات المعمول بها لإدارة تلك المخاطر. في تراوحها ما بين المرحلة الجزئية (المرحلة 1) وبين المرحلة التكيفية (المرحلة 4)، تصف المراحل الدرجة المتزايدة من الدقة والتعقيد في ممارسات إدارة المخاطر السبرانية. تساعد هذه المراحل في تعيين مدى معرفة إدارة المخاطر السبرانية باحتياجات الأعمال، وكذلك مدى اندماجها في الممارسات العامة لإدارة المخاطر في المنظمة. تتضمن اعتباراتُ إدارة المخاطر العديد من جوانب الأمن السبراني، بما في ذلك مدى حضور اعتبارات الخصوصية والحريات المدنية في إدارة المخاطر السبرانية لدى المنظمة وفي استجابتها للمخاطر المحتملة.

تضع عملية اختيار المرحلة في عين الحسبان الممارسات الحالية لإدارة المخاطر، وبيئة المخاطر، والمتطلبات القانونية والتنظيمية، وممارسات مشاركة المعلومات، وأهداف الأعمال والرؤية، وسلسلة الإمداد، والقيود المنظمية لدى المنظمة. ينبغي على المنظمات أن تحدد المرحلة المرغوبة، مع التأكد من أن المستوى المختار يخدم أهداف المنظمة وقابل للتطبيق ويقلل من المخاطر السبرانية على الأصول والمصادر الحساسة إلى درجة تتقبلها المنظمة. ينبغي على المنظمات أن تضع في عين الاعتبار الاستفادة من الإرشادات الخارجية المستمدة من دوائر وهيئات الحكومة الفدرالية، ومراكز مشاركة وتحليل المعلومات (ISACs)، ومنظمات مشاركة وتحليل المعلومات (ISAOs)، ومستويات النضج الحالية، وغيرها من المصادر بهدف الاستعانة بها في تحديد المرحلة المرغوبة.

في حين أننا نحث المنظمات المصنفة بأنها مرحلة 1 (المرحلة الجزئية) على أن تنتقل إلى المرحلة 2 أو أعلى، إلا أن المراحل لا تمثّل مستويات النضج. إن الهدف من المراحل هو دعم اتخاذ القرار في المنظمة فيما يتعلق بكيفية إدارة المخاطر السبرانية، وفيما يتعلق أيضًا بأيّ أبعاد المنظمة هي ذات أولوية أعلى ويمكنها أن تحصل على المزيد من المصادر. يُنصح بالتقدم إلى مرحلة أعلى عندما تشير تحليلات فعالية التكلفة إلى إمكانية الحد من المخاطر السبرانية بشكل مجدٍ وفعال من حيث التكلفة.

يمكن الحصول على نسخة مجانية من هذا المنشــور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

يعتمد النجاح في تطبيق إطار العمل على تحقيق المخرجات المذكورة في النموذج (أو النماذج) الهدف للمنظمة، وليس على المرحلة المحددة. ومع ذلك فإن اختيار وتعيين المرحلة يؤثر بشكل طبيعي على نماذج إطار العمل. ستساعد توصية المراحل المقدمة من قبل مديري مستوى الأعمال، كما هي موافق عليها من قبل الإدارة العليا، على تحديد المناخ العام الذي تتم فيه إدارة المخاطر السبرانية ضمن المنظمة، كما ينبغي أن يؤثر أيضًا في عملية وضع الأولويات في النموذج الهدف وتقييمات التقدم في معالجة الثغرات.

فيما يلي تعريف بكل مرحلة من المراحل:

المرحلة 1: المرحلة الجزئية

- عملية إدارة المخاطر: ممارسات المنظمة في إدارة المخاطر السبرانية ليس لها طابع رسمي، والمخاطر يتم إدارتها بطريقة مخصصة لكل حالة، وبعض الأحيان على شكل ردود فعل. قد لا تكون الأولويات الخاصة بنشاطات الأمن السبراني قد وُضعت بناءً على أهداف المنظمة المتعلقة بالمخاطر، أو بيئة التهديدات، أو متطلبات الأعمال.
- برنامج إدارة المخاطر المتكامل: يوجد وعي محدود بالمخاطر السبرانية على مستوى المنظمة. تقوم المنظمة بتطبيق إدارة المخاطر السبرانية على فترات غير منتظمة وعلى أساس كل حالة على حدى، وذلك بسبب الخبرة المتنوعة أو المعلومات المكتسبة من مصادر خارجية. قد لا تمتلك المنظمة عمليات تتيح مشاركة معلومات الأمن السبراني ضمن المنظمة.
- المشاركة الخارجية: لا تعرف المنظمة دورها في البيئة الكبرى فيما يتعلق بالأطراف التي تعتمد على المنظمة أو بتلك التي تعتمد المنظمة عليها. لا تتعاون المنظمة مع الجهات الأخرى (مشترين، موزعين، أطراف معتمد عليها، أطراف تعتمد على المنظمة، منظمات مشاركة وتحليل المعلومات ISAOs، الباحثين، الحكومات) ولا تستقبل المعلومات منها (عن التهديدات، والممارسات المثلى، والتقنيات)، كما أنها لا تشارك هذه المعلومات مع الآخرين. بشكل عام، المنظمة غير واعية بالمخاطر السبرانية لسلاسل الإمداد والمتعلقة بالمنتجات والخدمات التي تقدمها أو تستخدمها.

المرحلة 2: مرحلة الوعي بالمخاطر

- عملية إدارة المخاطر: ممارسات إدارة المخاطر تمت الموافقة عليها من قبل الإدارة ولكن قد لا يتم اعتمادها كسياسة عامة في كامل المنظمة. تم وضع الأولويات وحاجات الحماية المتعلقتين بنشاطات الأمن السبراني بناءً على أهداف المنظمة المتعلقة بالمخاطر، أو بيئة التهديدات، أو متطلبات الأعمال.
- برنامج إدارة المخاطر المتكامل: يوجد وعي بالمخاطر السبرانية على مستوى المنظمة، إلا أنه لم يتم وضع منهجية لإدارة المخاطر السبرانية تشمل كل المنظمة. تتم مشاركة معلومات الأمن السبراني ضمن المنظمة بشكل غير رسمي. يتم أخذ الأمن السبراني في عين الاعتبار عند وضع الأهداف والبرامج المنظمية في بعض مستويات المنظمة وليس جميعها. هنالك تقييم للمخاطر السبرانية على الأصول المنظمية والخارجية، إلا أنه لا تتم إعادة التقييم بشكل معتاد.
- المشاركة الخارجية: بشكل عام، تعرف المنظمة دورها في البيئة الكبرى فيما يتعلق إما بالأطراف التي تعتمد على المنظمة أو بتلك التي تعتمد المنظمة عليها، ولكن ليس كليهما. تتعاون المنظمة مع الجهات الأخرى وتستقبل منها بعض المعلومات، كما تقوم بإنتاج معلوماتها الخاصة، إلا أنها قد لا تشارك هذه المعلومات مع الآخرين. بالإضافة إلى ذلك، المنظمة واعية بالمخاطر السبرانية لسلاسل الإمداد والمتعلقة بالمنتجات والخدمات التي تقدمها أو تستخدمها، ولكنها لا تتصرف بشكل مستمر أو رسمي حيال تلك المخاطر.

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

المرحلة 3: مرحلة قابلية التكرار

- عملية إدارة المخاطر: ممارسات إدارة المخاطر تمت الموافقة عليها رسميًا وتُعتبر واحدة من سياسات المنظمة. يتم تحديث ممارسات الأمن السبراني للمنظمة بشكل على فترات منتظمة بناءً على تطبيق عمليات إدارة المخاطر على التغيرات في متطلبات الأعمال/رؤية المنظمة والأفق المتغير للتهديدات والتكنولوجيا.
- برنامج إدارة المخاطر المتكامل: هنالك منهجية على مستوى المنظمة لإدارة المخاطر السبرانية. تم تعريف السياسات والعمليات والإجراءات المبنية كلها على الوعي بالمخاطر، كما يتم تطبيقها كما هو مقرر ومراجعتها. الطرق المتسقة مع بعضها البعض جاهزة للاستجابة بشكل فعال للتغيرات في المخاطر. يمتلك الموظفون المعرفة والمهارات اللازمة لتأدية أدوارهم ومسؤولياتهم المقررة. تراقب المنظمة على المخاطر السبرانية على الأصول المنظمية على نحو متواصل ودقيق. يتواصل كبار التنفيذيين للأمن السبراني ولغير الأمن السبراني على نحو منتظم فيما يخص المخاطر السبرانية. يقوم كبار التنفيذيين بالتأكد من الاهتمام بالأمن السبراني في كل خطوط التشغيل داخل المنظمة.
- المشاركة الخارجية: تفهم المنظمة دورها والأطراف التي تعتمد – المنظمة – عليها والأطراف التي تعتمد على المنظمة ضمن البيئة الكبرى، وقد تساهم في زيادة فهم هذا المجتمع للمخاطر. تتعاون المنظمة وعلى نحو منتظم مع الجهات الأخرى وتستقبل منها المعلومات التي تكمّل المعلومات التي تنتجها داخليًا، كما تشارك المعلومات مع الجهات الأخرى. كما أنها على وعي بالمخاطر السبرانية لسلسلة الإمداد والمتعلقة بالمنتجات والخدمات التي تقدمها أو تستخدمها. بالإضافة إلى ذلك، تتصرف المنظمة بشكل رسمي حيال تلك المخاطر، بما في ذلك وجود آليات مثل الاتفاقيات الخطية للإبلاغ عن متطلبات خط الأساس وإنشاء هياكل الحوكمة (مثل مجالس شؤون المخاطر)، وتطبيق ومراقبة السياسات.

المرحلة 4: مرحلة التكيف:

- عملية إدارة المخاطر: تقوم المنظمة بتكييف ممارسات الأمن السبراني بناءً على نشاطات الأمن السبراني السابقة والحالية، بما في ذلك الدروس المستفادة والمؤشرات التنبئية. من خلال عملية التحسين المستمر الذي يتضمن دمج تقنيات وممارسات الأمن السبراني المتقدمة، تتكيف المنظمة على نحو نشط مع التهديدات والتكنولوجيا المتغيرتين، كما تستجيب في الوقت المناسب وبشكل فعال للتهديدات المتطورة والمعقدة.
- برنامج إدارة المخاطر المتكامل: هنالك منهجية على مستوى المنظمة لإدارة المخاطر السبرانية تستخدم السياسات والعمليات والإجراءات المبنية كلها على الوعي بالمخاطر للتعامل مع أحداث الأمن السبراني المحتملة. العلاقة بين المخاطر السبرانية وأهداف المنظمة مفهومة بشكل واضح وتدخل في عملية اتخاذ القرارات. كبار التنفيذيين يراقبون المخاطر السبرانية على حد سواء مع مراقبتهم للمخاطر المالية والمخاطر الأخرى التي تواجه المنظمة. ميزانية المنظمة مبنية على فهم الوضع الحالي والوضع المتوقع لبيئة المخاطر ولمستوى تحمل المخاطر. تقوم وحدات العمل بتطبيق الرؤية التنفيذية وتحليل المخاطر التي على مستوى النظام ضمن سياق مستوى تحمل المنظمة للمخاطر. إدارة المخاطر السبرانية تشكل جزءًا من ثقافة المنظمة، وتنبثق من الدراية بالنشاطات السابقة ومن الوعي المستمر بالنشاطات المطبقة على الأنظمة والشبكات. تستطيع المنظمة استيعاب التغيرات الطارئة على أهداف الأعمال/الرؤية في كيفية التعامل مع المخاطر والإبلاغ عنها.
- المشاركة الخارجية: تفهم المنظمة دورها والأطراف التي تعتمد – المنظمة – عليها والأطراف التي تعتمد على المنظمة ضمن البيئة الكبرى، وتساهم في زيادة فهم هذا المجتمع للمخاطر. كما تقوم باستقبال وإنتاج ومراجعة المعلومات المرتبة حسب أولويتها والتي تغذّي التحليل المتواصل لمخاطر المنظمة في ظل تزايد التهديدات وتطور التكنولوجيا. تشارك المنظمة تلك المعلومات داخليًا وخارجيًا مع متعاونين آخرين. تستخدم المنظمة معلومات فورية أو شبه فورية لفهم والتصرف حيال المخاطر السبرانية

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

لسلسلة الإمداد المتعلقة بالمنتجات والخدمات التي تقدمها أو تستخدمها. تتواصل الشركة مع الآخرين بشكل استباقي باستخدام الآليات الرسمية (مثل الاتفاقيات) وغير الرسمية لتطوير علاقات قوية مع سلاسل الإمداد وللمحافظة عليها.

