إطار عمل الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا - النسخة 2.0

المعهد الوطني للمعايير والتكنولوجيا

هذا المنشور متاح مجانًا عبر هذا الرابط: https://doi.org/10.6028/NIST.CSWP.29.ara

26فبراير 2024

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

26 فبراير 2024

الملخص

يوفّر إطار عمل الأمن السيبراني (CSF) "النسخة 2.0" الصادر عن المعهد الوطني للمعايير والتكنولوجيا إرشادات للقطاع الصناعي، والجهات الحكومية، وسائر المؤسسات في مجال إدارة مخاطر الأمن السيبراني. كما يوفّر إطار العمل آلية لتصنيف المخرجات السيبرانية الشاملة، تتيح لأي مؤسسة — بغض النظر عن حجمها أو قطاعها أو مستوى نضجها — تعزيز فهم أنشطتها السيبرانية، وتقييمها، وترتيبها حسب الأولوية، والترويج لها. ولا يفرض هذا الإطار أساليب محددة أو إلزامية لتحقيق هذه المخرجات، بل يرتبط بمصادر إلكترونية إضافية تقدم إرشادات حول الممارسات والضوابط التي يُمكن استخدامها لتحقيق تلك المخرجات. تصف هذه الوثيقة إطار عمل الأمن السيبراني (النسخة 2.0)، وعناصره، وبعض الطرق المتنوعة التي يُمكن استخدامه بها.

الكلمات المفتاحية

الأمن السيبراني؛ إطار عمل الأمن السيبراني؛ حوكمة مخاطر الأمن السيبراني؛ إدارة مخاطر الأمن السيبراني؛ إدارة مخاطر المؤسسة؛ الملفات التعريفية؛ المستويات.

الجمهور المستهدف

الجمهور الرئيسي المستهدف بهذا الإطار هم المسؤولون عن تطوير وقيادة برامج الأمن السيبراني. يمكن أيضًا للمشاركين في إدارة المخاطر — من المديرين التنفيذيين وأعضاء مجالس الإدارة إلى المتخصصين في المشتريات والتكنولوجيا، ومديري المخاطر، والمحامين، وخبراء الموارد البشرية، ومدققي الأمن السيبراني — الاستفادة من هذا الإطار في توجيه قراراتهم المتعلقة بالأمن السيبراني. إضافةً إلى ذلك، يشكّل هذا الإطار أداة مفيدة للجهات المعنية بصياغة السياسات أو التأثير فيها — كالجمعيات، والمنظمات المهنية، والجهات التنظيمية — في تحديد أولويات إدارة مخاطر الأمن السيبراني ونشرها.

المحتوى الإضافي

سيواصل المعهد الوطني للمعايير والتكنولوجيا تطوير وتوفير موارد إضافية لدعم المؤسسات في تطبيق إطار عمل الأمن السيبراني، بما في ذلك الأدلة الإرشادية السريعة والملفات التعريفية المجتمعية. تتوفر جميع الموارد لكل من يرغب في الاطلاع عليها عبر الموقع الإلكتروني لإطار عمل الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا. نرحب بإرسال الاقتراحات الخاصة بالموارد الإضافية لإدراجها على الموقع الإلكتروني لإطار عمل الأمن السيبراني الصادر عن موقع المعهد الوطني للمعايير والتكنولوجيا عبر البريد الإلكتروني: cyberframework@nist.gov.

ملاحظات للقراء

لم تُدرج الوثائق المشار إليها أو المستشهد بها أو المقتبسة في هذا المنشور ضمن هذه الوثيقة كاملةً، ما لم يُذكر خلاف ذلك.

قبل إصدار النسخة 2.0، كان يُعرف إطار عمل الأمن السيبراني باسم "إطار تحسين الأمن السيبراني للبنية التحتية الحيوية". وقد توقفنا عن استخدام هذا المسمى في إطار عمل الأمن السيبراني (النسخة 2.0).

شكروتقدير

يُعد هذا الإطار نتاج جهود تعاونية مستمرة بين القطاع الصناعي، والأوساط الأكاديمية، والحكومة في الولايات المتحدة وعلى المستوى العالمي. يتقدم المعهد الوطني للمعايير والتكنولوجيا بخالص الشكر والتقدير لجميع من ساهموا في تطوير هذه النسخة من إطار عمل الأمن السيبراني.

26 فبراير 2024

يمكن الاطلاع على معلومات عن عملية تطوير إطار عمل الأمن السيبراني من خلال الموقع الإلكتروني لإطار عمل الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا. كما يمكن دائمًا مشاركة الدروس المستفادة من استخدام الإطار مع المعهد الوطني للمعايير والتكنولوجيا عبر البريد الإلكتروني: cyberframework@nist.gov.

فهرس المحتويات

قائمة الأشكال

تمهيد

صُمّم إطار عمل الأمن السيبراني (CSF) "النسخة 2.0" لمساعدة المؤسسات رغم اختلاف أحجامها وقطاعاتها، سواء كانت صناعية أو حكومية أو أكاديمية أو غير ربحية، في إدارة مخاطر الأمن السيبراني والحد منها. ويُعد الإطار أداة فعالة مهما كان مستوى نضج المؤسسة أو درجة التطور الفني لبرامج الأمن السيبراني لديها. ومع ذلك، لا يتبع الإطار نهجًا موحدًا يصلح لجميع الحالات؛ إذ إن لكل مؤسسة مزيجًا من المخاطر المشتركة والفريدة، إلى جانب اختلاف في مستويات تقبل المخاطر وتحملها، وتنوع في رسالتها وأهدافها. لذلك، فإن تطبيق هذا الإطار سيختلف حتمًا من مؤسسة إلى أخرى.

سيتم من الناحية المثالية، استخدام اطار عمل الأمن السيبراني لمعالجة مخاطر الأمن السيبراني جنبًا إلى جنب مع المخاطر المؤسسية الأخرى، بما في ذلك تلك المخاطر المتعلقة بالخصوصية، أو المخاطر المالية، أو سلاسل التوريد، أو السمعة، أو التقنية، أو المخاطر المادية.

يوضح الإطار المخرجات المستهدفة التي يُفترض أن يفهمها جمهور واسع، بما يشمل المديرين التنفيذيين والإداريين والممارسين، على اختلاف مستويات خبرتهم التقنية في مجال الأمن السيبراني. وبفضل حيادية هذه المخرجات من حيث القطاع، والدولة، والتكنولوجيا، فهي توفّر للمؤسسة المرونة اللازمة لمعالجة مخاطرها وتكنولوجياتها وأهدافها الخاصة. كما أن هذه المخرجات ترتبط بشكل مباشر بقائمة من الضوابط الأمنية المحتملة، التي يمكن اعتمادها فورًا لتخفيف المخاطر السيبرانية.

ورغم أن الإطار ليس إلزامياً بطبيعته، فإنه يساعد المستخدمين على فهم المخرجات المطلوبة واختيارها بشكل مناسب. كما يقدّم الإطار اقتراحات لتحقيق مخرجات محددة، مستندًا إلى مجموعة موسعة من الموارد الإلكترونية الداعمة للإطار، بما في ذلك سلسلة من الأدلة السريعة (QSG). إضافةً إلى أدوات متنوعة بصيغ قابلة للتنزيل، لتيسير عمل المؤسسات الراغبة في أتمتة بعض عملياتها. توفّر الأدلة الإرشادية السريعة طرقًا مبدئية لتطبيق الإطار، وتشجّع القارئ على استكشاف المزيد من الموارد المتاحة عبر موقع المعهد الوطني للمعايير والتكنولوجيا. ويُوصى بالنظر إلى الإطار والموارد التكميلية المتاحة على الموقع الإلكتروني لإطار عمل الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا، وغيرها، باعتبارها "حافظة أدوات" لدعم جهود إدارة المخاطر والحد منها. وبغض النظر عن طريقة استخدامه، يحفّز الإطار مستخدميه على تقييم وضعهم السيبراني في سياقه الخاص، ثم تكيفه بما يتلاءم مع احتياجاتهم الخاصة.

استنادًا إلى النسخ السابقة، يقدّم إطار عمل الأمن السيبراني (النسخة 2.0) مزايا جديدة تُبرز بشكل خاص أهمية بالاستفادة من النسخ السابقة، يقدّم إطار عمل الأمن السيبراني (النسخة 2.0) مزايا جديدة تُبرز أهمية *الحوكمة* و*سلاسل التوريد*. كما حظيت الأدلة الإرشادية السريعة باهتمام خاص لضمان ملاءمتها وسهولة الوصول إليها من قِبل المؤسسات بمختلف أحجامها، سواء كانت صغيرة أو كبيرة. يوفّر المعهد الوطني للمعايير والتكنولوجيا حاليًا *أمثلة تنفيذية ومراجع معرفية*، ويحرص على تحديثها بشكل منتظم. يُعد إنشاء *ملفات التعريف المؤسسية* لكل من الوضع الراهن والمستهدف وسيلة فعالة تمكّن المؤسسات من مقارنة حالتها الحالية بما تطمح إلى تحقيقه، مما يساعد على تسريع وتيرة تنفيذ الضوابط وتقييم فعاليتها.

ومع تزايد مخاطر الأمن السيبراني باستمرار، تبرز الحاجة إلى أن تكون إدارة تلك المخاطر عملية دائمة ومتواصلة. وينطبق ذلك سواء كانت المؤسسة في بدايات تعاملها مع التحديات السيبرانية، أو كانت تتمتع بخبرة واسعة وتملك فريقًا سيبرانيًا متقدمًا وموارد مخصصة. صُمم هذا الإطار ليخدم جميع أنواع المؤسسات، ومن المتوقع أن يقدّم إرشادات فعالة وملائمة لسنوات عديدة مقبلة.

1. نظرة عامة على إطار عمل الأمن السيبراني

تمثل هذه الوثيقة النسخة 2.0 من إطار عمل الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا ("*الإطار*"). وتتألف مما يلي:

- تشكل ***"نواة إطار العمل"*** جوهر الإطار، وهي تصنيف للمخرجات السيبرانية رفيعة المستوى، يمكن أن يساعد أي مؤسسة في إدارة مخاطرها السيبرانية بفعالية. تتكوّن نواة الإطار من تسلسل هرمي يضم الوظائف (Functions)، والتصنيفات (Categories)، والتصنيفات الفرعية (Subcategories)، التي توضح تفاصيل كل مخرج بشكل دقيق. وقد صُمّمت هذه المخرجات لتكون مفهومة لجميع فئات الجمهور المستهدف، من المديرين التنفيذيين ومديري الإدارات إلى الممارسين، بغض النظر عن مستوى خبرتهم التكنولوجية في مجال الأمن السيبراني. ونظرًا لحيادية هذه المخرجات من حيث القطاع والدولة والتكنولوجيا، فإنها تمنح المؤسسة المرونة الكافية لمعالجة مخاطرها وتكنولوجياتها وأهدافها الخاصة.
- ***الملفات التعريفية المؤسسية (CSF Organizational Profiles)*** هي وسيلة لعرض الوضع السيبراني الحالي أو المستهدف للمؤسسة، وذلك بالاعتماد على مخرجات نواة إطار العمل.
- ***المستويات (CSF Tiers)*** هي مستويات تُستخدم في الملفات التعريفية لوصف مدى نضج المؤسسة في حوكمة وإدارة المخاطر السيبرانية. كما توفّر المستويات سياقًا يعكس كيفية تعامل المؤسسة مع مخاطر الأمن السيبراني، ومدى شمولية الإجراءات المعتمدة لإدارتها.

تصف هذه الوثيقة المخرجات المنشودة التي قد تسعى المؤسسة إلى تحقيقها، دون أن تفرض مخرجات معينة ودون أن تفرض كيفية تحقيقها. بل تقدم أوصافًا *لكيفية* تحقيق هذه المخرجات عبر مجموعة من الموارد الإلكترونية التكميلية المتاحة على الموقع الإلكتروني لإطار عمل الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا. توفر هذه الموارد إرشادات إضافية حول الممارسات والضوابط التي يمكن الاستعانة بها لتحقيق المخرجات المنشودة، وتهدف إلى دعم المؤسسة في فهم إطار عمل الأمن السيبراني (CSF) واعتماده وتطبيقه بفعالية. وتشمل هذه الموارد:

- *المراجع المعرفية (Informative References)* وتُشير إلى مصادر التوجيه عن كل مخرج من الإرشادات والمعايير والأطر والسياسات والأنظمة العالمية وما إليها.
- *النماذج التنفيذية (Implementation Examples)* التي توضح الطرق التي يمكن تنفيذها لتحقيق كل نتيجة.
- *الأدلة السريعة (Quick-Start Guides)* التي توفّر إرشادات عملية لاستخدام الإطار وموارده المتوفرة عبر الإنترنت، بما في ذلك التحول من النسخ السابقة إلى النسخة 2.0.
- *الملفات التعريفية المجتمعية والقوالب المؤسسية* التي تساعد المؤسسات في تطبيق الإطار وتحديد أولوياتها في إدارة مخاطر الأمن السيبراني.