2.3 نماذج إطار العمل

نموذج إطار العمل ("النموذج") هو مواءمة الوظائف والتصنيفات والتصنيفات الفرعية مع متطلبات الأعمال، ومستوى تحمل المخاطر، وموارد المنظمة. يتيح النموذج للمنظمات تأسيس خارطة طريق لتقليل المخاطر السبرانية تتواءم مع الأهداف المنظمية، كما يضع -النموذج- في عين الاعتبار المتطلبات القانونية/التنظيمية والممارسات المثلى ضمن مجال الصناعة ويعكس أولويات إدارة المخاطر. نظرًا لتعقيد العديد من المنظمات، يمكن للمنظمة أن تختار أكثر من نموذج يتواءم مع مكوّنات محددة ويلبي احتياجاتها الفردية.

يمكن استخدام نماذج إطار العمل لوصف الحالة الراهنة أو الحالة المنشودة لبعض نشاطات الأمن السبراني المحددة. النموذج الراهن يشير إلى مخرجات الأمن السبراني المحققة في الوقت الراهن. النموذج الهدف يشير إلى المخرجات المنشودة لتحقيق أهداف إدارة المخاطر السبرانية. تدعم النماذجُ متطلباتِ الأعمال/الرؤية وتعينها في الإبلاغ عن المخاطر ضمن المنظمة نفسها وبين المنظمات الأخرى. لا يتضمن إطار العمل هذا على وصف لقوالب جاهزة للنماذج، مما يتيح مرونة أكثر في التطبيق.

قد تكشف المقارنة بين النماذج (مثل مقارنة النموذج الراهن مع النموذج الهدف) عن الفجوات التي ينبغي التعامل معها لتحقيق أهداف إدارة المخاطر السبرانية. قد تساهم خطة العمل للتعامل مع هذه الفجوات بهدف تحقيق تصنيف أو تصنيف فرعي معين، قد تساهم في خارطة الطريق الموصوفة أعلاه. أولويات سد الفجوات يتم ترتيبها بناءً على احتياجات الأعمال وعمليات إدارة المخاطر. هذه المنهجية المبنية على المخاطر تتيح للمنظمة تقدير الموارد اللازمة (مثل الموظفين والتمويل) لتحقيق أهداف الأمن السبراني على نحو فعال من حيث التكلفة وذي أولويات مرتبة. بالإضافة إلى ذلك، إطار العمل هو منهجية مبنية على المخاطر، حيث قابلة التطبيق وتحقيق تصنيف فرعي معين يخضعان لنطاق النموذج.

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

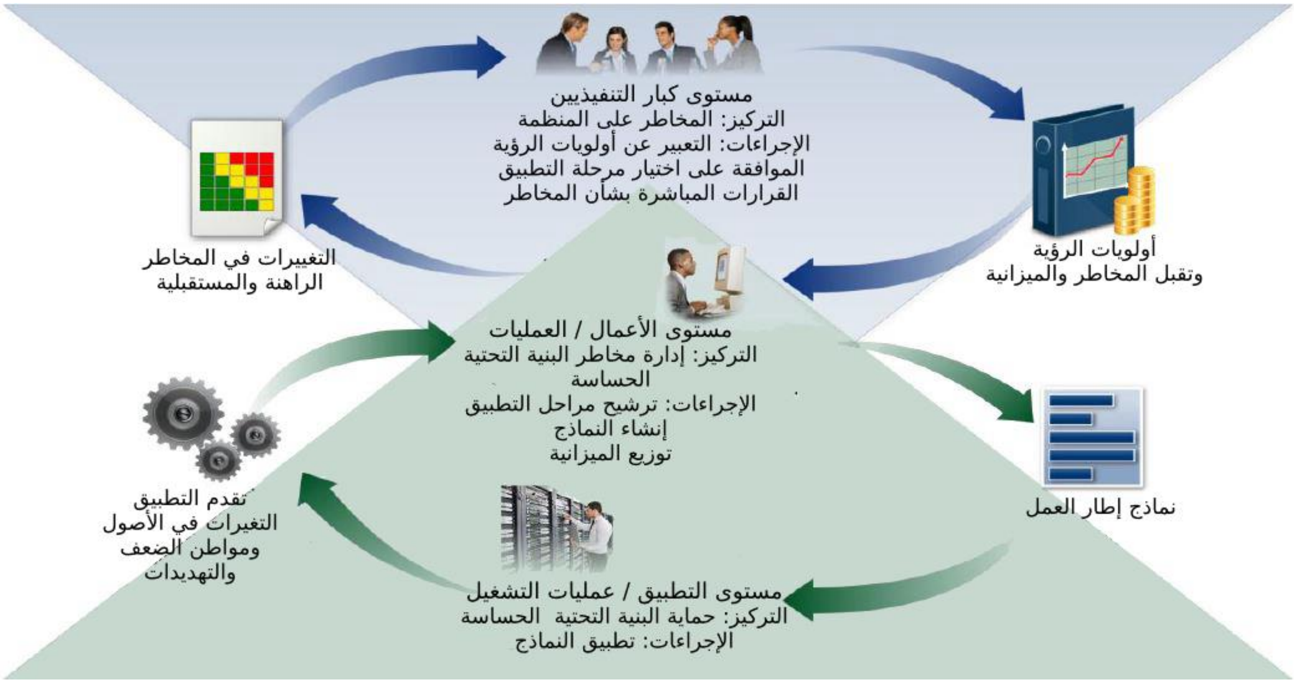
2.4 تنسيق تطبيق إطار العمل

يصف الشكل 2 التدفق الشائع للمعلومات والقرارات في المستويات التالية ضمن المنظمة:

- المستوى التنفيذي
- مستوى الأعمال/العمليات
- مستوى التطبيق/عمليات التشغيل

يقوم المستوى التنفيذي بإبلاغ مستوى الأعمال/العمليات بأولويات الرؤية والموارد المتاحة والمستوى العام لتقبل المخاطر. أما مستوى الأعمال/العمليات فيستخدم هذه المعلومات كمدخلات في عملية إدارة المخاطر، ومن ثم يتعاون مع مستوى التطبيق/عمليات التشغيل لإبلاغه باحتياجات الأعمال ولصنع النموذج. يقوم مستوى التطبيق/عمليات التشغيل بإبلاغ مستوى الأعمال/العمليات بشأن التقدم في تطبيق النموذج. بعدها، يستخدم مستوى الأعمال/العمليات هذه المعلومات للقيام بتقييم الأثر. ثم يقوم مستوى الأعمال/العمليات بتقديم تقرير إلى المستوى التنفيذي عن نتائج تقييم الأثر بهدف تبيان عملية إدارة المخاطر، كما يقدم التقرير إلى مستوى التطبيق/عمليات التشغيل بهدف التوعية بالأثر على الأعمال.

إدارة المخــاطر



شكل 2: تدفق المعلومات والقرارات في المنظمة

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

3.0 كيفية استخدام إطار العمل

يمكن للمنظمة أن تستخدم إطار العمل كجزء مهم من عمليتها المنهجية لتحديد وتقييم وإدارة المخاطر السبرانية. إن إطار العمل غير مصمم لاستبدال العمليات الموجودة، فبإمكان المنظمة أن تبقى على استخدام عملياتها الحالية مع وضعها تحت غطاء إطار العمل لتحديد الفجوات في منهجيتها الحالية حيال المخاطر السبرانية ولرسم خارطة طريق تقود نحو التحسين. باستخدام إطار العمل كأداة لإدارة المخاطر السبرانية، يمكن للمنظمة أن تقرر النشاطات الأكثر أهمية في عملية تقديم الخدمات الحساسة، كما يمكنها أن ترتب النفقات بحسب أولويتها لتعظيم أثر الاستثمار.

إن إطار العمل مصمم لتكميل العمليات التشغيلية الموجودة والمتعلقة بالأعمال والأمن السبراني. يمكن للإطار أن يكون قاعدة لبناء برنامج جديد للأمن السبراني، أو لوضع آلية لتحسين البرنامج الموجود. يقدم إطار العمل وسائل للتعبير عن متطلبات الأمن السبراني أمام شركاء الأعمال والعملاء، كما يساعد في تحديد الفجوات في ممارسات الأمن السبراني لدى المنظمة. كما يقدم مجموعة عامة من الاعتبارات والعمليات للنظر في الآثار المترتبة على الخصوصية والحريات المدنية ضمن سياق برنامج الأمن السبراني.

يمكن تطبيق إطار العمل عبر جميع مراحل دورة الحياة المكونة من التخطيط والتصميم والبناء/الشراء والنشر والتشغيل وإيقاف التشغيل. مرحلة التخطيط هي بداية دورة الحياة لكل نظام، وهي التي تمهّد الطريق لكل ما بعدها. ينبغي الإعلان عن اعتبارات الأمن السبراني الشاملة ووصفها بأقصى ما يمكن من الوضوح، كما ينبغي على الخطة أن تدرك أنه من المحتمل أن تلك الاعتبارات والمتطلبات سوف تتطور خلال ما تبقى من دورة الحياة. ينبغي أن تستوعب مرحلة التصميم متطلباتِ الأمن السبراني كجزء من عملية أكبر لهندسة الأنظمة متعددة التخصصات[10]. أحد أبرز الإنجازات في مرحلة التصميم هو التحقق من أن مواصفات نظام الأمن السبراني تلبّي احتياجات المنظمة ومتطلباتها للتخلص من المخاطر كما هو مذكور في نموذج إطار العمل. ينبغي أن تُدرج مخرجات الأمن السبراني المرغوبة والمرتبة حسب أولويتها في النموذج الهدف في الحالات التالية: 1) تطوير النظام أثناء مرحلة البناء؛ 2) شراء النظام أو تسليم تطويره إلى مصادر خارجية خلال مرحلة الشراء. ذلك النموذج الهدف نفسه يمكن أن يكون بمثابة قائمة من خصائص الأمن السبراني التي ينبغي تقييمها عند نشر النظام للتأكد من أن جميع الخصائص قد تم تطبيقها. بعدها، ينبغي على مخرجات الأمن السبراني المحددة بواسطة إطار العمل أن تكون القاعدة للعمليات الجارية للنظام، وهذا يشمل إعادة التقييم بين الحين الآخر، تسجيل النتائج في النموذج الراهن، التأكد من أن متطلبات الأمن السبراني لا زالت مستوفاة. إن الشبكات المعقدة من التبعيات (مثل الضوابط المشتركة أو التي يعوض بعضها البعض) فيما بين الأنظمة عادةً ما تعني أن المخرجات الموثقة في النموذج الهدف للأنظمة ذات العلاقة يجب أن تؤخذ في عين الحسبان أثناء إيقاف تشغيل الأنظمة.

الأقسام الآتية تطرح طرقًا مختلفة يمكن للمنظمات أن تستخدم إطار العمل بها.

3.1 مراجعة أساسية للممارسات الأمن السبراني

يمكن استخدام إطار العمل لمقارنة نشاطات الأمن السبراني الحالية للمنظمة مع الممارسات الواردة في نواة إطار العمل. يمكن للمنظمة أن تفحص مدى تحقيقها للمخرجات المذكورة في التصنيفات الأساسية والتصنيفات الفرعية من خلال إنشاء النموذج الراهن، وذلك بما يتماشى مع الوظائف الخمس الأساسية: التحديد، الحماية، الرصد، الاستجابة، الاستعادة. قد تجد المنظمة أنها قد حققت المخرجات المرغوبة بالفعل، وبالتالي فإن إدارة الأمن السبراني تتناسب مع المخاطر المعروفة. عوضًا عن ذلك، قد تقرر المنظمة بأنها تملك الفرص (أو الحاجة) للتطور. يمكن للمنظمة استخدام هذه المعلومة لتطوير خطة عمل لتعزيز

[10] المنشور الخاص الصادر عن المعهد الوطني للمعايير والتكنولوجيا NIST المجلد الأول 800-160، "هندسة *نظام الأمن"، والاعتبارات المتعلقة باتباع "نهج متعدد التخصصات" في "هندسة نظم التأمين الجديرة بالثقة"*، تأليف روس وآخرين، نوفمبر {تشرين الثاني} عام 2016 (تم تحديثه بتاريخ 21 مارس 2018)،الموقع الإلكتروني https://doi.org/10.6028/NIST.SP.800-160v1

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

ممارسات الأمن السبراني الموجودة ولتقليل المخاطر السبرانية. وأيضًا، قد تجد المنظمة أنها تستثمر أكثر من اللازم لتحقيق بعض المخرجات. يمكن للمنظمة أن تستخدم هذه المعلومة لإعادة ترتيب أولويات ما لديها من الموارد.

في حين أن الوظائف الخمسة الأساسية لا تحل محل عملية إدارة المخاطر، إلا أنها ستقدّم لكبار التنفيذيين وغيرهم طريقة موجزة لاستخلاص المفاهيم الأساسية للمخاطر السبرانية لكي يتمكنوا من تقييم طريقة إدارة المخاطر التي تم تحديدها، وكذلك تقييم وضع المنظمة بالنسبة إلى معايير وإرشادات وممارسات الأمن السبراني الموجودة. كما يمكن لإطار العمل أن يساعد المنظمة في الإجابة عن أسئلة أساسية، مثل "كيف هو وضعنا؟" عندها يمكن لها أن تتحرك على بصيرة أكثر لتعزيز ممارستها في الأمن السبراني في المكان والزمان اللازمين

3.2 تأسيس أو تطوير برنامج الأمن السبراني

تعرض الخطوات التالية كيف يمكن للمنظمة أن تستخدم إطار العمل لتأسيس برنامج جديد للأمن السبراني أو لتطوير البرنامج الموجود. ينبغي أن يتم تكرار هذه الخطوات حسبما تقتضي الضرورة لتطوير الأمن السبراني باستمرار.

الخطوة الأولى: الأولويات والنطاق. تقوم المنظمة بتحديد أهداف الأعمال/الرؤية الخاصة بها وأولوياتها المنظمية عالية المستوى. من خلال هذه المعلومات، تقوم المنظمة باتخاذ قرارات استراتيجية تتعلق بتطبيقات الأمن السبراني، وتحدد نطاق الأنظمة والأصول التي تدعم خط الأعمال المختار أو العملية المختارة. يمكن تكييف إطار العمل لدعم خطوط الأعمال أو العمليات المختلفة ضمن المنظمة، والتي قد تختلف احتياجات أعمالها ومستويات تقبل المخاطر لديها. يمكن لمستويات تقبل المخاطر أن تنعكس في مرحلة التطبيق المستهدفة.

الخطوة الثانية: التوجيه. حالما يتم تحديد نطاق برنامج الأمن السبراني لخط الأعمال أو العملية، تقوم المنظمة بتحديد الأنظمة والأصول ذات العلاقة، المتطلبات التنظيمية، والمنهجية العامة للمخاطر. بعدها تقوم باستشارة المصادر لتحديد التهديدات ومواطن الضعف المنطبقة على تلك الأنظمة والأصول.

الخطوة الثالثة: إنشاء نموذج راهن. تقوم المنظمة بتطوير نموذج راهن عن طريق تحديد أي مخرجات التصنيفات ومخرجات التصنيفات الفرعية لنواة إطار العمل يتم تحقيقها في الوقت الراهن. إذا لوحظ أن أحد المخرجات محقق بشكل جزئي فستساعد هذه الملاحظة في دعم الخطوات اللاحقة عن طريق توفير معلومات عن خط الأساس.

الخطوة الرابعة: تقييم المخاطر. يمكن للتقييم أن يكون موجَّهًا من قبل عملية إدارة المخاطر العامة للمنظمة أو النشاطات السابقة لتقييم المخاطر. تقوم المنظمة بتحليل البيئة التشغيلية لمعرفة احتمالية أحداث الأمن السبراني وتأثير كل حدث على المنظمة. من المهم أن تحدد المنظمة المخاطر وأن تستخدم معلومات التهديدات السبرانية من المصادر الداخلية والخارجية لكي تحصل على فهم أفضل لاحتمالية وتأثير أحداث الأمن السبراني.

الخطوة الخامسة: إنشاء نموذج هدف. تقوم المنظمة بإنشاء نموذج هدف يركّز على تقييم التصنيفات الأساسية والفرعية لإطار العمل والتي تصف مخرجات الأمن السبراني التي تنشدها المنظمة. كما يمكن للمنظمات أن تقوم بتطوير تصنيفاتها الأساسية والفرعية الخاصة لاستيعاب المخاطر المنظمية التي تتفرد بها. وأيضًا، يمكن للمنظمة أن تأخذ في عين الاعتبار تأثيرات ومتطلبات أصحاب المصالح الخارجيين، مثل مؤسسات القطاع الأخرى والعملاء وشركاء الأعمال، أثناء إنشاء النموذج الهدف. ينبغي على النموذج الهدف أن يعكس بوضوح المعايير التي تتضمنها مرحلة التطبيق المستهدفة.

الخطوة السادسة: تحديد الفجوات وتحليلها وترتيبها حسب الأولوية. تقوم المنظمة بمقارنة النموذج الراهن مع النموذج الهدف لتحديد الفجوات. بعدها تقوم بإنشاء خطة عمل ذات أولويات للتعامل مع الفجوات – خطة عمل تعكس دوافع المهمة وتكاليفها وفوائدها ومخاطرها – لتحقيق المخرجات الواردة في النموذج الهدف. بعد ذلك، تقوم المنظمة بتحديد

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الموارد اللازمة، بما في ذلك الأموال وقوى العمل، للتعامل مع الفجوات. استخدام النماذج على هذا النحو يشجّع المنظمة على اتخاذ قرارات مدروسة بشأن نشاطات الأمن السبراني، ويعزز من إدارة المخاطر، كما يتيح للمنظمة للقيام بتحسينات هادفة وفعالة من حيث التكلفة.

الخطوة السابعة: تطبيق خطة العمل. تقوم المنظمة بتحديد الإجراءات التي سيتم اتخاذها للتعامل مع الفجوات، لو وُجدت، التي تم تحديدها في الخطوة السابقة، ثم تقوم بتعديل ممارساتها الحالية في الأمن السبراني من أجل الوصول إلى النموذج الهدف. للمزيد من الإرشادات، يورد إطار العمل مجموعة أمثلة لمراجع معرفية تتعلق بالتصنيفات والتصنيفات الفرعية، إلا أنه ينبغي على المنظمة أن تحدد المعايير والإرشادات والممارسات، بما في ذلك تلك التي يختص بها القطاع، والتي تناسب احتياجاتها أكثر.

تكرّر المنظمة هذه الخطوات حسب الحاجة للاستمرار في تقييم وتحسين أمنها السبراني. مثلًا، قد تجد المنظمات أن إعادة الخطوة الثانية (التوجيه) بشكل أكثر تكرارًا يحسّن من جودة تقييم المخاطر. بالإضافة إلى ذلك، تستطيع المنظمات أن تراقب حالة التقدم من خلال التحديثات المستمرة على النموذج الراهن، وبالتالي مقارنة النموذج الراهن مع النموذج الهدف. كما يمكن للمنظمة أن تستخدم هذه العملية لمواءمة برنامجها للأمن السبراني مع مرحلة التطبيق المرغوبة لديها.

3.3 إبلاغ أصحاب المصلحة بمتطلبات الأمن السبراني

يقدم إطار العمل لغة مشتركة للحديث عن المتطلبات فيما بين أصحاب المصلحة المستقلّين والمسؤولين عن تقديم المنتجات والخدمات الأساسية للبنية التحتية الحساسة. مثل:

- يمكن للمنظمة أن تستخدم النموذج الهدف للتعبير عن متطلبات إدارة المخاطر السبرانية أمام مقدم خدمات خارجي (مثل مقدّم خدمة الحوسبة السحابية التي يتم تصدير البيانات إليها).
- يمكن للمنظمة أن تعبّر عن حالة الأمن السبراني لديها عن طريق النموذج الراهن لإعداد تقرير بالنتائج أو لمقارنة مع متطلبات الاكتساب.
- يمكن لصاحب\مشغّل البنية التحتية الحساسة، بعد تحديده للشريك الخارجي الذي تعتمد عليه تلك البنية التحتية، أن يستخدم النموذج الهدف لإيصال التصنيفات والتصنيفات الفرعية المطلوبة.
- يمكن لقطاع البنية التحتية الحساسة أن ينشئ (نموذجًا مستهدفًا) بحيث يمكن استخدامه فيما بين مكونات القطاع كأساس أولي ومعيار لإنشاء نماذجهم المستهدفة الخاصة.
- يمكن للمنظمة أن تدير المخاطر السبرانية بشكل أفضل بين أصحاب المصلحة عبر تقييم وضعهم في البنية التحتية الحساسة وفي الاقتصاد الرقمي الأوسع، وذلك من خلال استخدام مراحل التطبيق.

يشكّل التواصل جزءًا مهمًا جدًا بين أصحاب المصلحة في أعلى وأسفل سلاسل الإمداد. سلاسل الإمداد هي مجموعات معقدة وموزعة عالميًا ومتداخلة من المصادر والعمليات بين عدة مستويات من المنظمات. تبدأ سلاسل الإمداد بالحصول على المنتجات والخدمات، وتمتد من تصميم المنتجات والخدمات وتطويرها وتصنيعها ومعالجتها وإيصالها إلى المستخدم النهائي. نظرًا إلى هذه العلاقات المعقدة والمتداخلة، فإن إدارة مخاطر سلاسل الإمداد (SCRM) تُعدّ وظيفة منظمية حساسة.

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

إدارة مخاطر سلاسل الإمداد السبرانية (Cyber SCRM) هي مجموعة من النشاطات الضرورية لإدارة المخاطر السبرانية المرتبطة بالأطراف الخارجية. وبشكل أخص، تتعامل إدارة مخاطر سلاسل الإمداد السبرانية مع كل من تأثيرات الأمن السبراني التي تمتلكها المنظمة على الأطراف الخارجية، وتأثيرات الأمن السبراني التي تمتلكها الأطراف الخارجية على المنظمة[11].