يمكن للمؤسسات استخدام نواة الإطار والملفات التعريفية والمستويات، مع الموارد التكميلية، من أجل الفهم والتقييم وتحديد الأولويات والتواصل بشأن مخاطر الأمن السيبراني:

- **الفهم والتقييم**: توصيف الوضع السيبراني الحالي أو المستهدف لمؤسسة كاملها أو جزء منها، وتحديد الفجوات، وتقييم التقدم نحو معالجتها.
- **تحديد الأولويات**: تحديد وترتيب الإجراءات الخاصة بإدارة المخاطر السيبرانية حسب الأولوية بما يتماشى مع رسالة المؤسسة ومتطلباتها القانونية والتنظيمية وتوجهاتها لإدارة المخاطر.
- **التواصل**: استخدام لغة مشتركة للتواصل الداخلي والخارجي حول المخاطر والقدرات والحاجات والتوقعات السيبرانية.

صُمم إطار عمل الأمن السيبراني لدعم المؤسسات على اختلاف أحجامها وقطاعاتها، سواء كانت صناعية، أو حكومية، أو أكاديمية، أو غير ربحية، بغض النظر عن درجة نضج برامجها للأمن السيبراني، في إدارة مخاطر الأمن السيبراني والحد منها بفعالية. ويُعد هذا الإطار موردًا محوريًا يمكن تبنّيه بشكل طوعي واستنادًا إلى السياسات والقرارات الحكومية. كما أن التصنيفات والمعايير المشار إليها والإرشادات والإجراءات المرتبطة بها غير مقتصرة على دولة بعينها، إذ استفادت منه العديد من الحكومات والمؤسسات داخل الولايات المتحدة وخارجها في النسخ السابقة.

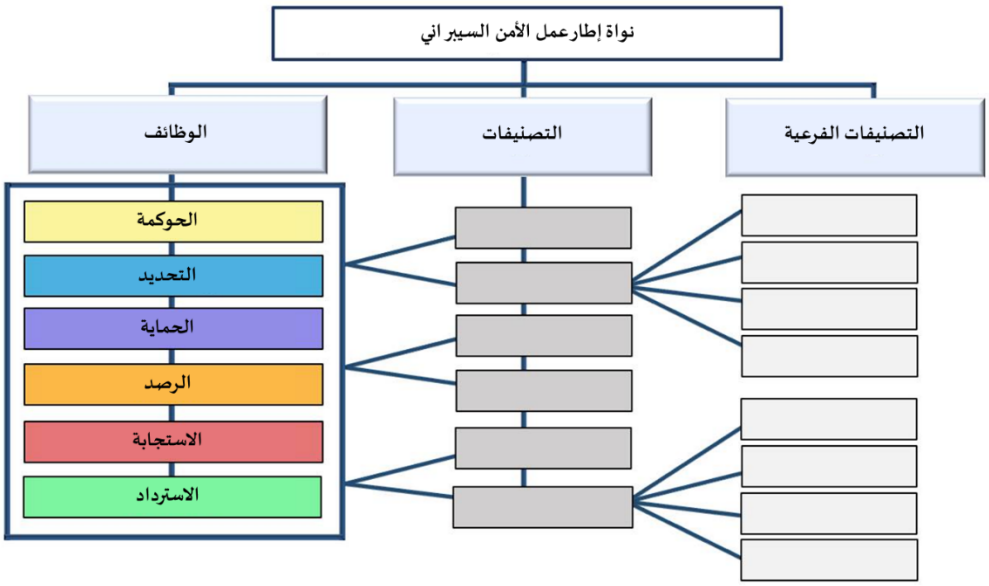
ينبغي استخدام هذا الإطار بالتوازي مع موارد أخرى، مثل الأطر والمعايير والإرشادات وأفضل الممارسات، بهدف تعزيز إدارة مخاطر الأمن السيبراني ودعم الإدارة الشاملة لمخاطر تكنولوجيا المعلومات والاتصالات على مستوى المؤسسة. وقد صُمم الإطار ليكون مرنًا وقابلًا للتكيّف مع احتياجات كل مؤسسة على حدة. ونظرًا لتفاوت المؤسسات في طبيعة مخاطرها، ومستويات تقبّلها لها، ورسائلها وأهدافها، فإن منهجياتها في تطبيق إطار عمل الأمن السيبراني ستتباين تبعًا لذلك.

تتبع بقية هذه الوثيقة الهيكل التالي:

- القسم 2: شرح أساسيات نواة إطار العمل من حيث الوظائف والتصنيفات الفرعية.
- القسم 3: تعريف مفهومي الملفات التعريفية والمستويات.
- القسم 4: نظرة عامة على بعض الموارد المختارة لإطار العمل والمتوفرة عبر الإنترنت وتشمل المراجع المعرفية والنماذج التنفيذية والأدلة السريعة.
- القسم 5: كيفية دمج إطار عمل الأمن السيبراني مع برامج إدارة المخاطر الأخرى.
- الملحق A: نواة إطار العمل.
- الملحق B: تمثيل تصوّري لمستويات إطار العمل.
- الملحق C: معجم مصطلحات إطار العمل.

2. مقدمة إلى نواة إطار العمل

A الملحق نواة الإطار، وهي مجموعة من مخرجات الأمن السيبراني مصنّفة حسب الوظائف، ثم التصنيفات، وأخيرًا التصنيفات الفرعية، كما هو موضح في الشكل 1. لا تشكل هذه المخرجات قائمة مرجعية للإجراءات الواجب اتخاذها، إذ تختلف الإجراءات المحددة لتحقيق كل مخرج من مؤسسة إلى أخرى حسب السياق، كما يختلف المسؤول عن تنفيذها. ولا يشير ترتيب الوظائف والتصنيفات وكذلك التصنيفات الفرعية وحجمها إلى ترتيب زمني أو أولوية محددة. وقد صُمم هيكل البنية ليُركز أساسًا على المسؤولين عن تنفيذ إدارة المخاطر داخل المؤسسة.



الشكل 1 هيكل نواة إطار العمل

تنظم الوظائف الأساسية في نواة إطار عمل الأمن السيبراني — الحوكمة (GOVERN)، والتحديد (IDENTIFY)، والحماية (PROTECT)، والرصد (DETECT)، والاستعادة (RESPOND)، والاسترداد (RECOVER) — المخرجات السيبرانية على أعلى مستوى.

- **الحوكمة (GOVERN)** : *وضع استراتيجية إدارة المخاطر السيبرانية للمؤسسة وتعميمها ومراقبة تنفيذها، وتحديد السياسات والتوقعات ذات الصلة*. توفر وظيفة الحوكمة مخرجات تساعد المؤسسة على توجيه وتحديد باقي الوظائف الخمس الأخرى حسب الأولوية، بما يتماشى مع رسالتها وتوقعات أصحاب المصلحة. وتُعد أنشطة الحوكمة ضرورية لدمج الأمن السيبراني في الاستراتيجية الأشمل لإدارة مخاطر المؤسسة. تركز وظيفة الحوكمة على فهم السياق التنظيمي، ووضع استراتيجية للأمن السيبراني وإدارة مخاطر سلسلة التوريد السيبرانية، وتحديد الأدوار والمسؤوليات والصلاحيات، ووضع السياسات، والإشراف على تنفيذ استراتيجية الأمن السيبراني.

- **التحديد (IDENTIFY)**: *فهم المؤسسة للمخاطر السيبرانية الحالية*. فهم الأصول (مثل البيانات، والأجهزة، والبرمجيات، والأنظمة، والمرافق، والخدمات، والموارد البشرية)، والمورّدين، والمخاطر ذات الصلة، بهدف تحديد الأولويات بما يتماشى مع استراتيجياتها للمخاطر واحتياجات الرسالة التي حُدّدت في وظيفة الحوكمة. تشمل هذه الوظيفة أيضًا تحديد فرص تحسين سياسات المؤسسة وخططها وعملياتها وإجراءاتها وممارساتها، بما يدعم إدارة مخاطر الأمن السيبراني ويوجه الجهود عبر جميع الوظائف الست.

- **الحماية (PROTECT)**:*تطبيق الضوابط اللازمة لإدارة المخاطر السيبرانية*. بمجرد تحديد الأصول والمخاطر وترتيبها حسب الأولوية، تدعم وظيفة الحماية قدرة المؤسسة على تأمين تلك الأصول بهدف منع أو تقليل احتمالية وتأثير الأحداث السيبرانية الضارة، مع زيادة فرص الاستفادة من الفرص المحققة والأثر الناتج عنها. تشمل المخرجات المرتبطة بهذه الوظيفة ما يلي: إدارة الهوية والمصادقة عليها

والتحكم في الوصول؛ والوعي والتدريب؛ وأمن البيانات؛ وأمن المنصات (أي تأمين الأجهزة والبرمجيات والخدمات للمنصات المادية والافتراضية)؛ وقدرة البنية التحتية التكنولوجية على الصمود.

- **الرصد (DETECT):** *اكتشاف وتحليل الهجمات أو التهديدات السيبرانية المحتملة*. تمكّن وظيفة الرصد من تحديد وتحليل الشذوذات ومؤشرات الاختراق وغيرها من الأحداث التي قد تشير إلى وقوع حوادث سيبرانية. وتُعد هذه الوظيفة أساسية لنجاح أنشطة الاستجابة والاسترداد.
- **الاستجابة (RESPOND):** *الإجراءات المتخذة عند اكتشاف حادث سيبراني*. تدعم وظيفة الاستجابة قدرة المؤسسة على احتواء آثار الحوادث السيبرانية، وتشمل مخرجاتها: إدارة الحوادث، والتحليل، والتقليل، والإبلاغ، والاتصالات.
- **الاسترداد (RECOVER):** *استرداد الأصول والعمليات التي تأثرت بالحوادث السيبرانية*. تدعم وظيفة استرداد العمليات إلى وضعها الطبيعي في الوقت المناسب للحد من آثار الحوادث ولضمان إجراء الاتصالات المناسبة أثناء جهود الاسترداد.

ورغم أن معظم أنشطة إدارة مخاطر الأمن السيبراني تركز على منع وقوع الأحداث السلبية، إلا أنها قد تتيح أيضًا فرصًا لتحقيق مكاسب إيجابية. فقد تسهم التدابير المتخذة للحد من المخاطر السيبرانية في تحقيق مزايا استراتيجية للمؤسسة، مثل زيادة الإيرادات. فعلى سبيل المثال، يمكن للمؤسسة الاستفادة من المساحات غير المستخدمة في منشآتها من خلال تأجيرها لمزوّد استضافة تجاري، لاستضافة مراكز بيانات لها ولمؤسسات أخرى، ثم نقل نظام مالي رئيسي من مركز البيانات الداخلي إلى مقدم خدمات خارجي بهدف تقليل المخاطر السيبرانية

يعرض الشكل 2 وظائف إطار عمل الأمن السيبراني (CSF) في صورة عجلة دائرية، لأن جميع الوظائف مترابطة فيما بينها. فعلى سبيل المثال، تصنف المؤسسة الأصول ضمن وظيفة التحديد (IDENTIFY)، وتتخذ إجراءات لتأمين تلك الأصول ضمن وظيفة الحماية (PROTECT). ستدعم الاستثمارات في التخطيط والاختبار ضمن وظيفتي الحوكمة (GOVERN) والتحديد (IDENTIFY) الاكتشاف الفوري للأحداث غير المتوقعة ضمن وظيفة الرصد (DETECT)، كما تُمكّن من تنفيذ إجراءات الاستجابة والاسترداد من الحوادث السيبرانية ضمن وظيفتي الاستجابة (RESPOND) والاستعادة ((RECOVER. تتوسط وظيفة الحوكمة (GOVERN) هذه العجلة لأنها توجه قيام المؤسسة بتنفيذ الوظائف الخمس الأخرى.

الشكل 2 وظائف إطار عمل الأمن السيبراني (CSF Functions)

ينبغي تنفيذ الوظائف بالتوازي. ينبغي تنفيذ الإجراءات الداعمة لوظائف الحوكمة، والتحديد، والحماية، والرصد بشكل مستمر، وينبغي أن تكون الإجراءات الداعمة لوظائف الاستجابة والاسترداد جاهزة دائمًا مع تفعيلها عند وقوع حوادث أمنية سيبرانية. لكل وظيفة دور حيوي يتعلق بالحوادث السيبرانية. تُسهم مخرجات وظائف الحوكمة، والتحديد، والحماية في منع الحوادث والاستعداد لها، بينما تُسهم مخرجات وظائف الحوكمة، والكشف، والاستجابة، والاسترداد في اكتشاف الحوادث والتعامل معها.