أحد الأهداف الأساسية لإدارة مخاطر سلاسل الإمداد السبرانية هو تحديد وتقييم وتخفيف خطر "المنتجات والخدمات التي قد تحتوي على وظائف خبيثة محتملة، أو قد تكون زائفة، أو قد تكون عرضة للمخاطر بسبب ممارسات التصنيع والتطوير الرديئة ضمن سلسلة الإمداد السبرانية."[12] قد تحتوي إدارة سلاسل الإمداد السبرانية على النشاطات التالية:

- وضع متطلبات الأمن السبراني المطلوبة من المورّدين
- سنّ متطلبات الأمن السبراني من خلال الاتفاقيات الرسمية (مثل العقود)
- التحدث مع المورّدين بشأن كيفية التحقق من تلك المتطلبات وكيفية المصادقة عليها
- التحقق من أن متطلبات الأمن السبراني يتم الالتزام بها من خلال منهجيات متعددة للتقييم
- حوكمة وإدارة النشاطات المذكورة أعلاه

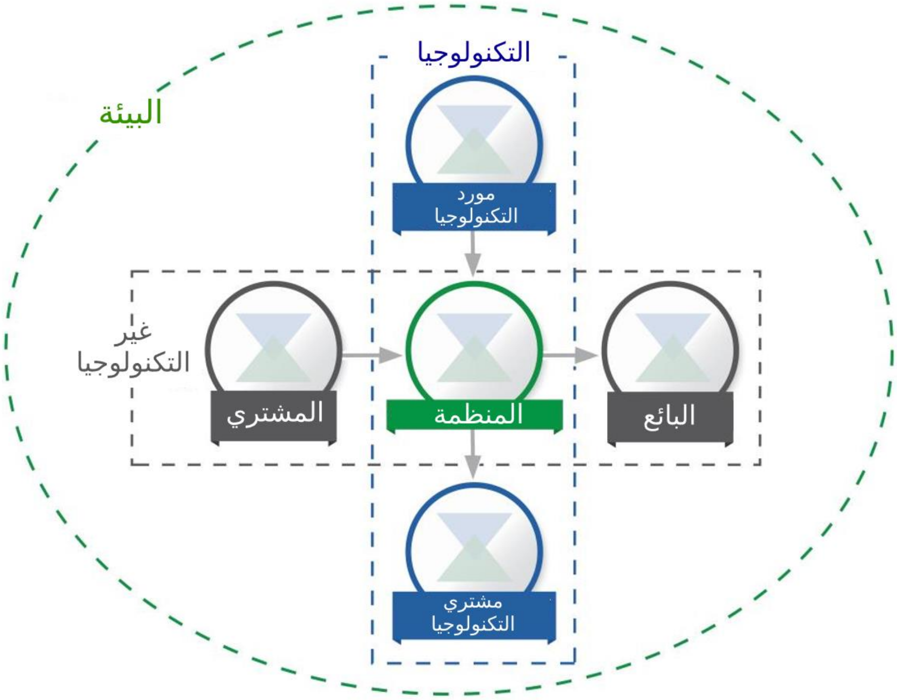
كما هو مبين في الشكل رقم (3)، تشمل إدارة مخاطر سلاسل الإمداد السبرانية (Cyber SCRM) موردي التكنولوجيا والمشترين، فضلا عن الموردين والمشترين للمواد غير التكنولوجية، حيث تمثل تكنولوجيا المعلومات (IT) الحد الأدنى للتكنولوجيا، وأنظمة التحكم الصناعية (ICS) النظم الفيزيائية السيبرانية، والأجهزة الموصلة بشكل أكثر عموما، بما في ذلك "شبكة الإنترنت من الأمور" (IoT)ويصور الشكل رقم (3) منظمة في نقطة واحدة في الوقت المحدد. ومع ذلك، فمن خلال المسار العادي للعمليات التجارية، فستمثل معظم المنظمات كلا من دور المورد "المنبع" و دور المشتري "المصب" في إطار علاقاتها بالمنظمات الأخرى أو بالمستخدمين النهائيين.

---

[11] التواصل بشأن "متطلبات الأمن السبراني" (القسم 3-3) وقرارات الشراء (القسم 3.4) يعالجان فقط إطارين للاستخدام من إطارات مخاطر سلاسل الإمداد السبرانية (Cyber SCRM) ولا يهدفان إلى معالجة مخاطر سلاسل الإمداد السبرانية (Cyber SCRM) بصورة شاملة.

[12] المنشور الخاص الصادر عن المعهد الوطني للمعايير والتكنولوجيا NIST رقم 800-160، "ممارسات تأمين مخاطر سلسلة الموردين لنظم المعلومات الإتحادية والمنظمات، تأليف بويتز وآخرين، إبريل {نيسان} عام 2015، الموقع الإلكتروني:
https://doi.org/10.6028/NIST.SP.800-161

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018



شكل 3: علاقات سلسلة الإمداد السبرانية

تشكّل الأطراف الموصوفة في الشكل 3 بيئةَ الأمن السبراني للمنظمة. تُبرز هذه العلاقات الدورَ المحوري الذي تلعبه إدارة مخاطر سلاسل الإمداد السبرانية في التعامل مع مخاطر الأمن السبراني في البنية التحتية الحساسة وفي الاقتصاد الرقمي الأوسع. هذه العلاقات، وما تقدمه من منتجات وخدمات، وما تشتمل عليه من مخاطر، كل ذلك ينبغي تحديده وتقسيمه إلى إمكانيات وقائية ودفاعية للمنظمة، بالإضافة إلى بروتوكولاتها الخاصة بالاستجابة والاستعادة.

في الشكل أعلاه، يشير "المشتري" إلى المنظمات أو الأشخاص الذين يستهلكون منتجًا أو خدمةً ما من منظمة أخرى، ويشمل ذلك كلًا من المنظمات الربحية وغير الربحية. أما "المورّد" فيشمل مقدّمي المنتجات والخدمات المستخدمة في العمليات الداخلية للمنظمات (مثل البنية التحتية لتقنية المعلومات)، أو المدمجة مع المنتجات أو الخدمات المقدمة إلى المشتري. تنطبق هذه التسميات على كلٍّ من المنتجات والخدمات المعتمدة على التكنولوجيا وغير المعتمدة على التكنولوجيا.

سواء كان الاهتمام بتصنيفات فرعية فردية من نواة إطار العمل أم بالاعتبارات الشاملة للنموذج، فإن إطار العمل يوفّر للمنظمات ولشركائهم منهجية تساعدهم في التأكد من أن المنتج او الخدمة تتوافق مع المخرجات الأمنية الحساسة. من خلال البدء من اختيار المخرجات ذات العلاقة بالسياق (مثل نقل المعلومات الشخصية الحساسة، توفير الخدمات الحساسة، خدمات التحقق من البيانات، سلامة المنتجات أو الخدمات)، يمكن للمنظمة أن تقيّم شركاءها بناءً على تلك المعايير. فمثلًا، إذا كانت المنظمة في صدد شراء نظام ما يقوم بمراقبة التكنولوجيا التشغيلية (Operational Technology, OT) لاتصالات الشبكة غير الطبيعية، فإن التوفّر (Availability) قد يكون هدفًا مهمًا للأمن السبراني ينبغي تحقيقه، كما ينبغي أن يدفع هذا الهدف نحو تقييم مورّد التكنولوجيا بناءً على التصنيفات الفرعية ذات العلاقة (مثل ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5)

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

3.4 قرارات الشراء

بما أن النموذج الهدف هو عبارة عن قائمة من متطلبات الأمن السبراني المرتبة حسب الأولوية، يمكن استخدامه في دراسة القرارات المتعلقة بشراء المنتجات والخدمات. تختلف هذه العملية عن إبلاغ أصحاب المصلحة بمتطلبات الأمن السبراني (المذكورة في القسم 3.3) من حيث أنه قد يكون من المحال فرض متطلبات الأمن السبراني على المورّد. ينبغي أن يكون الهدف هو اتخاذ أفضل قرار للشراء من بين مجموعة مورّدين، اعتمادًا على قائمة من متطلبات الأمن السبراني تم وضعها بعناية. قد يعني ذلك في أغلب الأحيان الاضطرار إلى بعض المقايضات، وذلك بمقارنة عدة منتجات أو خدمات ذات فجوات معروفة مع النموذج الهدف.

عند شراء المنتج أو الخدمة، يمكن استخدام النموذج أيضًا في تتبع ومعالجة المخاطر السبرانية المتبقية. مثلًا، إذا لم يكن المنتج أو الخدمة اللذين تم شراؤهما لا يفيان بكافة الشروط المذكورة في النموذج الهدف، يمكن للمنظمة أن تعالج المخاطر المتبقية من خلال إجراءات إدارية أخرى. كما يمكن للنموذج أن يوفّر للمنظمة منهجية لتقييم ما إذا كان المنتج يفي بمخرجات الأمن السبراني من خلال آليات المراجعة والاختبار بشكل دوريّ.

3.5 تحديد فرص المراجع المعرفية الجديدة أو المنقحة

يمكن استخدام إطار العمل لتحديد الفرص المتاحة لما هو جديد أو منقّح من المعايير أو الإرشادات أو الممارسات، حيث يمكن للمراجع المعرفية الإضافية أن تساعد المنظمة في معالجة الحاجات المستجدة. قد تكتشف المنظمة التي تطبّق أحد التصنيفات الفرعية، أو التي تقوم بتطوير تصنيف فرعي جديد، أن هنالك بعض المراجع المعرفية الجديدة لأحد النشاطات ذات العلاقة. للتعامل مع تلك الحاجة، قد تتعاون المنظمة مع قادة التكنولوجيا و/أو مؤسسات وضع المعايير لوضع مسودة وتطوير وتنسيق معايير أو إرشادات أو ممارسات.

3.6 منهجية لحماية الخصوصية والحريات المدنية

يقوم هذا القسم بوصف منهجية للتعامل مع مسائل الخصوصية الفردية والحريات المدنية، والتي يمكن أن يتسبب بها الأمن السبراني. تهدف هذه المنهجية لأن تكون مجموعة عامة من الاعتبارات والعمليات، وذلك لأن مسائل الخصوصية والحريات المدنية قد تختلف باختلاف القطاع أو بمرور الزمن، ويمكن للمنظمات أن تتعامل مع هذه الاعتبارات والعمليات باستخدام مجموعة من التطبيقات التقنية. على أية حال، ليست كل النشاطات في برنامج الأمن السبراني تثير اعتبارات الخصوصية والحريات المدنية. قد تكون هنالك حاجة لتطوير معايير وإرشادات وممارسات مثلى إضافية تقنية تتعلق بالخصوصية، وذلك من أجل دعم التطبيقات التقنية المطوّرة.

ترتبط الخصوصية بالأمن السبراني ارتباطًا وثيقًا، فنشاطات الأمن السبراني في المنظمة يمكن ان تخلق مخاطر على الخصوصية والحريات المدنية عندما يتم استخدام المعلومات الشخصية أو جمعها أو معالجتها أو صيانتها أو الكشف عنها. من الأمثلة على ذلك: نشاطات الأمن السبراني التي تتسبب في جمع أو الاحتفاظ بمعلومات شخصية بشكل يفوق الحاجة؛ الكشف عن أو استخدام معلومات شخصية غير متعلقة بنشاطات الأمن السبراني؛ نشاطات تخفيف المخاطر السبرانية التي تتسبب في رفض الخدمة (Denial of Service) أو الآثار الأخرى المشابهة والمحتملة، بما في ذلك بعض أنواع مراقبة أو رصد الحوادث والتي قد تمنع حرية التعبير أو تكوين الجمعيات.

تتحمل الحكومة ومؤسساتها مسؤولية حماية الحريات المدنية الناشئة عن نشاطات الأمن السبراني. كما هو مشار إليه في المنهجية أعلاه، ينبغي على الحكومة أو مؤسساتها التي تملك أو تشغّل البنية التحتية الحساسة أن يكون لها عملية معتمدة لدعم تقيّد نشاطات الأمن السبراني بقوانين الخصوصية وتنظيماتها ومتطلباتها الدستورية المنطبقة.

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

للتعامل مع مسائل الخصوصية، بإمكان المنظمات أن تنظر في كيف يمكن لبرنامج الأمن السبراني لديها أن يتضمّن مبادئ الخصوصية، مثل: تقليص البيانات أثناء جمع والكشف عن والاحتفاظ بالمعلومات الشخصية المتعلقة بحوادث الأمن السبراني؛ وضع حدود خارج نشاطات الأمن السبراني على أي معلومات يتم جمعها خصيصًا لنشاطات الأمن السبراني؛ الشفافية في بعض نشاطات الأمن السبراني؛ موافقة الأفراد والتعويض عن الآثار العكسية الناشئة عن استخدام المعلومات الشخصية في نشاطات الأمن السبراني؛ جودة البيانات وسلامتها وأمنها؛ المسؤولية والتدقيق.

أثناء قيام المنظمة بتقييم نواة إطار العمل في **ملحـق (أ)** يمكن أخذ العمليات والنشاطات التالية في عين الاعتبار كوسيلة لمعالجة مسائل الخصوصية والحريات المدنية السابق ذكرها في الأعلى:

حوكمة المخاطر السبرانية:

- تقييم المنظمات للمخاطر السبرانية والاستجابة للمخاطر المحتملة يضع في عين الحسبان مسائل الخصوصية لبرنامج الأمن السبراني
- الأفراد ممن تقع على عاتقهم مسؤوليات تتعلق بالخصوصية السبرانية يعملون تحت الإدارة المناسبة ويتم تدريبهم بشكل جيد
- وجود عمليات لدعم تقيد نشاطات الأمن السبراني بقوانين الخصوصية وتنظيماتها ومتطلباتها الدستورية المنطبقة
- وجود عمليات لتقييم حالة تطبيق الإجراءات والضوابط المنظمية المذكورة أعلاه

منهجيات لتحديد وتوثيق وتصريح الأفراد للوصول إلى الأصول والأنظمة المنظمية:

- يتم الأخذ بالخطوات اللازمة لتحديد ومعالجة مسائل الخصوصية في إجراءات إدارة الهويات والتحكم بالوصول إلى الحد الذي يتضمن جمع المعلومات الشخصية أو الكشف عنها أو استخدامها

إجراءات نشر الوعي والتدريب:

- يتم تضمين المعلومات المنطبقة من السياسات المنظمية للخصوصية في تدريب ونشاطات زيادة وعي القوى العاملة في الأمن السبراني
- مقدّمو الخدمة الذين يقدمون خدمات تتعلق بالأمن السبراني للمنظمة على دراية بسياسات الخصوصية ذات العلاقة في المنظمة

رصد النشاطات الغريبة ومراقبة الأنظمة والأصول:

- وجود عمليات لمراجعة مسألة الخصوصية في عمليات رصد النشاطات الغريبة ومراقبة الأمن السبراني

نشاطات الاستجابة، بما في ذلك مشاركة المعلومات أو الجهود الأخرى لتقليل المخاطر:

- وجود عمليات لتقييم ومعالجة ما إذا كانت المعلومات الشخصية يتم مشاركتها خارج المنظمة كجزء من نشاطات مشاركة معلومات الأمن السبراني، ومدى هذه المشاركة وتوقيتها وكيفيتها
- وجود عمليات لمراجعة مسألة الخصوصية في جهود تخفيف المخاطر السبرانية في المنظمة

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

4.0 التقييم الذاتي للمخاطر السبرانية باستخدام إطار العمل

إن إطار عمل الأمن السبراني مصمم للتقليل من المخاطر من خلال تطوير إدارة المخاطر السبرانية على أهداف المنظمة. في الحالة المثالية، ستستطيع المنظمة أن تستخدم إطار العمل لقياس المخاطر الي تواجهها ولوضع قيم لها، وذلك إلى جانب التكاليف والفوائد الخاصة بالخطوات المتبعة للتقليل من المخاطر إلى درجة مقبولة. كلما كانت المنظمة أفضل في قدرتها على قياس المخاطر والتكاليف والفوائد الخاصة باستراتيجيات وخطوات الأمن السبراني، كلما كانت منهجيتها واستثماراتها في الأمن السبراني أكثر عقلانية وفعالية وقيمة.

بمرور الوقت، ينبغي أن يطوّر التقييم الذاتي والقياسات من عمليات صنع القرار المتعلق بأولويات الاستثمار. فمثلًا، قياس – أو على الأقل التوصيف الدقيق – جوانب حالة الأمن السبراني للمنظمة واتجاهاتها عبر الزمن – أو التوصيف الدقيق لها على الأقل – بإمكانه أن يتيح للمنظمة فهم معلومات ذات معنى عن المخاطر ونقلها إلى التابعين والمورّدين والمشترين والأطراف الأخرى. يمكن للمنظمة أن تنجز ذلك داخليًا أو عن طريق الاستعانة بطرف ثالث للقيام بالتقييم. إذا تم ذلك بطريقة صحيحة مع إدراك لأوجه القصور، يمكن لهذه القياسات أن تكون قاعدة لعلاقات قوية مبنية على الثقة داخل وخارج المنظمة على حد سواء.

لاختبار فعالية الاستثمارات، يجب على المنظمة أولًا أن تمتلك فهمًا واضحًا لأهدافها المنظمية، وللعلاقة بين تلك الأهداف وبين مخرجات الأمن السبراني الداعمة، وللكيفية التي يتم بها تطبيق وإدارة تلك المخرجات المنفصلة عن بعضها. في حين أن قياس كل تلك العناصر يقع خارج نطاق إطار العمل هذا، إلا أن مخرجات الأمن السبراني لنواة إطار العمل تدعم التقييم الذاتي لفعالية الاستثمار ونشاطات الأمن السبراني من خلال الطرق التالية:

- وضع القرارات حول الكيفية التي ينبغي للأجزاء من المختلفة من العمليات التشغيلية أن تؤثر بها على اختيار مرحلة التنفيذ المرغوبة
- تقييم منهجية المنظمة لإدارة المخاطر السبرانية عن طريق تحديد مرحلة التنفيذ الحالية
- ترتيب مخرجات الأمن السبراني حسب أولويتها عن طريق تطوير النماذج المستهدفة
- تحديد المدى الذي تقوم فيه خطوات محددة للأمن السبراني بتحقيق المخرجات المرغوبة عن طريق تقييم النماذج الحالية
- قياس درجة تطبيق قوائم الضوابط أو الإرشادات الفنية المدرجة كمراجع معرفية.

إن تطوير مقاييس أداء الأمن السبراني هو عملية دائمة التطور. ينبغي على المنظمات أن تكون عميقة التفكير ومبدعة وحذرة بشأن طرق توظيف القياسات لتحسين الاستخدام ليكون على الوجه الأمثل، مع تجنب الاعتماد على المؤشرات المصطنعة للوضع الحالي وللتقدم في تحسين إدارة المخاطر السبرانية. إن الحكم على المخاطر السبرانية يتطلب الانضباط وينبغي أن يتم بشكل دوري. في كل مرة يتم فيها توظيف القياسات كجزء من عملية إطار العمل، تُشجع المنظمات على تحديد ومعرفة لماذا تلك القياسات مهمة وكيف ستساهم في الإدارة العامة للمخاطر السبرانية. كما ينبغي على تلك المنظمات أن تكون على دراية بأوجه القصور لتلك القياسات المستخدمة.

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

على سبيل المثال، يمكن لتتّبع التدابير الأمنية ومخرجات الأعمال أن يقدم نظرة ثاقبة إلى الكيفية التي تؤثر بها التغييرات في الضوابط الأمنية الصغيرة على إنجاز الأهداف المنظمية. إن بعض الأهداف المنظمية لا يمكن التأكد من تحقيقها من خلال تحليل البيانات إلا بعد تحقيقها فعلًا. هذا النوع من التدابير المتأخرة يُعتبر أكثر كمالًا. إلا أنه في غالب الأحيان يكون من المفيد أكثر أن يتم التنبؤ باحتمالية وقوع المخاطر السبرانية وبالآثار التي قد يخلّفها، وذلك باستخدام تدابير قيادية.

إن المنظمات مدعوّة إلى الابتكار وإلى تخصيص الطريقة التي يُدخلون بها القياسات في تطبيقهم لإطار العمل مع الإدراك التام لفائدتهم ولأوجه القصور فيهم.

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

ملحـق (أ): نواة إطار العمل

يقدم هذا الملحق نواة إطار العمل: وهي قائمة من الوظائف والتصنيفات والتصنيفات الفرعية والمراجع المعرفية التي تصف أنشطة أمن سبراني معينة، والتي – أي الأنشطة – تشترك فيها جميع قطاعات البنية التحتية الحساسة. إن صيغة التقديم المختارة لنواة إطار العمل لا تقترح ترتيبًا محددًا لتطبيق التصنيفات والتصنيفات الفرعية والمراجع المعرفية، كما لا تحدد درجة أهمية لهذه العناصر. يمثل إطار العمل الوارد في هذا الملحق مجموعة مشتركة من الأنشطة لإدارة مخاطر الأمن السبراني. في حين أن إطار العمل ليس شاملًا، إلا أنه قابل للتوسعة، مما يسمح للمنظمات والقطاعات والكيانات الأخرى بأن تستخدم تصنيفات فرعية ومراجع معرفية فعالة من حيث التكلفة وذات كفاءة، والتي تتيح لهم إدارة مخاطر الأمن السبراني لديهم. يمكن اختيار الأنشطة من خلال نواة إطار العمل أثناء إنشاء نموذج إطار العمل، كما يمكن إضافة تصنيفات وتصنيفات فرعية ومراجع معرفية إضافية إلى النموذج. إن عملية إدارة المخاطر في المنظمة، والمتطلبات القانونية\التنظيمية، وأهداف الأعمال\المهام، والقيود التنظيمية هي التي توجّه عملية اختيار هذه الأنشطة أثناء إنشاء النموذج. تعتبر المعلومات الشخصية أحد مكونات البيانات أو الأصول المشار إليها في التصنيفات عند تقييم المخاطر الأمنية ووسائل الحماية.

في حين أن النتائج المقصودة التي تم تحديدها في الوظائف والتصنيفات والتصنيفات الفرعية هي نفسها بالنسبة لتقنية المعلومات (IT) وأنظمة التحكم الصناعي (ICS)، إلا أن البيئات التشغيلية والاعتبارات الخاصة بتقنية المعلومات (IT) وأنظمة التحكم الصناعي (ICS) تختلف. لدى أنظمة التحكم الصناعي (ICS) تأثير مباشر على العالم المادي، بما في ذلك المخاطر المحتملة على صحة وسلامة الأفراد، والتأثير على البيئة. بالإضافة إلى ذلك، تتمتع أنظمة التحكم الصناعي (ICS) بمتطلبات فريدة من حيث الأداء والموثوقية مقارنةً بتقنية المعلومات (IT) ، ويجب مراعاة أهداف السلامة والكفاءة عند تنفيذ إجراءات الأمن السبراني.

لسهولة الاستخدام ، تم إعطاء كل عنصر من عناصر نواة اطار العمل معرّفًا فريدًا. تحتوي كل من الوظائف والتصنيفات على معرّف أبجدي خاص، كما هو موضح في الجدول 1. تتم الإشارة إلى التصنيفيات الفرعية داخل كل تصنيف عدديًا؛ كما تم تضمين المعرف الخاص لكل تصنيف فرعي في الجدول 2.