يأتي اسم كل وظيفة بعد فعل يلخص محتواها. تنقسم كل وظيفة إلى *تصنيفات (Categories)* تمثل مخرجات سيبرانية مترابطة تشكل الوظيفة في مجملها. وتُقسم التصنيفات بدورها إلى *تصنيفات فرعية (Subcategories)* تصف بشكل أكثر تفصيلًا المخرجات التكنولوجية والإدارية المراد تحقيقها. التصنيفات الفرعية ليست شاملة، لكنها تُمثل مخرجات محددة تدعم كل تصنيف.

تنطبق الوظائف والتصنيفات الفرعية على جميع أنواع تكنولوجيا المعلومات والاتصالات (ICT) المستخدمة في المؤسسة، بما يشمل تكنولوجيا المعلومات (IT)، وإنترنت الأشياء (IoT)، والتكنولوجيا التشغيلية (OT). كما تنطبق على جميع أنواع البيئات التكنولوجية، بما في ذلك الحوسبة السحابية، والأنظمة المتنقلة، وأنظمة الذكاء الاصطناعي. تشكّل النواة الأساسية لإطار عمل الأمن السيبراني مكونًا استشرافيًا صُمم ليتماشى مع التغيرات المستقبلية في التكنولوجيا والبيئات التشغيلية.

3. مقدمة عن الملفات التعريفية والمستويات في إطار عمل الأمن السيبراني ((CSF Profiles and Tiers

يستعرض هذا القسم المفاهيم الأساسية للملفات التعريفية (Profiles) والمستويات (Tiers) في إطار عمل الأمن السيبراني.

3.1. الملفات التعريفية لإطار عمل الأمن السيبراني

يُعبّر الملف التعريفي المؤسسي لإطار عمل الأمن السيبراني عن الوضع الراهن و/أو المستهدف للأمن السيبراني داخل المؤسسة من حيث المخرجات الواردة في نواة (Core) الإطار. وتُستخدم الملفات التعريفية المؤسسية هذه لفهم وتكييف وتقييم وتحديد أولويات وتوصيل مخرجات الإطار، مع الأخذ في الحسبان أهداف رسالة المؤسسة، وتوقعات أصحاب المصلحة، والوضع الراهن للتهديدات، والمتطلبات. ومن ثم، يمكن للمؤسسة تحديد الإجراءات التي يتعين اتخاذها لتحقيق مخرجات محددة حسب الأولوية، وإبلاغ أصحاب المصلحة بهذه المعلومات.

يشتمل كل ملف تعريفي على العنصرين التاليين أو أيهما:

1. *الملف التعريفي الحالي (Current Profile)* الذي يحدد المخرجات الأساسية التي تحققها المؤسسة حالياً (أو تحاول تحقيقها)، ويصف كيفية أو مدى تحقيق كل نتيجة.
2. *ملف التعريف المستهدف (Target Profile)* الذي يحدد المخرجات المستهدفة التي اختارتها المؤسسة وأولويتها لتحقيق أهدافها في إدارة مخاطر الأمن السيبراني. ويأخذ الملف التعريفي المستهدف في الحسبان التغيّرات المتوقعة في وضع الأمن السيبراني للمؤسسة، مثل المتطلبات الجديدة، وتبني التكنولوجيا الحديثة، وتوجهات المعلومات الاستقصائية بشأن التهديدات السيبرانية.

> *يُعد الملف المجتمعي* (Community Profile) خط أساس لمخرجات إطار عمل الأمن السيبراني (CSF) يتم إنشاؤه ونشره لمعالجة المصالح والأهداف المشتركة بين عدد من الجهات. عادةً ما يتم تطوير الملف المجتمعي لقطاع معين، أو قطاع فرعي، أو تكنولوجيا محددة، أو نوع تهديد، أو حالة استخدام أخرى. يمكن للمؤسسة استخدام الملف المجتمعي بوصفه أساسًا لبناء ملفها التعريفي المستهدف (Target Profile). يمكن الاطلاع على نماذج للملفات المجتمعية على موقع إطار عمل الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا.

توضح الخطوات المعروضة في الشكل 3 والملخصة أدناه، أحد الطرق التي يمكن أن تستخدمها المؤسسة لتوظيف الملف التنظيمي (Organizational Profile) كأداة لدعم التحسين المستمر في الأمن السيبراني.

الشكل 3 خطوات إعداد واستخدام الملف التنظيمي لإطار عمل الأمن السيبراني

1. **تحديد نطاق الملف المؤسسي.** يجب توثيق الحقائق والافتراضات رفيعة المستوى التي يُبنى عليها الملف لتحديد نطاقه بشكل واضح. يمكن للمؤسسة إعداد عدد غير محدود من الملفات التنظيمية، كل منها يغطي نطاقًا مختلفًا. على سبيل المثال، يمكن إعداد ملف يغطي المؤسسة بالكامل، أو يُركّز على الأنظمة المالية فقط، أو يُعنى بالتعامل مع تهديدات الفدية الإلكترونية (Ransomware) وإجراءات الاستجابة للحوادث المرتبطة بهذه الأنظمة.

2. **جمع المعلومات اللازمة لإعداد الملف المؤسسي.** قد تشتمل الأمثلة على هذه المعلومات: السياسات الداخلية، وأولويات وموارد إدارة المخاطر، وملفات المخاطر المؤسسية، وسجلات تحليل أثر الأعمال (BIA)، ومتطلبات ومعايير الأمن السيبراني المتبعة في المؤسسة، والممارسات والأدوات المستخدمة (مثل الإجراءات والتدابير الوقائية)، بالإضافة إلى الأدوار والمسؤوليات.

3. **إنشاء الملف المؤسسي.** تُحدَّد أنواع المعلومات الواجب تضمينها في الملف بناءً على المخرجات ذات الصلة من إطار عمل الأمن السيبراني، مع توثيق المعلومات المطلوبة. ويُراعى عند إعداد الملف فهم تداعيات المخاطر المرتبطة بالملف الحالي، بهدف توجيه عمليات التخطيط وتحديد الأولويات للملف المستهدف. كما يُوصى بدراسة إمكانية الاستفادة من ملف مجتمعي قائم كمرجعية تُسهم في إعداد الملف المستهدف بفعالية.

4. **تحليل الفجوات بين الملف الحالي والمستهدف، وإعداد خطة العمل.** يُجرى تحليل فجوات لتحديد الفروقات بين الملف الحالي والمستهدف وتحليلها، ثم تطوير خطة عمل ذات أولويات واضحة (مثل سجل المخاطر، وتقرير تفصيلي للمخاطر، وخطة العمل والمراحل الرئيسية ([POA&M]) لمعالجة تلك الفجوات.

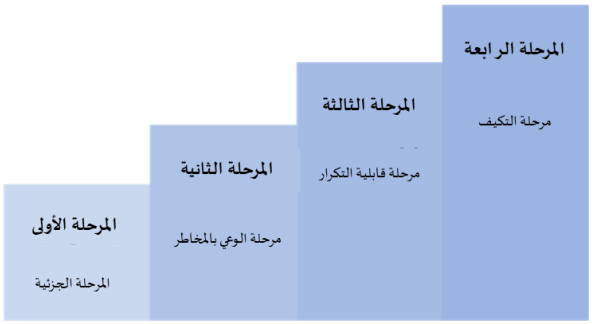
5. **تنفيذ خطة العمل وتحديث الملف المؤسسي.** تُنفذ خطة العمل لمعالجة الفجوات ودفع المؤسسة نحو تحقيق الملف التعريفي المستهدف. قد يكون لخطة العمل موعد نهائي عام ويمكن أن تستمر دوريًا.

ونظرًا لأهمية التحسين المستمر، يمكن للمؤسسة تكرار هذه الخطوات حسب الحاجة.

هناك استخدامات إضافية للملفات التعريفية المؤسسية. على سبيل المثال، يمكن استخدام الملف التعريفي الحالي لتوثيق القدرات السيبرانية للمؤسسة وفرص التحسين المحتملة، ومشاركتها مع أصحاب المصلحة الخارجيين مثل الشركاء التجاريين أو العملاء المحتملين. كما يمكن للملف التعريفي المستهدف أن يُعبّر عن متطلبات وتوقعات المؤسسة في إدارة مخاطر الأمن السيبراني تجاه الموردين والشركاء والجهات الأخرى بوصفه معيارًا تستهدف تلك الجهات تحقيقه.

3.2. مستويات إطار عمل الأمن السيبراني

قد تختار إحدى المؤسسات استخدام مستويات تنفيذ إطار العمل لإعداد كل من ملفاتها الحالية والمستهدفة، إذ تصف *المستويات* الدرجة الدقة في ممارسات إدارة المخاطر السيبرانية، وتوفّر سياقًا لتصور المؤسسة بشأن المخاطر السيبرانية والعمليات المنفذة لإدارة تلك المخاطر. وتوضح المستويات -على النحو الموضح في الشكل 4والمُوضح بشكل افتراضي الملحق Bممارسات المؤسسة لإدارة المخاطر السيبرانية، على سبيل المثال: المستوى الجزئي (المستوى الأول)، ومستوى الوعي بالمخاطر (المستوى الثاني)، ومستوى قابلية التكرار (المستوى الثالث)، ومستوى التكيف (المستوى الرابع) وتصف المستويات التحول من الاستجابات التي ليس لها طابع رسمي والمؤقتة إلى النُهج التي تمتاز بالمرونة وإدراك المخاطر والتحسين المستمر، وتسهم عملية اختيار مستويات الإطار في تحديد الوضع العام لآلية إدارة المخاطر السيبرانية داخل المؤسسة.



الشكل 4. مستويات إطار عمل الأمن السيبراني لإدارة المخاطر السيبرانية

من المفترض أن تُستخدم مستويات الإطار كعنصرٍ متمم لمنهجية إدارة المخاطر السيبرانية وليس بديلاً عنها، فعلى سبيل المثال، يمكن نشر هذه المستويات داخل المؤسسة والاستعانة بها كدراسة معيارية لتحديد النهج[1] المتبع لإدارة المخاطر السيبرانية في المؤسسة. ويتم الحث على الاستمرار في مسيرة التقدم والوصول إلى مراحل أعلى في الإطار عند وجود مخاطر أكبر أو تزايد المهام التنظيمية، أو عندما يشير تحليل التكاليف والفوائد إلى إمكانية الحد من المخاطر السيبرانية السلبية وفاعليتها من حيث التكلفة.

يوفر الموقع الإلكتروني لإطار عمل الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا معلومات إضافية عن استخدام الملفات التعريفية والمراحل والمستويات، ويتضمن إرشادات بشأن نماذج ملفات تعريفية مؤسسية تستضيفها الهيئة وسجل ملفات تعريفية مجتمعية متوفرة بصيغ قابلة للقراءة الآلية أو الاستخدام البشري.

[1] ولأغراض هذه الوثيقة، يشير لفظ "على مستوى المؤسسة" و"المؤسسة" إلى المعنى ذاته.

4. مقدمة عن الموارد الإلكترونية المتممة لإطار عمل الأمن السيبراني

قام المعهد الوطني للمعايير والتكنولوجيا، إلى جانب مؤسسات أخرى، بتطوير مجموعة من الموارد الإلكترونية لدعم المؤسسات في فهم إطار عمل الأمن السيبراني وتبنّيه وتطبيقه. وتتوفر هذه الموارد عبر الإنترنت، مما يسمح بتحديثها بوتيرة أسرع مقارنةً بهذه الوثيقة، التي يتم تحديثها بشكل أقل تواترًا حفاظًا على مرجعيتها واستقرارها للمستخدمين. كما أن هذه الموارد متاحة بصيغ قابلة للقراءة الآلية، بما يُسهّل استخدامها في الأنظمة التقنية المختلفة. ويقدّم هذا القسم نظرة عامة على ثلاثة أنواع رئيسية من هذه الموارد الإلكترونية: المراجع المعرفية، والنماذج التنفيذية، وأدلة البدء السريع.

المراجع المعرفية هي خرائط تشير إلى العلاقات بين معايير نواة إطار العمل والإرشادات واللوائح التنظيمية والمحتوى ذي الصلة، وتسهم هذه المراجع في توجيه كيفية تحقيق النتائج المرجوة من نواة إطار عمل المؤسسة، وقد تتعلق بقطاعات أو تكنولوجيا محددة، كما يمكن إعدادها من جانب المعهد أو مؤسسة أخرى. وتضم بعض المراجع المعرفية نطاق أضيق من التصنيفات الفرعية. فعلى سبيل المثال، قد يكون عنصر تحكم معين من الأمن والخصوصية 800-53 -ضوابط الأمن والخصوصية لأنظمة المعلومات والمؤسسات- أحد المراجع المتعددة اللازمة لتحقيق النتيجة الموضحة في تصنيف فرعي واحد، وقد تكون المراجع المعرفية الأخرى ذات مستوى أعلى، على سبيل المثال: شرط أساسي من سياسة تتناول جزئيًا العديد من التصنيفات الفرعية، ويسهم إطار عمل الأمن السيبراني في تمكين المؤسسة من تحديد المراجع المعرفية الأكثر صلة.