يمكن العثور على مواد داعمة إضافية، بما في ذلك المراجع المعرفية، تتعلق بإطار العمل على موقع NIST على الويب http://www.nist.gov/cyberframework/.

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

جدول 1 : المعرف الخاص بالوظيفة و التصنيف

المعرف الخاص بالوظيفة	الوظيفة	المعرف الخاص بالتصنيف	التصنيف
ID	التحديد (Identify)	ID.AM	إدارة الأصول (Asset Management)
		ID.BE	بيئة العمل (Business Environment)
		ID.GV	الحوكمة (Governance)
		ID.RA	تقييم المخاطر (Risk Assessment)
		ID.RM	استراتيجية إدارة المخاطر (Risk Management Strategy)
		ID.SC	إدارة مخاطر سلسلة الإمداد (Supply Chain Risk Management)
PR	الحماية (Protect)	PR.AC	إدارة الهوية والمصادقة عليها والتحكم في الوصول (Identity Management, Authentication and Access Control)
		PR.AT	الوعي والتدريب (Awareness and Training)
		PR.DS	أمن البيانات (Data Security)
		PR.IP	عمليات وإجراءات حماية المعلومات (Information Protection Processes and Procedures)
		PR.MA	الصيانة (Maintenance)
		PR.PT	التقنية الوقائية (Protective Technology)
DE	الرصد (Detect)	DE.AE	الحالات غير المعتادة والأحداث (Anomalies and Events)
		DE.CM	المراقبة الأمنية المستمرة (Security Continuous Monitoring)
		DE.DP	عمليات الرصد (Detection Processes)
RS	الاستجابة (Respond)	RS.RP	خطة الاستجابة (Response Planning)
		RS.CO	الاتصالات (Communications)
		RS.AN	التحليل (Analysis)
		RS.MI	التقليل (Mitigation)
		RS.IM	التحسينات (Improvements)
RC	الاستعادة (Recover)	RC.RP	خطة الاستعادة (Recovery Planning)
		RC.IM	التحسينات (Improvements)
		RC.CO	الاتصالات (Communications)

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

جدول 2 : نواة إطار العمل

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
التحديد **IDENTIFY (ID)**	إدارة الأصول Asset Management (ID.AM): يجب أن يتم تحديد البيانات، والأشخاص، والأجهزة، والأنظمة و المرافق التي تمكن المنظمة من تحقيق أهدافها، وأن تتم إدارتها طبقًا لأهميتها بالنسبة لأهداف المنظمة واستراتيجيتها لإدارة المخاطر	ID.AM-1: يتم جرد الأجهزة والأنظمة داخل المنظمة	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: يتم جرد منصات البرمجيات و التطبيقات داخل المنظمة	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: يتم إعداد خرائط للاتصالات التنظيمية وتدفق البيانات	**CIS CSC 12** **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: يتم فهرسة أنظمة المعلومات الخارجية	**CIS CSC 12** **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: الموارد (مثل المعدات، الأجهزة، البيانات، الوقت، الأشخاص، والبرمجيات) تعطى أولوية بناءً على تصنيفها وحساسيتها وقيمتها بالنسبة للمنظمة.	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
			NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
		ID.AM-6: يتم تحديد أدوار ومسئوليات جميع أطراف القوى العاملة، والطرف الثالث، وأصحاب المصلحة فيما يتعلق بالأمن السبراني (على سبيل المثال، الموردين، العملاء، الشركاء) وتوضيحه	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	بيئة العمل Business Environment (ID.BE): يجب أن تكون مهام المؤسسة وأهدافها وأصحاب المصالح ونشاطاتها مفهومة ومرتبة حسب الأولوية. تُستخدم هذه المعلومات لتعزيز قرارات مهام الأمن السبراني ومسؤولياته وإدارة المخاطر السبرانية	**ID.BE-1:** تم تحديد دور المؤسسة وإعلانها والإبلاغ عنها ضمن سلسلة الإمداد	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: يتم تحديد وإعلان وضع المنظمة في البنية التحتية الحساسة وقطاع الصناعة	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: يتم إنشاء وإعلان أولويات المنظمة وأهدافها ونشاطاتها	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: يتم إنشاء المهام الحساسة و التي تعتمد عليها المؤسسة لإنجاز خدماتها الحساسة	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: يتم إنشاء متطلبات الصمود لتقديم الخدمات الحساسة لجميع حالات التشغيل (مثل حالة الهجوم \ الضغط، والتعافي، وفي حالة التشغيل الاعتيادية)	**COBIT 5** BAI03.02, DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA- 14
	الحوكمة	ID.GV-1:	**CIS CSC 19**

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
	Governance (ID.GV): يجب أن تكون السياسات والإجراءات والعمليات المستخدمة لإدارة و مراقبة المتطلبات التنظيمية والقانونية والبيئية والتشغيلية ومتطلبات المخاطر مفهومة وأن تعزز إدارة المخاطر السبرانية	يتم إنشاء سياسات الأمن السبراني للمنظمة الإعلان عنها	**COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev. 4** -1 controls from all security control families
		ID.GV-2: يتم تنسيق مهام ومسؤوليات الأمن السبراني مع الأدوار الداخلية والشركاء الخارجيين	**CIS CSC 19** **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: أن يتم فهم وإدارة المتطلبات التنظيمية المتعلقة بالأمن السبراني، بما في ذلك التزامات الخصوصية والحريات المدنية	**CIS CSC 19** **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 4** -1 controls from all security control families
		ID.GV-4: أن تقوم عمليات الحوكمة وعمليات إدارة المخاطر بمعالجة مخاطر الأمن السبراني	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC 27001:2013** Clause 6 **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	تقييم المخاطر Risk Assessment (ID.RA): ان تفهم المنظمة مخاطر الأمن السبراني على عملياتها التشغيلية (بما في ذلك مهامها، وظائفها، صورتها و سمعتها) وعلى أصولها	ID.RA-1: تحديد وتوثيق ثغرات الأصول	**CIS CSC 4** **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
	المنظمية وعلى أفرادها.		**NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: يتم تلقي معلومات المخاطر السبرانية من منتديات ومصادر مشاركة المعلومات	**CIS CSC 4** **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16
		ID.RA-3: تحديد وتوثيق التهديدات الداخلية والخارجية	**CIS CSC 4** **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** Clause 6.1.2 **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: تحديد الآثار المحتملة على الأعمال واحتماليات الوقوع.	**CIS CSC 4** **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: استخدام التهديدات والثغرات والاحتمالات والتأثيرات لتحديد المخاطر	**CIS CSC 4** **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: تحديد الاستجابة للمخاطر وترتيبها بحسب الأولوية	**CIS CSC 4** **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Clause 6.1.3 **NIST SP 800-53 Rev. 4** PM-4, PM-9
	استراتيجية إدارة المخاطر	ID.RM-1:	**CIS CSC 4**

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
	Risk Management Strategy (ID.RM): إنشاء أولويات المنظمة وقيودها ومستوى تحمل المخاطر والافتراضات واستخدامها لدعم اتخاذ قرارات المخاطر التشغيلية	إنشاء وإدارة عمليات إدارة المخاطر والموافقة عليها من قبل أصحاب المصلحة	**COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: تحديد درجة تحمل المخاطر للمنظمة والتعبير عنها بشكل واضح	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: أن يستند تحديد المنظمة لدرجة تحملها للمخاطر على دورها في البنية التحتية الحساسة وتحليل المخاطر الخاصة بالقطاع	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11
	إدارة مخاطر سلسلة الإمداد Supply Chain Risk Management (ID.SC): وضع أولويات المنظمة والقيود ودرجة تحمل المخاطر والافتراضات واستخدامها لدعم قرارات المخاطر المرتبطة بإدارة مخاطر سلسلة الأمداد. كما أن المنظمة قد وضعت ونفذت العمليات تحديد وتقييم وإدارة مخاطر سلسلة الأمداد.	ID.SC-1: تحديد وإنشاء وتقييم وإدارة عمليات إدارة مخاطر سلسلة الإمداد السبرانية والموافقة عليها من قبل المعنيين	**CIS CSC 4** **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: تحديد الموردين والشركاء الآخرين لنظم المعلومات والمكونات والخدمات، وتحديد أولوياتها وتقييمها باستخدام عملية تقييم مخاطر سلسلة الإمداد السبراني	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
			ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: استخدام العقود مع الموردين والشركاء من الأطراف الأخرى لتنفيذ التدابير المناسبة والمصممة لتحقيق أهداف برنامج الأمن السبراني في المنظمة وخطة إدارة مخاطر سلسلة الإمداد السبراني.	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: تقييم الموردين والشركاء من الجهات الخارجية بشكل روتيني باستخدام عمليات التدقيق أو نتائج الاختبارات أو غير ذلك من أشكال التقييم للتأكد من استيفائهم لالتزاماتهم المذكورة في العقود.	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: إجراء تخطيط الاستجابة والاستعادة واختبار الخطط مع الموردين وموفري الخدمات من الأطراف الثالثة	**CIS CSC 19, 20** **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
الحماية **PROTECT (PR)**	إدارة الهوية والمصادقة عليها والتحكم في الوصول Identity Management and Access Control (PR.AC):	PR.AC-1: يتم إصدار بيانات الدخول وإدارتها وتوثيقها وتعطيلها والتدقيق فيها للأجهزة والمستخدمين والعمليات المصرح بها.	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
	الوصول إلى الأصول المادية والمنطقية والمرافق التابعة محصور في الأشخاص والعمليات والأجهزة المصرح لها، ويتم إدارته ليتناسق مع المخاطر المقيَّمة للوصول غير المصرح به إلى الأجهزة والعمليات المصرّح بها.		1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: يتم إدارة وحماية الوصول المادي للأصول	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: يتم إدارة الوصول عن بعد	**CIS CSC 12** **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: يتم إدارة صلاحيات وتصاريح الدخول، مع تطبيق مبدأ الحد الأدنى من الصلاحيات ومبدأ الفصل بين الواجبات	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5:	**CIS CSC** 9, 14, 15, 18

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
		يتم حماية تكامل الشبكة (مثل عزل الشبكات، وتقسيم الشبكات، إلخ)	**COBIT 5** DSS01.05, DSS05.02 **ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
		PR.AC-6: يتم إثبات الهويات وربطها مع بيانات الدخول، كما يتم التأكد من صحتها عند إجراء العمليات.	**CIS CSC, 16** **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: يتم التحقق من المستخدمين والأجهزة والأصول الأخرى (باستخدام التوثيق بعامل واحد أو عدة عوامل مثلًا) بما يتناسب مع مخاطر العملية (مثل المخاطر المتعلقة بأمن الأفراد وخصوصيتهم، والمخاطر المنظمية الأخرى).	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	التوعية والتدريب Awareness and Training (PR.AT):	PR.AT-1: يتم تعليم وتدريب جميع المستخدمين	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
	يتم توفير تعليم وتدريب توعوي بالأمن السبراني للأفراد والشركاء في المنظمة، لكي يقوموا بأداء مهامهم ومسؤولياتهم المتعلقة بالأمن السبراني بما يتناسب مع السياسات والإجراءات والاتفاقيات ذات العلاقة.		**ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: المستخدمون ذوو الصلاحيات المميزة يفهمون مهامهم ومسؤولياتهم	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: المعنيون من الطرف الثالث (مثل الموردين والعملاء والشركاء) يفهمون أدوارهم ومسؤولياتهم	**CIS CSC 17** **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
		PR.AT-4: الإدارة العليا تفهم مهامها ومسؤولياتها	**CIS CSC 17, 19** **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: الأشخاص المعنيون بالأمن المادي والأمن السبراني يفهمون مهامهم ومسؤولياتهم	**CIS CSC 17** **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13
	أمن البيانات Data Security (PR.DS): تتم إدارة المعلومات والسجلات (البيانات) بما يتماشى مع استراتيجية المنظمة للمخاطر لحماية سرية وسلامة وتوفر المعلومات.	PR.DS-1: البيانات المستقرة محمية	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
		PR.DS-2: البيانات المتنقلة محمية	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
		PR.DS-3: يتم إدارة الأصول بشكل رسمي خلال عمليات الإزالة والنقل والتخلص	**CIS CSC 1** **COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: أن تتوفر سعة كافية لضمان توفر البيانات	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BAI04.04 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: يتم تنفيذ وسائل الحماية ضد تسرب البيانات	**CIS CSC 13** **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4

يمكن الحصول على نسخة مجانية من هذا المنشــور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
		PR.DS-6: يتم استخدام آليات التحقق من السلامة للتأكد من سلامة البرمجيات والبرامج الثابتة والمعلومات	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: أن يتم الفصل بين بيئة (بيئات) التطوير والاختبار وبين بيئة الإنتاج	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: يتم استخدام آليات التحقق من السلامة للتحقق من سلامة الأجهزة	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISO/IEC 27001:2013** A.11.2.4 **NIST SP 800-53 Rev. 4** SA-10, SI-7
	عمليات وإجراءات حماية المعلومات Information Protection Processes and Procedures (PR.IP): يتم صيانة السياسات الأمنية (المعنية بالهدف والنطاق والأدوار والمسؤوليات والالتزام الإداري والتنسيق بين الكيانات التنظيمية) والعمليات والإجراءات، كما يتم استخدامها لإدارة حماية أنظمة المعلومات والأصول.	PR.IP-1: يتم إنشاء وصيانة خط الأساس لإعدادات تكنولوجيا المعلومات/أنظمة التحكم الصناعية مع دمج مبادئ الأمن (مثل مفهوم الحد الأدنى من الوظائف والصلاحيات)	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: يتم تطبيق دورة حياة تطوير الن لإدارة الأنظمة	**CIS CSC 18** **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3 **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
			NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: وجود عمليات التحكم في تغيير الإعدادات	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: يتم إجراء نسخ احتياطي للمعلومات والحفاظ عليها واختبارها	**CIS CSC 10** **COBIT 5** APO13.01, DSS01.01, DSS04.07 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: يتم الالتزام بالسياسات واللوائح المتعلقة ببيئة التشغيل المادية لأصول المنظمة	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: يتم إتلاف البيانات وفقًا للسياسة	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
			NIST SP 800-53 Rev. 4 MP-6
		PR.IP-7: يتم تحسين عمليات الحماية	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: يتم مشاركة فعالية تقنيات الحماية	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: خطط الاستجابة (الاستجابة للحوادث واستمرارية الأعمال) وخطط الاستعادة (الاستعادة بعد الحوادث والتعافي من الكوارث) موجودة وتتم إدارتها	**CIS CSC 19** **COBIT 5** APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: يتم اختبار خطط الاستجابة والاستعادة	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: يتم تضمين الأمن السبراني في ممارسات الموارد البشرية (مثل إلغاء صلاحيات الوصول، والتحري عن	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
		الموظفين)	**ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.IP-12: يتم تطوير وتنفيذ خطة إدارة الثغرات	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	الصيانة Maintenance (PR.MA): يتم إجراء صيانة وإصلاح مكونات نظم التحكم الصناعي ونظم المعلومات بما يتفق مع السياسات والإجراءات.	PR.MA-1: يتم إجراء وتسجيل عملية صيانة الأصول التابعة للمنظمة باستخدام أدوات معتمدة وتخضع للتحكم	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: تتم الموافقة على الصيانة عن بُعد لأصول المنظمة وتسجيلها وتنفيذها بطريقة تمنع الوصول غير المصرح به	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rev. 4** MA-4
	التكنولوجيا الوقائية Protective Technology (PR.PT): تتم إدارة حلول الأمن التقنية لضمان أمن وصمود الأنظمة والأصول، بما يتفق مع السياسات والإجراءات والاتفاقيات ذات الصلة.	PR.PT-1: يتم تحديد أرشيف التدقيق/السجلات وتوثيقه وتطبيقه ومراجعته وفقًا للسياسة	**CIS CSC** 1, 3, 5, 6, 14, 15, 16 **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

المراجع المعرفية	التصنيف الفرعي	التصنيف	الوظيفة
NIST SP 800-53 Rev. 4 AU Family			
CIS CSC 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06 **ISA 62443-3-3:2013** SR 2.3 **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8	PR.PT-2: أن تكون الوسائط القابلة للإزالة محمية ويتم تقييد استخدامها وفقًا للسياسة		
CIS CSC 3, 11, 14 **COBIT 5** DSS05.02, DSS05.05, DSS06.06 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53 Rev. 4** AC-3, CM-7	PR.PT-3: يتم العمل بمبدأ الحد الأدنى من الوظائف والصلاحيات عن طريق تهيئة الأنظمة لتوفير الإمكانيات الأساسية فقط		
CIS CSC 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	PR.PT-4: يتم حماية الاتصالات وشبكات التحكم		

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
		PR.PT-5: يتم تطبيق الآليات (مثل الفشل الآمن، موازنة الحمل، التبادل السريع) لتحقيق متطلبات الصمود في المواقف العادية والمواقف الخطرة.	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
الرصـد DETECT (DE)	الحالات غير المعتادة والأحداث Anomalies and Events (DE.AE): يتم رصد النشاط غير الطبيعي وفهم الأثر المحتمل للأحداث	DE.AE-1: يتم تأسيس وإدارة خط الأساس لعمليات الشبكة والتدفق المتوقع للبيانات للمستخدمين والأنظمة	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3 **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: يتم تحليل الأحداث التي تم رصدها لفهم أهداف وطرق الهجوم	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: يتم جمع بيانات الأحداث والربط فيما بينها من مصادر ومستشعرات متعددة	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4:	**CIS CSC** 4, 6

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
		يتم تحديد تأثير الأحداث	**COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: يتم إنشاء عتبات التنبيه من الأحداث	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	الرقابة الأمنية الدائمة Security Continuous Monitoring (DE.CM): يتم رصد نظام المعلومات والأصول لتحديد أحداث الأمن السبراني والتحقق من فعالية تدابير الحماية.	DE.CM-1: يتم مراقبة الشبكة للكشف عن الأحداث المحتملة للأمن السبراني	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: يتم رصد البيئة المادية للكشف عن الأحداث المحتملة للأمن السبراني	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: يتم مراقبة نشاط الموظفين للكشف عن الأحداث المحتملة للأمن السبراني	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: يتم رصد الأكواد الخبيثة	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
			ISO/IEC 27001:2013 A.12.2.1 **NIST SP 800-53 Rev. 4** SI-3, SI-8
		DE.CM-5: يتم رصد الأكواد المتنقلة الغير مصرح بها	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
		DE.CM-6: يتم مراقبة نشاط مزود الخدمة الخارجي لرصد الأحداث المحتملة للأمن السبراني	**COBIT 5** APO07.06, APO10.05 **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: يتم مراقبة الموظفين، والاتصالات، والأجهزة، والبرمجيات الغير المصرح بها	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: يتم البحث عن الثغرات	**CIS CSC** 4, 20 **COBIT 5** BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-5
	عمليات الرصد Detection Processes (DE.DP): يتم الاحتفاظ بعمليات وإجراءات الرصد واختبارها لضمان الوعي بالأحداث الشاذة.	DE.DP-1: أن تكون أدوار ومسؤوليات الرصد محددة بشكل جيد لضمان المساءلة	**CIS CSC 19** **COBIT 5** APO01.02**,** DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: أن تتوافق أنشطة الكشف مع جميع المتطلبات	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
		المنطقة	**ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: يتم اختبار عمليات الرصد	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: يتم إرسال معلومات رصد الأحداث	**CIS CSC 19** **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: يتم تحسين عمليات الرصد بشكل مستمر	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
الاستجابة Respond (RS)	خطة الاستجابة Response Planning (RS.RP): يتم تنفيذ وصيانة عمليات وإجراءات الاستجابة، لضمان الاستجابة لحوادث الأمن السبراني المرصودة.	RS.RP-1: يتم تنفيذ خطة الاستجابة أثناء أو بعد وقوع حادث	**CIS CSC 19** **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	الاتصالات Communications (RS.CO): يتم تنسيق أنشطة الاستجابة مع أصحاب المصلحة	RS.CO-1: يعرف الموظفون أدوارهم وترتيب العمليات عند الحاجة إلى الاستجابة	**CIS CSC 19** **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
	الداخليين والخارجيين (مثل الدعم الخارجي من وكالات إنفاذ القانون).		**ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: يتم الإبلاغ عن الحوادث بما يتفق مع المعايير المعمول بها	**CIS CSC 19** **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: يتم مشاركة المعلومات بما يتفق مع خطط الاستجابة	**CIS CSC 19** **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: يتم التنسيق مع أصحاب المصلحة بما يتفق مع خطط الاستجابة	**CIS CSC 19** **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: وجود تبادل طوعي للمعلومات مع أصحاب المصلحة الخارجيين لتحقيق الوعي بالأمن السيبراني على نطاق أوسع	**CIS CSC 19** **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15
	التحليل Analysis (RS.AN): يتم إجراء التحليلات لضمان الاستجابة الفعالة ودعم أنشطة الاستعادة.	RS.AN-1: يتم التحقيق في الإشعارات القادمة من أنظمة الرصد	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
			NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: يتم فهم التأثير الناتج عن الحادث	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: يتم تنفيذ التحليل الجنائي	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: يتم تصنيف الحوادث بما يتفق مع خطط الاستجابة	**CIS CSC 19** **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: يتم إنشاء العمليات لتلقي وتحليل ومواجهة الثغرات التي تم الكشف عنها للمنظمة من قبل مصادر داخلية وخارجية (مثل الاختبارات الداخلية أو نشرات الأمن أو الباحثين الأمنيين)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15
	التخفيف Mitigation (RS.MI): يتم تنفيذ الأنشطة لمنع تفاقم الحدث، وللتخفيف من آثاره، ولحل المشكلة.	RS.MI-1: يتم احتواء الحوادث	**CIS CSC 19** **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
		RS.MI-2: يتم تخفيف الحوادث	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: يتم تخفيف الثغرات التي تم تحديدها حديثا أو توثيقها على أنها مخاطر مقبولة	**CIS CSC 4** **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	التحسينات Improvements (RS.IM): تحسين أنشطة الاستجابة التنظيمية من خلال دمج الدروس المستفادة من أنشطة الرصد/الاستجابة الحالية والسابقة.	RS.IM-1: خطط الاستجابة تتضمن الدروس المستفادة	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: يتم تحديث استراتيجيات الاستجابة	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
الاستعادة RECOVER (RC)	خطة الاستعادة Recovery Planning (RC.RP): يتم تنفيذ عمليات وإجراءات الاستعادة وصيانتها لضمان استعادة النظم أو الأصول المتأثرة بحوادث الأمن السبراني.	RC.RP-1: يتم تنفيذ خطة الاستعادة خلال أو بعد حادث الأمن السبراني	**CIS CSC 10** **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	التحسينات Improvements (RC.IM): يتم تحسين تخطيط وعمليات الأستعادة من خلال دمج الدروس المستفادة في الأنشطة المستقبلية.	RC.IM-1: خطط الاستعادة تتضمن الدروس المستفادة	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2:	**COBIT 5** APO12.06, BAI07.08