تقدم *نماذج التنفيذ* أمثلة نظرية لخطوات دقيقة وعملية تسهم في تحقيق نتائج التصنيفات الفرعية. وتشمل الأفعال المستخدمة للتعبير عن النماذج المشاركة، والتوثيق، والإعداد، والتنفيذ، والمراقبة، والتحليل، والتقييم، والممارسة. ولا تضم هذه النماذج جميع الإجراءات التي يمكن للمؤسسة اتخاذها لتحقيق نتائجها، كما أنها لا تمثل الوضع الراهن للإجراءات المطلوبة لمواجهة المخاطر السيبرانية.

أدلة البدء السريع هي وثائق موجزة لمواضيع محددة تتعلق بإطار عمل الأمن السيبراني، وغالبًا ما تكون مصممة خصيصًا لجمهور محدد. ويمكن أن تسهم هذه الأدلة في تمكين المؤسسات من تطبيق إطار عمل الأمن السيبراني لقدرتها على تلخيص أجزاء محددة من الإطار إلى "خطوات أولية" عملية يمكن للمؤسسة أخذها بعين الاعتبار عند تحسين وضعها في الأمن السيبراني وإدارة المخاطر ذات الصلة، وتخضع هذه الأدلة إلى المراجعة ضمن إطارها الزمني، وتُضاف أدلة جديدة عند الحاجة.

يمكنكم دائمًا مشاركة اقتراحاتكم بشأن المراجع المعرفية الجديدة لإطار عمل الأمن السيبراني 2.0 مع المعهد الوطني للمعايير والتكنولوجيا عبر الموقع الإلكتروني التالي: olir@nist.gov. ويُرجى توجيه اقتراحاتكم الخاصة بالموارد الأخرى التي يمكن الرجوع إليها على الموقع الإلكتروني لإطار عمل الأمن السيبراني، بما يشمل مواضيع إضافية حول أدلة البدء السريع، إلى البريد الإلكتروني التالي: cyberframework@nist.gov.

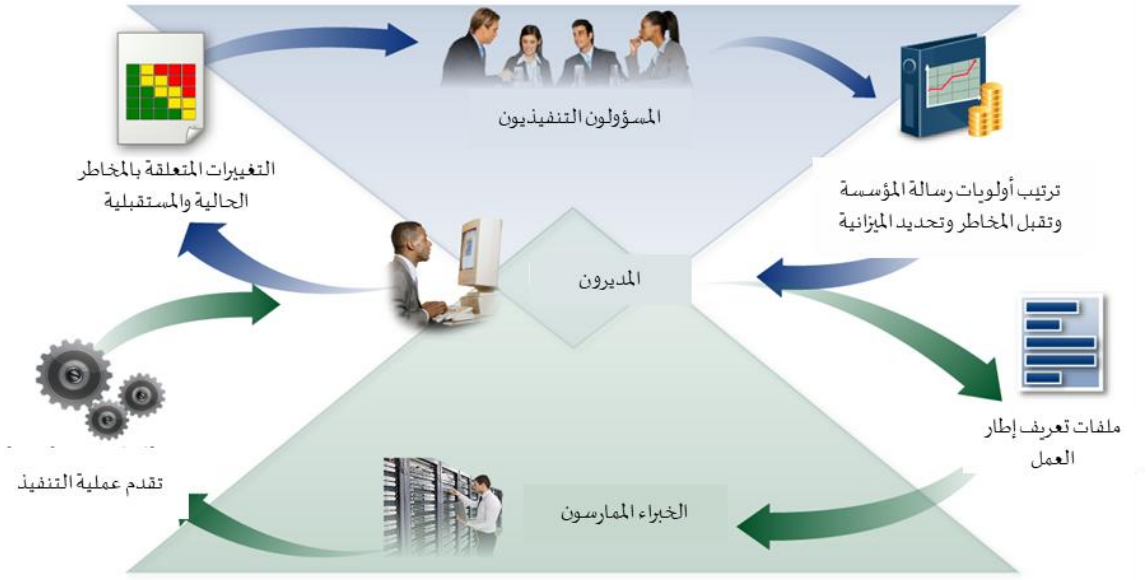
5. تحسين آلية الإبلاغ عن المخاطر السيبرانية ودمجها

تختلف آلية استخدام إطار عمل الأمن السيبراني باختلاف رسالة المؤسسة ومخاطرها. وبفهم توقعات أصحاب المصلحة ودرجة تقبلهم للمخاطر وقدرتهم على تحملها (على النحو المُحدد في وظيفة الحوكمة)، تتمكن المؤسسة من ترتيب أنشطة الأمن السيبراني حسب الأولوية لاتخاذ قرارات مدروسة بشأن نفقات الأمن السيبراني وإجراءاته. وقد تختار المؤسسة التعامل مع المخاطر بطريقة أو أكثر - بما يشمل طرق التخفيف من حدة المخاطر السلبية أو نقلها أو تجنبها أو تقبلها، وتحقيق المخاطر الإيجابية أو مشاركتها أو تعزيزها أو تقبلها - وذلك اعتمادًا على آثار هذه المخاطر واحتمالية حدوثها. والأهم أنه يمكن للمؤسسة استخدام إطار عمل الأمن السيبراني داخليًا لإدارة قدراتها في مجال الأمن السيبراني وخارجيًا للإشراف على الجهات الخارجية أو التواصل معها.

قد لا تعتمد المؤسسة إطار عمل الأمن السيبراني بصورته الكاملة، إلا أنه يمكن أن يشكّل أداة إرشادية فعّالة تُعينها على فهم المخاطر السيبرانية وتقييمها، وتصنيفها بحسب الأولوية، والإبلاغ عنها بشكل منهجي، مع تحديد الإجراءات المناسبة لمعالجتها. كما يمكن الاستفادة من النتائج المحددة في الإطار لدعم القرارات الاستراتيجية وتنفيذها، بما يسهم في تعزيز الوضع السيبراني العام للمؤسسة، وضمان استمرارية وظائفها الأساسية المرتبطة برسالتها، وذلك بما يتوافق مع أولوياتها ومواردها المتاحة.

5.1. تحسين عملية التواصل بشأن إدارة المخاطر

يوفّر إطار عمل الأمن السيبراني ركيزة أساسية لتحسين عملية التواصل بشأن توقعات الأمن السيبراني وعملية التخطيط والموارد، ويسهم في تعزيز مسار تدفّق المعلومات ثنائي الاتجاه (على النحو الموضّح في الجزء العلوي من الشكل 5) بين القيادات التنفيذية التي تركز على أولويات المؤسسة وتوجهها الاستراتيجي، وبين المديرين الذين يتولّون إدارة المخاطر السيبرانية المحددة التي قد تُخلف تأثيرًا يعوق تحقيق تلك الأولويات. ويدعم إطار العمل مسار تدفق مماثلاً (على النحو الموضّح في الجزء السفلي من الشكل 5) بين المديرين والممارسين المسؤولين عن تنفيذ التكنولوجيا وتفعيلها، ويُبرز الجانب الأيسر من الشكل مدى أهمية مشاركة الخبراء الممارسين للتحديثات والمرئيات والمخاوف مع المديرين والمسؤولين التنفيذيين.



الشكل 5. استخدام إطار عمل الأمن السيبراني لتحسين عملية التواصل لإدارة المخاطر

تشتمل إجراءات التحضير لإنشاء واستخدام ملفات تعريف تنظيمية على عمليات جمع معلومات حول أولويات المؤسسة ومواردها وتوجهات إدارة المخاطر من المسؤولين التنفيذيين، ثم يتعاون المديرون بعد ذلك مع الممارسين للإبلاغ بعن متطلبات العمل وإنشاء ملفات تعريف تنظيمية

تستند إلى معلومات عن المخاطر. وسيتخذ المديرون والخبراء الممارسين إجراءات لسد أي فجوات يتم تحديدها بين ملفات التعريف الحالية والمستهدفة، وستُوفر هذه الإجراءات مدخلات رئيسية لخطط العمل على مستوى المنظومة. وبتحقيق الهدف المنشود في جميع أنحاء المؤسسة - من خلال الضوابط والمراقبة المطبقة على مستوى المنظومة - يُمكن مشاركة النتائج المُحدثة من خلال سجلات المخاطر وتقارير سير العمل. وفي إطار التقييم الجاري، يكتسب المديرون مرئيات ثاقبة لإجراء تعديلات تُقلل من الأضرار المحتملة وتُعزز من المزايا المحتملة.

تدعم وظيفة الحوكمة عملية التواصل مع المسؤولين **التنفيذيين** بشأن المخاطر التنظيمية، وتتناول مناقشاتهم الاستراتيجية، لا سيّما كيفية تأثير أوجه عدم اليقين المتعلقة بالأمن السيبراني على تحقيق الأهداف التنظيمية. وتسهم مناقشات الحوكمة في دعم الحوار وعمليات الاتفاق المتعلقة باستراتيجيات إدارة المخاطر (بما يشمل مخاطر سلسلة الإمداد السيبرانية)؛ والأدوار والمسؤوليات والصلاحيات والسياسات والرقابة. ويُحدد المسؤولون التنفيذيون أولويات وأهداف الأمن السيبراني بناءً على تلك المتطلبات ويُبلغون في الوقت ذاته بتوقعاتهم بشأن قابلية المخاطرة والمساءلة والموارد. كما يتحملون مسؤولية دمج إدارة المخاطر السيبرانية ببرامج إدارة المخاطر المؤسسية وبرامج إدارة المخاطر ذات المستوى الأدنى (يُرجى الرجوع إلى القسم 5.2). ويمكن أن تتضمن عمليات التواصل الموضحة في النصف العلوي من الشكل 5 اعتبارات تتعلق بإدارة المخاطر المؤسسية والبرامج ذات المستوى الأدنى، ومن ثُم يمكن أن توجه المديرين والخبراء الممارسين.

تُستنبط أهداف الأمن السيبراني العامة التي يضعها المسؤولين التنفيذيين من مرئيات **المديرين** وتساعد في الوقت نفسه في توجيهم، وقد يتم تطبيق هذه الأهداف على خط عمل أو قسم تشغيلي بإحدى الجهات التجارية. أما في الجهات الحكومية، فقد تُطبق هذه الاعتبارات على مستوى قسم أو فرع معين. وسيركز المديرون -عند تطبيق إطار عمل الأمن السيبراني- على آلية تحقيق المستهدفات التي تحد من المخاطر من خلال الخدمات المشتركة والضوابط وسبل التعاون على النحو الموضح في "ملف المستهدفات"، ويتم تحسينها من خلال الإجراءات التي يتم تتبعها في خطة العمل (مثل سجل المخاطر، وتقرير تفاصيل المخاطر، وخطة العمل ومراحل الإنجاز).

ويُركز **الممارسون** على تحقيق الوضع المستهدف وقياس التغيرات ذات الصلة بالمخاطر التشغيلية للمساهمة في تخطيط أنشطة الأمن السيبراني المُحددة وتنفيذها ومراقبتها. وفي إطار تطبيق الضوابط اللازمة لإدارة المخاطر بمعدلٍ مقبول، يقوم الخبراء الممارسين بتزويد المديرين والمسؤولين التنفيذيين بالمعلومات اللازمة (على سبيل المثال: مؤشرات الأداء الرئيسية ومؤشرات المخاطر الرئيسية) لفهم وضع الأمن السيبراني في المؤسسة، واتخاذ قرارات مدروسة، والحفاظ على استراتيجية المخاطر أو تعديلها وفقًا لذلك. كما يُمكن للمسؤولين التنفيذيين دمج بيانات المخاطر السيبرانية هذه مع المعلومات المتعلقة بفئات المخاطر الأخرى التي يتم مواجهتها في المؤسسة. ويتم إدراج المستجدات المتعلقة بالتوقعات والأولويات في ملفات تعريف المؤسسة المُحدثة عند تكرار الدورة.

5.2. تحسين آلية الدمج مع برامج إدارة المخاطر الأخرى

تواجه المؤسسات بمختلف أنواعها طيفًا واسعًا من مخاطر تكنولوجيا المعلومات والاتصالات، (مثل مخاطر الخصوصية، وسلاسل الإمداد، والذكاء الاصطناعي)، وقد تعتمد أطر عمل وأدوات مخصصة لإدارة كل نوع من هذه المخاطر على حدة. وتتبنى بعض المؤسسات نهجًا تكامليًا يجمع بين جهود إدارة مخاطر تكنولوجيا المعلومات والاتصالات وغيرها من أنواع المخاطر ضمن إطار شامل لإدارة المخاطر المؤسسية. في المقابل، تفضل مؤسسات أخرى الفصل بين هذه الجهود لضمان التركيز المتخصص على كل جانب منها. أما المؤسسات الصغيرة، فغالبًا ما تتابع المخاطر على مستوى المؤسسة ككل، في حين تميل المؤسسات الكبرى إلى تخصيص جهود منفصلة لإدارة المخاطر، مع ربطها بإطار أوسع لإدارة المخاطر المؤسسية.

قد تتبنى المؤسسات نهج إدارة المخاطر المؤسسية لموازنة مجموعة من اعتبارات المخاطر، بما يشمل الأمن السيبراني، واتخاذ قرارات مدروسة. ويتلقى المسؤولون التنفيذيون مدخلات مهمة حول أنشطة المخاطر الحالية والمخطط لها، حيث يُدمجون استراتيجيات الحوكمة والمخاطر مع نتائج حالات الاستخدام السابقة لإطار عمل الأمن السيبراني. ويسهم إطار عمل الأمن السيبراني في تمكن المؤسسات من ترجمة مصطلحاتها الخاصة بالأمن السيبراني وإدارة المخاطر السيبرانية إلى لغة إدارة المخاطر العامة التي يفهمها المسؤولون التنفيذيون.

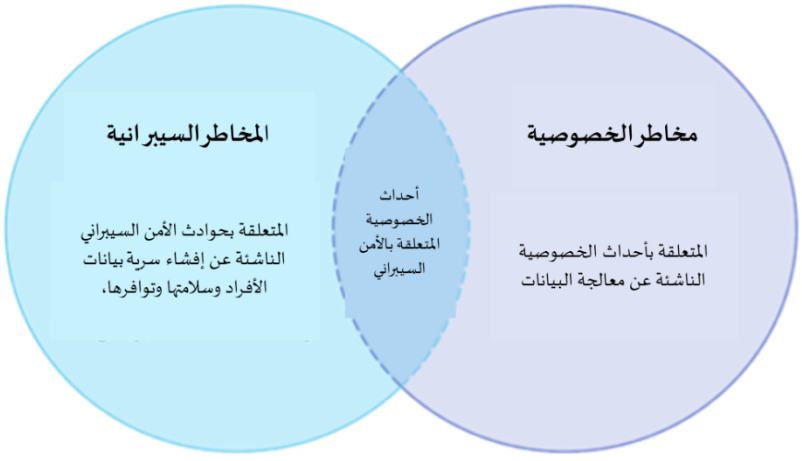
تتضمن موارد المعهد الوطني للمعايير والتكنولوجيا التي تصف العلاقة المتبادلة بين إدارة المخاطر السيبرانية وإدارة المخاطر المؤسسية ما يلي:

- *إطار عمل الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا 2.0 - دليل البدء السريع في إدارة المخاطر المؤسسية*
- التقرير المشترك بين الوكالات الصادر عن المعهد الوطني للمعايير والتكنولوجيا (IR 8286) *دمج إدارة المخاطر المؤسسية بإدارة المخاطر السيبرانية)*
- التقرير المشترك بين الوكالات 8286أ (IR 8286A)، *تحديد وتقدير المخاطر السيبرانية لإدارة المخاطر المؤسسية*
- التقرير المشترك بين الوكالات 8286ب (IR 8286B)، *ترتيب المخاطر السيبرانية حسب الأولوية لإدارة المخاطر المؤسسية*
- التقرير المشترك بين الوكالات 8286ج (IR 8286C)، *تنظيم المخاطر السيبرانية لإدارة المخاطر المؤسسية والإشراف على الحوكمة*
- التقرير المشترك بين الوكالات 8286د (IR 8286D)، *استخدام تحليل أثر الأعمال لتوجيه تحديد المخاطر ذات الأولوية والاستجابة لها*
- المنشور الخاص 800-221 (SP 800-221)، *تأثير مخاطر تكنولوجيا المعلومات والاتصالات على المؤسسات: حوكمة وإدارة برامج مخاطر تكنولوجيا المعلومات والاتصالات ضمن محفظة مخاطر المؤسسة*
- المنشور الخاص 800-221أ (SP 800-221A)، *نتائج مخاطر تكنولوجيا المعلومات والاتصالات: دمج برامج إدارة مخاطر تكنولوجيا المعلومات والاتصالات مع محفظة مخاطر المؤسسة*

قد تتحقق المؤسسة من جدوى إطار عمل الأمن السيبراني في عمليات دمج إدارة المخاطر السيبرانية ببرامج إدارة مخاطر تكنولوجيا المعلومات والاتصالات الفردية، على سبيل المثال:

- **إدارة المخاطر السيبرانية وتقييمها:** يمكن دمج إطار عمل الأمن السيبراني ببرامج إدارة وتقييم المخاطر السيبرانية المنفذة، مثل: *المنشور الخاص (SP 800-37)، وإطار عمل إدارة المخاطر المتعلقة بأنظمة المعلومات والمؤسسات، والمنشور الخاص (SP 800-30)، ودليل إجراء تقييمات المخاطر* من إطار عمل إدارة المخاطر الصادر عن المعهد الوطني للمعايير والتكنولوجيا. وفيما يتعلق بالمؤسسات التي تستخدم إطار عمل إدارة المخاطر الصادر عن المعهد الوطني للمعايير والتكنولوجيا ومجموعة منشوراته، يمكن استخدام إطار عمل الأمن السيبراني لتكملة نهج إطار عمل إدارة المخاطر في اختيار وترتيب الضوابط الواردة في المنشور الخاص (SP 800-53): ضوابط الأمن والخصوصية لأنظمة المعلومات والمؤسسات.

- **مخاطر الخصوصية:** على الرغم من أن كل من الأمن السيبراني والخصوصية يُعدان تخصصين مستقلين عن بعضهما، إلا أنهما يشتركان في أهدافهما في بعض الأحيان كما هو موضح في الشكل 6.



الشكل 6. العلاقة بين المخاطر السيبرانية ومخاطر الخصوصية

تُعد إدارة المخاطر السيبرانية أمرًا ضروريًا لمواجهة مخاطر الخصوصية المتعلقة بإفشاء سرية بيانات الأفراد وسلامتها وتوافرها، فعلى سبيل المثال، قد تؤدي عمليات اختراق البيانات إلى سرقة الهوية، إلا أنه تنشأ مخاطر الخصوصية أيضًا من خلال وسائل لا علاقة لها بحوادث الأمن السيبراني.

وتقوم المؤسسات بمعالجة البيانات لتحقيق رسالة معينة أو أغراض تجارية، مما قد يؤدي أحيانًا إلى مواجهة الأفراد مشاكل تتعلق بخصوصيتهم جراء معالجة البيانات. وقد تتمثل هذه المشاكل في طرق شتى إلا أن المعهد الوطني للمعايير والتكنولوجيا يرى أن هذه المشكلة قد تخلف آثار متفاوتة تتعلق بالكرامة (على سبيل المثال: إحراج أو خزي) وأضرار أخرى ملموسة بشكل أكبر (على سبيل المثال: تحيّز أو خسارة اقتصادية أو أذى جسدي). يمكن استخدام إطار عمل الخصوصية الصادر عن المعهد الوطني للمعايير والتكنولوجيا بجانب إطار عمل الأمن السيبراني لمواجهة المخاطر السيبرانية والخصوصية من مختلف جوانبها. وتشتمل منهجية تقييم مخاطر الخصوصية المتبعة في المعهد الوطني للمعايير والتكنولوجيا على قائمة بأمثلة المشاكل التي يتم مواجهتها للاستعانة بها في تقييمات مخاطر الخصوصية.

- **مخاطر سلسلة الإمداد:** بإمكان المؤسسة استخدام إطار عمل الأمن السيبراني لتعزيز إجراءات مراقبة المخاطر السيبرانية والتواصل مع أصحاب المصلحة عبر سلاسل الإمداد. وتعتمد التكنولوجيا بمختلف أنواعها على منظومة سلسلة إمداد معقدة وموزعة عالميًا وواسعة النطاق ومتداخلة وذات مسارات متنوعة جغرافيًا ومستويات متعددة من الاستعانة بمصادر خارجية. وتتألف هذه المنظومة من جهات من كل من القطاعين العام والخاص (على سبيل المثال: جهات الشراء، والمورّدين، والمطورّين، وجهات دمج الأنظمة، ومُقدمي خدمات الأنظمة الخارجيين، وغيرهم من مُقدمي الخدمات المتعلقة بالتكنولوجيا) التي تتفاعل فيما بينها لأغراض البحث عن المنتجات والخدمات التكنولوجية وتطويرها وتصميمها وتصنيعها وشرائها وتسليمها ودمجها وتشغيلها وصيانتها وحذفها أو أي أنشطة أخرى تتعلق باستخدامها أو إدارتها. وتُبنى عمليات التفاعل هذه وتتأثر بالتكنولوجيا والقوانين والسياسات والإجراءات والممارسات.

  تُعد إدارة مخاطر سلسلة الإمداد ذات أهمية حيوية للمؤسسات نظرًا لتعقد العلاقات وتداخلها في المنظومة. تُعد إدارة مخاطر سلسلة الإمداد للأمن السيبراني من العمليات المنهجية لإدارة التعرض للمخاطر السيبرانية عبر سلاسل الإمداد، ووضع استراتيجيات وسياسات وعمليات وإجراءات مناسبة للتصدي لتلك المخاطر. وتُعد التصنيفات الفرعية التي تندرج ضمن التصنيف الرئيسي لإدارة مخاطر سلسلة الإمداد للأمن السيبراني [سلاسل الإمداد المتعلقة بالحوكمة] أداةً للربط بين النتائج التي تُركز بشكل حصري على الأمن السيبراني وتلك التي تُركز على إدارة مخاطر سلسلة الإمداد للأمن السيبراني ذات الصلة. ويقدم المنشور الخاص (SP 800-161r1) (المراجعة 1) - *ممارسات إدارة مخاطر سلسلة الإمداد للأمن السيبراني للأنظمة والمؤسسات* - معلومات متعمقة عن إدارة مخاطر سلسلة الإمداد للأمن السيبراني.

- **المخاطر الناشئة عن التكنولوجيا المتطورة:** تظهر مخاطر جديدة بظهور التكنولوجيا والتطبيقات الجديدة، ومن الأمثلة المعاصرة على ذلك الذكاء الاصطناعي الذي ينطوي على مخاطر تتعلق بالأمن السيبراني والخصوصية، بالإضافة إلى أنواع أخرى عديدة من المخاطر. وتم إعداد إطار إدارة مخاطر الذكاء الاصطناعي الصادر عن المعهد الوطني للمعايير والتكنولوجيا للمساهمة في التصدي لهذه المخاطر. كما ستسهم جهود مواجهة كل من مخاطر الذكاء الاصطناعي ومخاطر المؤسسات الأخرى (مثل المخاطر المالية، والمخاطر السيبرانية، ومخاطر السمعة، ومخاطر الخصوصية) في الوصول إلى نتائج أكثر تكاملاً وكفاءة مؤسسية. وتُطبّق اعتبارات ونهج إدارة المخاطر السيبرانية والخصوصية على إجراءات تصميم أنظمة الذكاء الاصطناعي وتطويرها ونشرها وتقييمها واستخدامها. وتستخدم نواة إطار عمل إدارة مخاطر الذكاء الاصطناعي الوظائف والتصنيفات الرئيسية والتصنيفات الفرعية لوصف نتائج الذكاء الاصطناعي والمساعدة في إدارة المخاطر المتعلقة به.

الملحق A. نواة إطار عمل الأمن السيبراني

يصف هذا الملحق الوظائف والتصنيفات الرئيسية والتصنيفات الفرعية لنواة إطار عمل الأمن السيبراني. ويوضح الجدول 1 أسماء وظائف وتصنيفات نواة إطار عمل الأمن السيبراني 2.0 التي تحتوي على مُعرف أبجدي خاص بها، ويرتبط مسمى كل وظيفة في الجدول بالجزء الخاص بها من الملحق. لم يتم ترتيب الوظائف والتصنيفات الرئيسية والتصنيفات الفرعية للنواة ترتيبًا أبجديًا، والهدف من ذلك تلبية احتياجات المسؤولين عن تفعيل إدارة المخاطر داخل المؤسسة. كما أن عُمِّد إلى عدم ترقيم التصنيفات الفرعية بالشكل التسلسلي؛ وتشير الفجوات في الترقيم إلى التصنيفات الفرعية لإطار عمل الأمن السيبراني 1.1 التي تم نقلها في الإطار 2.0.