يمكن الحصول على نسخة مجانية من هذا المنشــور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

الوظيفة	التصنيف	التصنيف الفرعي	المراجع المعرفية
		يتم تحديث استراتيجيات الاستعادة	**ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	الاتصالات Communications (RC.CO): يتم تنسيق أنشطة الاستعادة مع الأطراف الداخلية والخارجية (على سبيل المثال: مراكز التنسيق ومقدمو خدمات الإنترنت وأصحاب أنظمة الهجوم والضحايا وفريق التعامل مع الحوادث الأمنية الحاسوبية والموردون الآخرون).	RC.CO-1: يتم إدارة تدار العلاقات العامة	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
		RC.CO-2: يتم تحسين السمعة بعد وقوع حادث	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: يتم إبلاغ أنشطة الاستعادة إلى الجهات المعنية الداخلية والخارجية بالإضافة إلى فرق الإدارة والتنفيذ	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4

يمكن العثور على المعلومات المتعلقة بالمراجع المعرفية الموضحة في ملحق (أ) في المواقع التالية:

- تحديد الأهداف للمعلومات والتكنولوجيا المتصلة بها والتحكم فيها (COBIT) http://www.isaca.org/COBIT/Pages/default.aspx
- الضوابط الأمنية الحرجة للدفاع السبراني الفعّال (CIS Control): https://www.cisecurity.org
- المعهد الأمريكي للمعايير الوطنية/الجمعية الدولية للتشغيل الآلي (ANSI/ISA) 62443-2-1 (99.02.01)-2009 تأمين التحول الآلي في الصناعة وأنظمة التحكم: إنشاء برنامج أمني للتحكم في عملية التحول الصناعي الآلي https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03)-2013, نظام أمني التحكم في عملية التحول للآلية: متطلبات النظام الأمني ومستويات الأمان: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- نظام معايير الجودة ISO/IEC 27001 تكنولوجيا المعلومات – تقنيات الأمن – نظم إدارة أمن المعلومات – الشروط والمتطلبات https://www.iso.org/standard/54534.html

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

- المنشور الخاص الصادر عن المعهد الوطني للمعايير والتكنولوجيا NIST رقم 53-800 الطبعة الرابعة - المنشور الخاص الصادر عن المعهد الوطني للمعايير والتكنولوجيا NIST رقم -53 800 الطبعة الرابعة "التحكم في الأمن والخصوصية لنظم المعلومات الفيديرالية والمؤسسات، الصادر في إبريل 2013 (يشتمل على تحديثات سارية المفعول بتاريخ 22 يناير 2015) ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*: https://www.iso.org/standard/54534.html
- NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (including updates as of January 22, 2015). https://doi.org/10.6028/NIST.SP.800-53r4.

المراجع المعرفية قد تم ربطها بمستوى الضوابط فقط، على الرغم من أن أي تحسين للضابط قد يكون مفيدًا لتحقيق مخرجات التصنيف الفرعي.

إن الربط بين "التصنيف الفرعي" في نواة إطار العمل والأقسام المحددة في "المراجع المعرفية" لا يُقصد به التحديد بشكل قاطع ما إذا كانت الأقسام المحددة في "المراجع المعرفية" تقدم المخرجات المرغوبة من " التصنيف الفرعي ".

المراجع المعرفية ليست شاملة، حيث أنه لا يتم ربط كل عنصر (على سبيل المثال ، الضابط ، المتطلبات) بمرجع معلوماتي معين في " التصنيف الفرعي" في نواة إطار العمل

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

ملحق (ب): المصطلحات

يعرّف هذا الملحق مصطلحات مختارة مستخدمة في المنشور.

جدول 3 : مصطلحات إطار العمل

مشتر	الأشخاص أو المؤسسات التي تستهلك منتجًا أو خدمة معينة.
التصنيف	تقسيم "الوظائف" إلى مجموعات من مخرجات الأمن السبراني، والتي ترتبط ارتباطًا وثيقًا بالاحتياجات البرمجية وبأنشطة معينة. تشمل أمثلة التصنيفات: "إدارة الأصول" و "إدارة الهوية والتحكم في الوصول" و "عمليات الرصد".
البنية التحتية الحساسة	الأنظمة والأصول، سواء كانت مادية أو افتراضية، ذات الأهمية البالغة بالنسبة للولايات المتحدة، لدرجة أن عجز أو تدمير هذه الأنظمة والأصول سيكون له تأثير مدمر على الأمن السبراني أو الأمن الاقتصادي الوطني أو الصحة العامة الوطنية أو السلامة أو أي مزيج من هذه الأمور.
الأمن السبراني	عملية حماية المعلومات عن طريق منع الهجمات والكشف عنها والاستجابة لها.
حدث الأمن السبراني	تغيير في مجال الأمن السبراني قد يكون له تأثير على العمليات المنظمية (بما في ذلك المهمة أو القدرات أو السمعة).
حادثة (حادث) الأمن السبراني	حدث متعلق بالأمن السبراني تم وصفه بأن له تأثير على المنظمة مما يؤدي إلى الحاجة إلى الاستجابة والاستعادة.
الرصد (الوظيفة)	تطوير وتنفيذ الأنشطة المناسبة لتحديد وقوع حدث أمن سبراني.
إطار العمل	نهج قائم على المخاطر للحد من مخاطر الأمن السبراني، ويتألف من ثلاثة أجزاء: نواة إطار العمل، و نماذج إطار العمل، وطبقات تنفيذ إطار العمل. يُعرف أيضًا باسم "إطار عمل الأمن السبراني".
نواة إطار العمل	مجموعة من أنشطة الأمن السبراني والمراجع الشائعة في مجالات قطاعات البنية التحتية الحيوية ويتم تنظيمها حول نتائج معينة. "نواة إطار العمل" تشتمل على أربعة أنواع من العناصر: الوظائف، والتصنيفات، والتصنيفات الفرعية، والمراجع المعرفية.
مرحلة تنفيذ إطار العمل	عدسة يمكن من خلالها الاطلاع على خصائص نهج المنظمة في المخاطرة - كيف ترى المؤسسة مخاطر الأمن السبراني والعمليات القائمة لإدارة هذه المخاطر.
نموذج إطار العمل	تمثيل للنتائج التي اختارها نظام معين أو منظمة معينة من تصنيفات إطار العمل والتصنيفات الفرعية.
الوظيفة	أحد المكونات الرئيسية للإطار العمل. توفر "الوظيفة" أعلى مستوى من الهيكل لتنظيم أنشطة الأمن السبراني الأساسية في التصنيفات والتصنيفات الفرعية. الوظائف الخمس هي: التحديد والحماية والرصد والاستجابة والاستعادة.
التحديد	تطوير فهم المنظمة لإدارة مخاطر الأمن السبراني على الأنظمة والأصول

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

(الوظيفة)	والبيانات والقدرات.
مراجع معرفية	جزء محدد من المعايير والإرشادات والممارسات المشتركة بين قطاعات البنية التحتية الحساسة، والتي توضح طريقة تحقيق النتائج المرتبطة بكل "تصنيف الفرعي". أحد أمثلة المراجع المعرفية هو ISO / IEC 27001 Control A.10.8.3، والذي يدعم التصنيف الفرعي "حماية البيانات المنتقلة " الذي يقع ضمن تصنيف "أمن البيانات" في وظيفة "الحماية".
الكود المتنقل	برنامج (على سبيل المثال، سكربت أو ماكرو أو تعليمات محمولة أخرى) يمكن إرساله دون تغيير إلى مجموعة من المنصات غير المتجانسة وتنفيذه باستخدام دلالات متطابقة.
الحماية (الوظيفة)	تطوير وتنفيذ الضمانات المناسبة لضمان تقديم خدمات البنية التحتية الحيوية.
مستخدم ذو صلاحيات	مستخدم مصرحّ (وبالتالي، موثوق به) لأداء وظائف متعلقة بالأمان والتي لا يُسمح للمستخدمين العاديين بتنفيذها.
الاستعادة (الوظيفة)	تطوير وتنفيذ الأنشطة المناسبة للحفاظ على خطط الصمود واستعادة أي قدرات أو خدمات تعرضت للتلف بسبب حدث الأمن السبراني.
الاستجابة (الوظيفة)	تطوير وتنفيذ الأنشطة المناسبة لاتخاذ إجراءات بشأن حدث ذو علاقة بالأمن السبراني المرصود.
الخطر	مقياس لمدى التهديد الذي يشكله ظرف أو حدث محتملان على كيان ما، وعادة ما يتكون من: (i) التأثيرات السلبية التي قد تنشأ في حالة حدوث الظرف أو الحدث ؛ و (ii) احتمال حدوثها.
إدارة المخاطر	عملية تحديد وتقييم والاستجابة للمخاطر.
التصنيف الفرعي	تقسيم إحدى "التصنيفات" إلى مخرجات محددة من الأنشطة التقنية و/أو الإدارية. تتضمن الأمثلة على التصنيف الفرعي: " يتم فهرسة أنظمة المعلومات الخارجية"، و " البيانات المستقرة محمية "، و " يتم التحقيق في إشعارات أنظمة الرصد".
المورد	مزودو المنتجات والخدمات المستخدمة لأغراض داخلية في المؤسسة (على سبيل المثال، البنية التحتية لتكنولوجيا المعلومات) أو المدمجة في منتجات الخدمات المقدمة إلى مشتري تلك المنظمة.
تصنيف	مخطط التقسيم.

يمكن الحصول على نسخة مجانية من هذا المنشـور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018

ملحق (ج): الاختصارات

يعرّف هذا الملحق الاختصارات المختارة المستخدمة في المنشور.

ANSI	American National Standards Institute	المعهد الأمريكي الوطني للمعايير الوطنية الأمريكية
CEA	Cybersecurity Enhancement Act of 2014	قانون تعزيز الأمن السبراني لعام 2014
CIS	Center for Internet Security	مركز لأمن الإنترنت
COBIT	Control Objectives for Information and Related Technology	أهداف الرقابة على المعلومات والتكنولوجيا المتصلة بها
CPS	Cyber-Physical Systems	النظم السبرانية المادية
CSC	Critical Security Control	السيطرة الأمنية الحرجة
DHS	Department of Homeland Security	وزارة الأمن الوطني
EO	Executive Order	أمر تنفيذي
ICS	Industrial Control Systems	أنظمة التحكم الصناعية
IEC	International Electrotechnical Commission	اللجنة الكهروتقنية الدولية
IoT	Internet of Things	إنترنت الأشياء
IR	Interagency Report	التقرير المشترك بين الوكالات
ISA	International Society of Automation	الجمعية الدولية للتشغيل الآلي
ISAC	Information Sharing and Analysis Center	مركز التحليل وتبادل المعلومات
ISAO	Information Sharing and Analysis Organization	منظمة تبادل المعلومات وتحليلها
ISO	International Organization for Standardization	المنظمة الدولية للمعايير (أيزو)
IT	Information Technology	تكنولوجيا المعلومات
NIST	National Institute of Standards and Technology	المعهد الوطني للمعايير والتكنولوجيا
OT	Operational Technology	تكنولوجيا التشغيل
PII	Personally Identifiable Information	معلومات شخصية
RFI	Request for Information	طلب للحصول على المعلومات
RMP	Risk Management Process	عملية إدارة المخاطر
SCRM	Supply Chain Risk Management	إدارة المخاطر في سلسلة التوريد
SP	Special Publication	منشور خاص

يمكن الحصول على نسخة مجانية من هذا المنشــور على الموقع الإلكتروني https://doi.org/10.6028/NIST.CSWP.04162018