الجدول 1. أسماء وظائف وتصنيفات نواة إطار عمل الأمن السيبراني 2.0 ومُعرفاتها

الوظيفة	التصنيف	المُعرف الخاص بالتصنيف
الحوكمة (GV)	السياق المؤسسي	GV.OC
	استراتيجية إدارة المخاطر	GV.RM
	الأدوار والمسؤوليات والصلاحيات	GV.RR
	السياسة	GV.PO
	الإشراف	GV.OV
	إدارة مخاطر سلسلة الإمداد للأمن السيبراني	GV.SC
التحديد (ID)	إدارة الأصول	ID.AM
	تقييم المخاطر	ID.RA
	التحسين	ID.IM
الحماية (PR)	إدارة الهوية والمصادقة عليها والتحكم في الوصول	PR.AA
	الوعي والتدريب	PR.AT
	أمن البيانات	PR.DS
	أمن المنصات	PR.PS
	مرونة البنية التحتية للتكنولوجيا	PR.IR
الرصد (DE)	المراقبة المستمرة	DE.CM
	تحليل الأحداث السلبية	DE.AE
الاستجابة (RS)	إدارة الحوادث	RS.MA
	تحليل الحوادث	RS.AN
	الاستجابة للحوادث والإبلاغ عنها والتواصل بشأنها	RS.CO
	التخفيف من حدّة الحوادث	RS.MI
الاستعادة (RC)	تنفيذ خطة الاستعادة بعد الحوادث	RC.RP
	نشر خطة الاستعادة بعد الحوادث	RC.CO

تتوفر نواة إطار عمل الأمن السيبراني والمراجع المعرفية وأمثلة التنفيذ على الموقع الإلكتروني لإطار عمل الأمن السيبراني 2.0 ومن خلال الأداة المرجعية لإطار عمل الأمن السيبراني 2.0 التي تتيح للمستخدمين استكشافها وتصديرها بتنسيقات سهلة القراءة للبشر والآلات. كما تتوفر نواة إطار عمل الأمن السيبراني 2.0 بتنسيق قديم مشابه لتنسيق إطار عمل الأمن السيبراني 1.1.

الحوكمة (GV): يتم وضع ونشر ومراقبة استراتيجية إدارة المخاطر السيبرانية للمؤسسة وتوقعاتها وسياساتها

- **السياق المؤسسي (GV.OC):** يتم فهم الظروف - الرسالة وتوقعات أصحاب المصلحة والتبعيات والمتطلبات القانونية والتنظيمية والتعاقدية - المحيطة بقرارات إدارة المخاطر السيبرانية في المؤسسة
  - **GV.OC-01:** يتم إدراك رسالة المؤسسة وتؤثر على إدارة المخاطر السيبرانية
  - **GV.OC-02:** يتم التعرف على أصحاب المصلحة الداخليين والخارجيين، وفهم ودراسة متطلباتهم وتوقعاتهم بشأن إدارة المخاطر السيبرانية
  - **GV.OC-03:** يتم فهم وإدارة المتطلبات القانونية والتنظيمية والتعاقدية المتعلقة بالأمن السيبراني - بما يشمل التزامات الخصوصية والحريات المدنية
  - **GV.OC-04:** يتم إدراك وتعميم الأهداف والقدرات والخدمات الأساسية التي يعتمد عليها أصحاب المصلحة الخارجيون أو يتوقعونها من المؤسسة
  - **GV.OC-05:** يتم إدراك وتعميم النتائج والقدرات والخدمات التي تعتمد عليها المؤسسة
- **استراتيجية إدارة المخاطر (GV.RM):** يتم تحديد أولويات المؤسسة وقيودها وبيانات تحمل المخاطر وتقبلها والافتراضات ذات الصلة وتعميمها واستخدامها لدعم إجراءات اتخاذ القرارات المتعلقة بالمخاطر التشغيلية
  - **GV.RM-01:** يتولى أصحاب المصلحة في المؤسسة مسؤولية تحديد أهداف إدارة المخاطر واعتمادها
  - **GV.RM-02:** يتم إعداد بيانات تحمل المخاطر وتقبلها وتعميمها وحفظها
  - **GV.RM-03:** يتم تضمين أنشطة ونتائج إدارة المخاطر السيبرانية في عمليات إدارة المخاطر المؤسسية
  - **GV.RM-04:** يتم تحديد وتعميم التوجه الاستراتيجي الذي يصف خيارات الاستجابة المناسبة للمخاطر
  - **GV.RM-05:** يتم إنشاء خطوط تواصل بشأن المخاطر السيبرانية في المؤسسة، بما يشمل المخاطر من المورّدين والجهات الخارجية الأخرى
  - **GV.RM-06:** يتم إنشاء طريقة موحّدة لحساب المخاطر السيبرانية المُعمَّمة وتوثيقها وتصنيفها وترتيبها حسب الأولوية والإبلاغ عنها
  - **GV.RM-07:** يتم تحديد الفرص الاستراتيجية (على سبيل المثال: المخاطر الإيجابية) وإدراجها في مناقشات المخاطر السيبرانية التنظيمية
- **الأدوار والمسؤوليات والصلاحيات (GV.RR):** يتم تحديد الأدوار والمسؤوليات والصلاحيات المتعلقة بالأمن السيبراني وتعميمها لتعزيز المساءلة وتقييم الأداء وإجراء التحسين المستمر
  - **GV.RR-01:** تتولى القيادة التنظيمية مهام المسؤولية والمساءلة عن المخاطر السيبرانية ونشر ثقافة أخلاقية تدرك بالمخاطر وتخضع للتحسين المستمر
  - **GV.RR-02:** يتم تحديد الأدوار والمسؤوليات والصلاحيات المتعلقة بإدارة المخاطر السيبرانية، ويتم تعميمها وفهمها وتنفيذها
  - **GV.RR-03:** يتم تخصيص الموارد الكافية بما يتناسب مع استراتيجية المخاطر السيبرانية والأدوار والمسؤوليات والسياسات ذات الصلة
  - **GV.RR-04:** يندرج الأمن السيبراني ضمن ممارسات الموارد البشرية
- **السياسة (GV.PO):** يتم وضع سياسة الأمن السيبراني للمؤسسة وتعميمها وتنفيذها
  - **GV.PO-01:** يتم إعداد سياسة إدارة المخاطر السيبرانية بناءً على السياق التنظيمي واستراتيجية الأمن السيبراني والأولويات ويتم تعميمها وتنفيذها

- **GV.PO-02:** تتم مراجعة سياسة إدارة المخاطر السيبرانية وتحديثها وتعميمها وتنفيذها لتعكس التغييرات في المتطلبات والتهديدات والتكنولوجيا ورسالة المؤسسة

- **الإشراف (GV.OV):** يتم استخدام نتائج أنشطة وأداء إدارة المخاطر السيبرانية على مستوى المؤسسة لتوجيه استراتيجية إدارة المخاطر وتحسينها وتعديلها
  - **GV.OV-01:** يتم مراجعة نتائج استراتيجية إدارة المخاطر السيبرانية لتوجيه الاستراتيجية والتوجه وتعديلهما
  - **GV.OV-02:** تُراجع استراتيجية إدارة المخاطر السيبرانية وتُعدّل لضمان تلبيتها لمتطلبات المؤسسة ومواجهتها لكافة المخاطر.
  - **GV.OV-03:** يُقيّم أداء إدارة المخاطر السيبرانية في المؤسسة ويُراجع لإدخال التعديلات اللازمة.

- **إدارة مخاطر سلسلة الإمداد للأمن السيبراني:** يحدد أصحاب المصلحة في المؤسسة عمليات إدارة مخاطر سلسلة الإمداد للأمن السيبراني، وينشئونها ويديرونها ويراقبونها ويحسنونها.
  - **GV.SC-01:** يتولى أصحاب المصلحة في المؤسسة مسؤولية تحديد واعتماد برنامج إدارة مخاطر سلسلة الإمداد للأمن السيبراني واستراتيجيتها وأهدافها وسياساتها وعملياتها
  - **GV.SC-02:** تُحدد أدوار ومسؤوليات الأمن السيبراني للموردين والعملاء والشركاء، وتُنسّق وتُنشر داخليًا وخارجيًا.
  - **GV.SC-03:** تُدمج إدارة مخاطر سلسلة الإمداد للأمن السيبراني ضمن إدارة الأمن السيبراني، إدارة المخاطر المؤسسية، تقييم المخاطر، وعمليات التحسين.
  - **GV.SC-04:** يتم التعرف على الموردين وترتيبهم حسب الأهمية
  - **GV.SC-05:** تُحدد المتطلبات اللازمة لمواجهة المخاطر السيبرانية في سلاسل الإمداد، تُرتب حسب الأولوية، وتُدمج في العقود والاتفاقيات مع الموردين والجهات الخارجية ذات الصلة.
  - **GV.SC-06:** يتم إجراء عمليات التخطيط وبذل العناية الواجبة لتقليل المخاطر قبل الدخول في علاقات رسمية مع المورّدين أو الجهات الخارجية الأخرى
  - **GV.SC-07:** يتم فهم المخاطر الناتجة عن المورّد ومنتجاته وخدماته والجهات الخارجية الأخرى وتسجيلها وترتيبها حسب الأولوية وتقييمها والاستجابة لها ومراقبتها طول مدة التعامل
  - **GV.SC-08:** يتم تضمين المورّدين ذوي الصلة والجهات الخارجية الأخرى في أنشطة التخطيط للحوادث والاستجابة لها والتعافي بعدها
  - **GV.SC-09:** يتم دمج ممارسات أمن سلسلة الإمداد في برامج الأمن السيبراني وإدارة المخاطر المؤسسية، ويتم مراقبة أدائها طوال دورة حياة المنتج التكنولوجي والخدمة المقدمة
  - **GV.SC-10:** تضم خطط إدارة مخاطر سلسلة الإمداد للأمن السيبراني أحكامًا للأنشطة التي تُجرى بعد إبرام اتفاقيات الشراكة أو الخدمة

التحديد (ID): لقد اتضحت المخاطر السيبرانية الحالية التي تواجهها المؤسسة

- **إدارة الأصول (ID.AM):** يتم تحديد الأصول (مثل البيانات، والأجهزة، والبرمجيات، والأنظمة، والمرافق، والخدمات، والأشخاص) التي تمكّن المؤسسة من تحقيق أهداف أعمالها، وإدارتها بما يتماشى مع أهميتها النسبية لأهداف المؤسسة واستراتيجيتها في إدارة المخاطر.
  - **ID.AM-01:** توفر المؤسسة سجلات جرد محدثة للأجهزة التي تديرها.

- **ID.AM-02:** توفر المؤسسة سجلات جرد محدثة للبرمجيات والخدمات والأنظمة.
- **ID.AM-03:** توفر المؤسسة تمثيلات مثل المخططات أو النماذج للاتصالات الشبكية المصرح بها، بالإضافة إلى تدفقات البيانات الداخلة والخارجة من الشبكة.
- **ID.AM-04:** يتم توفير سجلات جرد للخدمات المقدمة من الموردين.
- **ID.AM-05:** تُحدَّد أولويات الأصول بناءً على تصنيفها، وأهميتها، والموارد المرتبطة بها، ومدى تأثيرها على تحقيق رسالة المؤسسة.
- **ID.AM-07:** يتم توفير سجلات جرد للبيانات وأنواعها المحددة، إضافةً إلى البيانات الوصفية (الميتاداتا) المرتبطة بها.
- **ID.AM-08:** تُدار الأنظمة، والأجهزة، والبرمجيات، والخدمات، والبيانات بشكل منهجي طوال دورة حياتها

- **تقييم المخاطر (ID.RA):** تدرك المؤسسة مخاطر الأمن السيبراني التي قد تؤثر عليها، وعلى أصولها، وعلى الأفراد المرتبطين بها.
  - **ID.RA-01:** يتم تحديد الثغرات في الأصول، والتحقق منها، وتوثيقها.
  - **ID.RA-02:** يتم تلقي معلومات المخاطر السيبرانية من منتديات ومصادر مشاركة المعلومات
  - **ID.RA-03:** يتم تحديد وتوثيق التهديدات الداخلية والخارجية التي تواجه المؤسسة.
  - **ID.RA-04:** تُحدد التأثيرات المحتملة واحتمالية استغلال التهديدات للثغرات، ويتم توثيقها بدقة.
  - **ID.RA-05:** يُستخدم تحليل التهديدات والثغرات، إلى جانب تقييم احتمالية وقوعها وتأثيراتها، لفهم المخاطر الكامنة وتوجيه أولويات الاستجابة لها.
  - **ID.RA-06:** تُختار استجابات المخاطر وتُحدد أولوياتها، ويُخطط لتنفيذها، وتُتابع مراحل التنفيذ، ويُتواصل بشأنها باستمرار.
  - **ID.RA-07:** تتم إدارة التغييرات والاستثناءات من خلال تقييم تأثيرها على المخاطر، وتوثيقها، وتتبعها
  - **ID.RA-08:** يتم تنفيذ عمليات مخصصة لاستقبال وتحليل والرد على الإفصاحات المتعلقة بالثغرات الأمنية.
  - **ID.RA-09:** يتم تقييم صحة وسلامة الأجهزة والبرمجيات قبل اقتنائها واستخدامها.
  - **ID.RA-10:** يتم تقييم الموردين المهمين قبل الشراء أو التعاقد معهم.

- **التحسين (ID.IM):** تُحدد فرص التحسين لعمليات وإجراءات وأنشطة إدارة مخاطر الأمن السيبراني في المؤسسة على مستوى جميع وظائف إطار عمل الأمن السيبراني.
  - **ID.IM-01:** تُحدَّد التحسينات بناءً على نتائج التقييمات.
  - **ID.IM-02:** تُحدَّد التحسينات من خلال اختبارات وأنشطة الأمن السيبراني، بما في ذلك تلك التي تُجرى بالتنسيق مع المورّدين والجهات الخارجية ذات الصلة.
  - **ID.IM-03:** تُحدَّد التحسينات من خلال تنفيذ العمليات والإجراءات والأنشطة التشغيلية
  - **ID.IM-04:** يتم إعداد خطط الاستجابة للحوادث وخطط الأمن السيبراني الأخرى التي تؤثر على العمليات، ويتم تعميمها، وتوفيرها، وتحسينها.

الحماية (PR): تُستخدم تدابير الحماية كوسيلة لإدارة مخاطر الأمن السيبراني ضمن المؤسسة.

- **إدارة الهوية والمصادقة عليها والتحكم في الوصول (PR.AA):** يُقتصر الوصول إلى الأصول المادية والمنطقية على المستخدمين والخدمات والأجهزة المصرح بها فقط، ويتم إدارته بما يتناسب مع مستوى الخطر الخاضع للتقييم الناتج عن الوصول غير المصرح به.
  - **PR.AA-01:** تتولى المؤسسة إدارة هويات وبيانات اعتماد المستخدمين والخدمات والأجهزة المصرح بها.
  - **PR.AA-02:** يتم التحقق من الهويات وربطها ببيانات الاعتماد بناءً على سياق التفاعلات.
  - **PR.AA-03:** يتم إجراء المصادقة للمستخدمين والخدمات والأجهزة.
  - **PR.AA-04:** يتم حماية إثباتات الهوية وتبادلها والتحقق من صحتها
  - **PR.AA-05:** تُحدَّد أذونات الوصول، والحقوق، والتفويضات ضمن سياسة معتمدة، ويتم إدارتها وتطبيقها ومراجعتها، مع الالتزام بمبدأ الحد الأدنى من الامتيازات ومبدأ فصل المهام.
  - **PR.AA-06:** يتم إدارة ومراقبة وتطبيق التحكم في الوصول الفعلي إلى الأصول بما يتناسب مع مستوى المخاطر.

- **التوعية والتدريب (PR.AT):** يتم تزويد موظفي المؤسسة بالتوعية والتدريب في مجال الأمن السيبراني، لتمكينهم من أداء المهام المرتبطة بالأمن السيبراني.
  - **PR.AT-01:** يتم تزويد الموظفين بالتوعية والتدريب اللازمين لاكتساب المعرفة والمهارات التي تمكّنهم من أداء المهام العامة مع مراعاة مخاطر الأمن السيبراني.
  - **PR.AT-02:** يتم تزويد الأفراد في الأدوار المتخصصة بالتوعية والتدريب اللازمين لاكتساب المعرفة والمهارات التي تمكّنهم من أداء المهام ذات الصلة مع مراعاة مخاطر الأمن السيبراني.

- **أمن البيانات (PR.DS):** تُدار البيانات بما يتماشى مع استراتيجية المخاطر الخاصة بالمؤسسة، وذلك لحماية سرية المعلومات وسلامتها وتوافرها.
  - **PR.DS-01:** حماية سرية البيانات المخزنة ومراعاة سلامتها وتوافرها
  - **PR.DS-02:** حماية سرية البيانات أثناء النقل ومراعاة سلامتها وتوافرها
  - **PR.DS-10:** حماية سرية البيانات المُستخدمة ومراعاة سلامتها وتوافرها
  - **PR.DS-11:** يتم إنشاء نسخ احتياطية من البيانات، وحمايتها، وتوفيرها، واختبارها.

- **أمن المنصّة (PR.PS):** يتم إدارة الأجهزة والبرمجيات (مثل البرامج الثابتة وأنظمة التشغيل والتطبيقات) والخدمات على المنصات المادية والافتراضية بما يتماشى مع استراتيجية المخاطر المتبعة لدى المؤسسة، وذلك لحماية سريتها وسلامتها وتوافرها.
  - **PR.PS-01:** يتم إعداد ممارسات إدارة التهيئة وتنفيذها
  - **PR.PS-02:** يتم توفير البرمجيات أو استبدالها أو إزالتها بما يتناسب مع مستوى المخاطر.
  - **PR.PS-03:** يتم توفير الأجهزة أو استبدالها أو إزالتها بما يتناسب مع مستوى المخاطر.
  - **PR.PS-04:** يتم إنشاء سجلات الأحداث وتوفيرها لأغراض المراقبة المستمرة.
  - **PR.PS-05:** يتم منع تثبيت وتشغيل البرمجيات غير المصرح بها.
  - **PR.PS-06:** يتم دمج ممارسات تطوير البرمجيات الآمنة ضمن دورة حياة تطوير البرمجيات، ويتم مراقبة أدائها باستمرار طوال مراحل الدورة.

- **مرونة البنية التحتية للتكنولوجيا (PR.IR):** تُدار البُنى الأمنية بما يتماشى مع استراتيجية المخاطر المتبعة لدى المؤسسة، وذلك لحماية سرية الأصول وسلامتها وتوافرها، وتعزيز قدرة المؤسسة على الصمود.
  - **PR.IR-01:** يتم حماية الشبكات والبيئات من الوصول والاستخدام المنطقي غير المصرح به.
  - **PR.IR-02:** تُحمى الأصول التكنولوجية للمؤسسة من التهديدات البيئية.
  - **PR.IR-03:** تُطبَّق آليات تضمن تحقيق متطلبات القدرة على الصمود في كل من الظروف العادية والظروف المعاكسة
  - **PR.IR-04:** يتم توفير سعة موارد كافية لضمان استمرارية توفر الخدمات.

الرصد (DE): يتم اكتشاف الهجمات السيبرانية المحتملة وحالات الاختراق، ويتم تحليلها.

- **المراقبة المستمرة (DE.CM):** يتم مراقبة الأصول لاكتشاف الحالات الشاذة، ومؤشرات الاختراق، وغيرها من الأحداث السلبية المحتملة.
  - **DE.CM-01:** يتم مراقبة الشبكات وخدماتها للكشف عن الأحداث السلبية المحتملة
  - **DE.CM-02:** يتم مراقبة البيئة المادية للكشف عن الأحداث السلبية المحتملة
  - **DE.CM-03:** يتم مراقبة أنشطة الموظفين واستخدامات التكنولوجيا لاكتشاف الأحداث السلبية المحتملة.
  - **DE.CM-06:** يتم مراقبة أنشطة وخدمات مزوّد الخدمة الخارجي لاكتشاف الأحداث السلبية المحتملة.
  - **DE.CM-09:** تُراقَب مكونات الحوسبة من أجهزة وبرمجيات وبيئات تشغيل وبيانات لرصد الأحداث السلبية المحتملة.
- **تحليل الأحداث السلبية (DE.AE):** تخضع الحالات الشاذة، ومؤشرات الاختراق، وغيرها من الأحداث السلبية المحتملة للتحليل لتوصيف هذه الأحداث والكشف عن الحوادث السيبرانية.
  - **DE.AE-02:** يتم تحليل الأحداث السلبية المحتملة لفهم الأنشطة المرتبطة بها بشكل أفضل.
  - **DE.AE-03:** يتم ربط المعلومات من مصادر متعددة.
  - **DE.AE-04:** يتم فهم الأثر المُقدَّر ونطاق الأحداث السلبية.
  - **DE.AE-06:** يتم تقديم المعلومات المتعلقة بالأحداث السلبية إلى الموظفين والأدوات المصرح لهم بالوصول إليها.
  - **DE.AE-07:** تُدمج معلومات التهديدات السيبرانية والمعلومات السياقية الأخرى ضمن عملية التحليل.
  - **DE.AE-08:** يُعلن عن الحوادث عندما تستوفي الأحداث السلبية المعايير المحددة للحوادث.

الاستجابة (RS): تُتخذ الإجراءات المناسبة بشأن الحادث السيبراني المكتشف.

- **إدارة الحوادث (RS.MA):** تتم إدارة الاستجابات للحوادث السيبرانية المكتشفة.
  - **RS.MA-01:** تُنفذ خطة الاستجابة للحوادث بالتنسيق مع الجهات الخارجية ذات الصلة بمجرد إعلان الحادث.

- **RS.MA-02:** يتم فرز تقارير الحوادث والتحقق من صحتها
- **RS.MA-03:** يتم تصنيف الحوادث وترتيبها حسب الأولوية
- **RS.MA-04:** يتم تصعيد الحوادث أو رفعها إلى الجهات المعنية حسب الحاجة.
- **RS.MA-05:** يتم تطبيق معايير التعافي من الحادث

- **تحليل الحوادث (RS.AN):** تُجرى التحقيقات لضمان استجابة فعّالة ودعم أنشطة التحليل الجنائي والتعافي.
  - **RS.AN-03:** يُجرى التحليل لتحديد ما وقع أثناء الحادث وتحديد السبب الجذري له.
  - **RS.AN-06:** تُسجَّل الإجراءات المتخذة أثناء التحقيق، ويتم الحفاظ على سلامة سجلاتها ومصدرها.
  - **RS.AN-07:** تُجمَع بيانات الحادث والبيانات الوصفية المرتبطة به، ويتم الحفاظ على سلامتها ومصدرها.
  - **RS.AN-08:** يتم تقدير حجم الحادث والتحقق من صحته.

- **الاستجابة للحوادث والإبلاغ عنها والتواصل بشأنها (RS.CO):** يتم تنسيق أنشطة الاستجابة مع الجهات الداخلية والخارجية حسبما تقتضي القوانين واللوائح أو السياسات المعمول بها.
  - **RS.CO-02:** يُخطر أصحاب المصلحة الداخليين والخارجيين بالحوادث
  - **RS.CO-03:** تُشارك المعلومات مع أصحاب المصلحة الداخليين والخارجيين المعنيين

- **التخفيف من حدّة الحوادث (RS.MI):** يُنفذ العديد من الأنشطة لمنع توسع الحوادث والتخفيف من آثارها
  - **RS.MI-01:** يتم احتواء الحوادث
  - **RS.MI-02:** يتم القضاء على الحوادث

الاستعادة (RC): يتم استعادة الأصول والعمليات المتأثرة بحادث الأمن السيبراني

- **تنفيذ خطة الاستعادة بعد الحوادث (RC.RP):** يتم تنفيذ أنشطة الاستعادة لضمان التوافر التشغيلي للأنظمة والخدمات المتضررة من حوادث الأمن السيبراني
  - **RC.RP-01:** يُنفَّذ إجراء الاستعادة الوارد في خطة الاستجابة بمجرد بدء التعامل مع الحادث.
  - **RC.RP-02:** يتم تحديد إجراءات التعافي وتحديد نطاقها وترتيبها حسب الأولوية وتنفيذها
  - **RC.RP-03:** يُتحقق من سلامة النسخ الاحتياطية وأصول الاستعادة الأخرى قبل استخدامها للاستعادة
  - **RC.RP-04:** يتم النظر في وظائف المهمة الحرجة وإدارة مخاطر الأمن السيبراني لإنشاء معايير تشغيلية بعد الحادث
  - **RC.RP-05:** يتم التحقق من سلامة الأصول المستعادة، واستعادة الأنظمة والخدمات، والتأكد من عودة التشغيل إلى الوضع الطبيعي.
  - **RC.RP-06:** يُعلن عن انتهاء استعادة الحادث بناءً على معايير محددة، وتُستكمل الوثائق المتعلقة بالحادث.

- **نشر خطة الاستعادة بعد الحوادث (RC.CO):** تُنسق أنشطة الاستعادة مع الجهات الداخلية والخارجية.

- **RC.CO-03:** يتم إبلاغ أنشطة الاستعادة والتقدم في استعادة القدرات التشغيلية إلى الجهات المعنية المحددة داخل المؤسسة وخارجها.
- **RC.CO-04:** تُشارك التحديثات العامة حول استعادة الحوادث باستخدام الطرق والرسائل المعتمدة.

الملحق **B**. مستويات إطار عمل الأمن السيبراني

يحتوي الجدول رقم 2 على تمثيل تصوري لمستويات إطار عمل الأمن السيبراني التي نوقشت في القسم رقم 3. تصنف المستويات مدى دقة ممارسات حوكمة مخاطر الأمن السيبراني (الحوكمة) وممارسات إدارة مخاطر الأمن السيبراني (التحديد والحماية والرصد والاستجابة والاستعادة) في المؤسسة.

الجدول رقم 2. تمثيل تصوّري لمستويات إطار عمل الأمن السيبراني

المستوى	حوكمة مخاطر الأمن السيبراني	إدارة مخاطر الأمن السيبراني
المستوى الأول: جزئي	تُدار عملية تطبيق استراتيجية مخاطر الأمن السيبراني التنظيمية بطريقة مخصصة. تُحدد الأولويات بطريقة مخصصة وغير مستندة رسميًا إلى الأهداف أو بيئة التهديدات.	هناك وعي محدود بمخاطر الأمن السيبراني على مستوى المؤسسة. تنفذ المؤسسة إدارة مخاطر الأمن السيبراني بشكل غير منتظم وحسب كل حالة على حدة. قد لا تمتلك المؤسسة عمليات تتيح مشاركة معلومات الأمن السيبراني داخلها. في كثير من الأحيان، لا تدرك المؤسسة بشكل كامل حجم مخاطر الأمن السيبراني المرتبطة بمورديها والمنتجات والخدمات التي تحصل عليها وتستخدمها.
المستوى الثاني: الوعي بالمخاطر	تُقرّ الإدارة ممارسات إدارة المخاطر، لكنها قد لا تكون معتمدة كسياسة موحّدة على مستوى المؤسسة. تُحدَّد أولويات أنشطة الأمن السيبراني واحتياجات الحماية مباشرةً استنادًا إلى أهداف المخاطر التنظيمية، وبيئة التهديدات، أو متطلبات الأعمال والمهام.	توجد درجة من الوعي بمخاطر الأمن السيبراني على مستوى المؤسسة، لكن لا يزال غائبًا نهج شامل لإدارتها على نطاق مؤسسي كامل. قد يُدرج الأمن السيبراني ضمن أهداف وبرامج المؤسسة على بعض المستويات، دون أن يشمل ذلك المؤسسة بأكملها. تُقيَّم مخاطر الأمن السيبراني للأصول الداخلية والخارجية، لكن هذا التقييم غالبًا ما يفتقر إلى الانتظام والدورية. تُتداول معلومات الأمن السيبراني داخل المؤسسة بطرق غير رسمية. تُدرك المؤسسة المخاطر السيبرانية المرتبطة بمورديها والمنتجات والخدمات التي تستخدمها، لكنها لا تعتمد استجابات رسمية أو متسقة لمعالجتها.
المستوى الثالث: قابلية التكرار	تُعتمد ممارسات إدارة المخاطر رسميًا في المؤسسة، وتُوثَّق في سياسات واضحة ومحددة. تُحدَّد السياسات والعمليات والإجراءات استنادًا إلى فهم دقيق للمخاطر، وتُطبَّق وفقًا لما هو مخطط، وتُراجع. تُحدَّث ممارسات الأمن السيبراني في المؤسسة بانتظام، استنادًا إلى تطبيق إدارة المخاطر على تغيّرات متطلبات الأعمال والمهام، والتهديدات، والمشهد التكنولوجي.	تتبنّى المؤسسة نهجًا شاملًا لإدارة مخاطر الأمن السيبراني على مستوى جميع وحداتها. تُشارك معلومات الأمن السيبراني بانتظام على مستوى المؤسسة بأكملها. تعتمد المؤسسة أساليب متسقة وفعالة للاستجابة لتغيرات المخاطر. يمتلك الموظفون الكفاءة والمعرفة اللازمة لأداء أدوارهم ومسؤولياتهم بفاعلية. تُجري المؤسسة مراقبة مستمرة ودقيقة لمخاطر الأمن السيبراني المرتبطة بالأصول. يتواصل كبار المسؤولين التنفيذيين، في مجال الأمن السيبراني وخارجه، بشكل منتظم بشأن مخاطر الأمن السيبراني. يحرص المسؤولون التنفيذيون على دمج اعتبارات الأمن السيبراني في جميع خطوط الأعمال داخل المؤسسة. تعتمد استراتيجية المخاطر في المؤسسة على فهم مخاطر الأمن السيبراني المرتبطة بالموردين، والمنتجات، والخدمات التي تقتنيها وتستخدمها. يتعامل الموظفون مع هذه المخاطر بأسلوب رسمي عبر آليات تشمل الاتفاقيات المكتوبة التي تحدد المتطلبات الأساسية، وهياكل الحوكمة مثل مجالس المخاطر، إلى جانب تنفيذ السياسات ومتابعة الالتزام بها. تُنفذ هذه الإجراءات بانتظام وبصورة متسقة وفقًا للخطة، مع مراقبتها ومراجعتها المستمرة لضمان فعاليتها.
المستوى الرابع: التكيف	تعتمد المؤسسة نهجًا شاملًا لإدارة مخاطر الأمن السيبراني، يستند إلى سياسات وعمليات وإجراءات مبنية على فهم دقيق للمخاطر، لمعالجة الأحداث السيبرانية المحتملة.	تُكيّف المؤسسة ممارساتها في مجال الأمن السيبراني استنادًا إلى أنشطتها السابقة والحالية، بما يشمل الدروس المستفادة والمؤشرات التنبؤية. ومن خلال تبني نهج التحسين المستمر، الذي يدمج التقنيات المتقدمة والممارسات الرائدة في مجال الأمن

المستوى	حوكمة مخاطر الأمن السيبراني	إدارة مخاطر الأمن السيبراني
	تُفهم العلاقة بين مخاطر الأمن السيبراني وأهداف المؤسسة بوضوح، وتؤخذ بعين الاعتبار في عملية اتخاذ القرار. يراقب المسؤولون التنفيذيون مخاطر الأمن السيبراني ضمن الإطار ذاته المُستخدم لمراقبة المخاطر المالية وسائر المخاطر المؤسسية الأخرى. تُبنى ميزانية المؤسسة على فهم دقيق لبيئة المخاطر الحالية والمتوقعة، ومستوى تحملها للمخاطر. تُنفّذ وحدات الأعمال رؤية المسؤولين التنفيذيين وتحلل المخاطر على مستوى الأنظمة، بما يتوافق مع حدود تحمل المخاطر المعتمدة في المؤسسة. تشكل إدارة مخاطر الأمن السيبراني جزءًا أصيلًا من ثقافة المؤسسة. وتتطور هذه الإدارة استنادًا إلى الوعي بالتجارب السابقة، والمتابعة المستمرة للأنشطة على أنظمة وشبكات المؤسسة. وتتطور هذه الإدارة بناءً على الوعي بالتجارب السابقة والرصد المستمر للأنشطة على أنظمة وشبكات المؤسسة.	السيبراني، تتمكن المؤسسة من التكيّف بفعالية مع المشهد التكنولوجي المتغير، والاستجابة بسرعة وكفاءة للتهديدات السيبرانية المتطورة والمعقدة. تستخدم المؤسسة معلومات فورية أو شبه فورية لفهم المخاطر السيبرانية المرتبطة بمورديها والمنتجات والخدمات التي تعتمد عليها، وتتخذ إجراءات مستمرة لمعالجتها. تُتبادل معلومات الأمن السيبراني بشكل مستمر داخل المؤسسة ومع الجهات الخارجية المصرح لها.

الملحق C. مسرد المصطلحات

فئة إطارعمل الأمن السيبراني
مجموعة من النتائج المرتبطة بالأمن السيبراني تُشكّل مجتمعة وظيفة متكاملة ضمن إطار عمل الأمن السيبراني.

الملف التعريفي المجتمعي لإطارعمل الأمن السيبراني
خط أساس لمخرجات إطار عمل الأمن السيبراني (CSF) يتم إنشاؤه ونشره لمعالجة المصالح والأهداف المشتركة بين عدد من الجهات. عادةً ما يتم تطوير الملف المجتمعي لقطاع معين، أو قطاع فرعي، أو تكنولوجيا محددة، أو نوع تهديد، أو حالة استخدام أخرى. يمكن للمؤسسة استخدام الملف المجتمعي بوصفه أساسًا لبناء ملفها التعريفي المستهدف (Target Profile).

نواة إطارعمل الأمن السيبراني
تصنيف للمخرجات السيبرانية الشاملة، يمكن أن يساعد أي مؤسسة في إدارة مخاطرها السيبرانية بفعالية. تتكوّن نواة الإطار من تسلسل هرمي يضم الوظائف (Functions)، والتصنيفات (Categories)، والتصنيفات الفرعية (Subcategories)، التي توضح تفاصيل كل مخرج بشكل دقيق.

الملف التعريفي الحالي لإطارعمل الأمن السيبراني
قسم من الملف التنظيمي الذي يحدد المخرجات الأساسية التي تحققها المؤسسة حالياً (أو تحاول تحقيقها)، ويصف كيفية أو مدى تحقيق كل نتيجة.

وظيفة إطارعمل الأمن السيبراني
تحقيق أعلى مستوى من مخرجات الأمن السيبراني. حيث يتألف الإطار من ست وظائف رئيسية: الحوكمة، والتحديد، والحماية، والرصد، والاستجابة، والاستعادة.

مثال على تنفيذ إطارعمل الأمن السيبراني
تمثيل تصوّري موجز وموجّه نحو التنفيذ لأسلوب يساعد في تحقيق أحد مخرجات الإطار الأساسية.

المرجع المعرفي في إطارعمل الأمن السيبراني
رسم توضيحي يوضّح العلاقة بين أحد مخرجات الإطار الأساسي ومعيار قائم أو إرشادات أو لوائح أو محتوى ذي صلة.

الملف التنظيمي في إطارعمل الأمن السيبراني
وسيلة لعرض الوضع السيبراني الحالي أو المستهدف للمؤسسة، وذلك بالاعتماد على مخرجات نواة إطار العمل.

دليل بدء التشغيل السريع لإطارعمل الأمن السيبراني
مصدر إضافي يوفّر إرشادات مختصرة وعملية بشأن مواضيع محددة ذات صلة بالإطار.

الفئة الفرعية في إطارعمل الأمن السيبراني
مجموعة من المخرجات التفصيلية للأنشطة السيبرانية التكنولوجية والإدارية، تُشكّل جزءًا من إحدى فئات الإطار.

ملف التعريف المستهدف في إطارعمل الأمن السيبراني
جزء من ملف التعريف التنظيمي الذي يحدد المخرجات المستهدفة التي اختارتها المؤسسة وأولويتها لتحقيق أهدافها في إدارة مخاطر الأمن السيبراني.

مستوي إطارعمل الأمن السيبراني

مستويات تُستخدم في الملفات التعريفية لتوصيف مدى نضج المؤسسة في حوكمة وإدارة المخاطر السيبرانية. يوجد أربعة مستويات: المستوى الجزئي (المستوى الأول)، ومستوى الوعي بالمخاطر (المستوى الثاني)، ومستوى قابلية التكرار (المستوى الثالث)، ومستوى التكيف (المستوى الرابع)

تم تحديد بعض الأجهزة أو الأدوات أو البرمجيات أو المواد، سواء التجارية أو غير التجارية، في هذه الوثيقة بهدف توضيح الإجراءات التجريبية بشكل كافٍ. ولا يُعتبر هذا التحديد توصية أو تأييدًا من المعهد الوطني للمعايير والتكنولوجيا لأي منتج أو خدمة، كما لا يدل على أن العناصر المذكورة هي بالضرورة أفضل ما هو متاح لهذا الغرض.

سياسات سلسلة المنشورات الفنية للمعهد الوطني للمعاييروالتكنولوجيا
بيانات حقوق النشر والاستخدام والتراخيص
صيغة مُعرّف منشورات السلسلة الفنية للمعهد الوطني للمعايير والتكنولوجيا

كيفية الاستشهاد بهذه النشرة من سلسلة المنشورات الفنية للمعهد الوطني للمعاييروالتكنولوجيا:
المعهد الوطني للمعايير والتكنولوجيا (2024). إطار عمل الأمن السيبراني للمعهد الوطني للمعايير والتكنولوجيا، الإصدار الثاني (المعهد الوطني للمعايير والتكنولوجيا، غايثرسبيرغ، ماريلاند)، ورقة بيضاء للأمن السيبراني صادرة عن المعهد الوطني للمعايير والتكنولوجيا (CSWP) الوثيقة رقم 29 من سلسلة الأوراق البيضاء للأمن السيبراني الصادرة عن المعهد الوطني للمعايير والتكنولوجيا. https://doi.org/10.6028/NIST.CSWP.29

بيانات جهة الاتصال
cyberframework@nist.gov

المعهد الوطني للمعايير والتكنولوجيا
عناية: قسم الأمن السيبراني التطبيقي، مختبر تكنولوجيا المعلومات
100 بورو درايف (الرمز البريدي 2000)، غايثرسبيرغ، ميريلاند 20899-2000