الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

ملحق المنهجية والمواءمة
لضوابط الأمن السيبراني للأنظمة التشغيلية

Operational Technology Cybersecurity Controls Methodology and Mapping Annex (OTCCMM -1: 2022)

إشارة المشاركة: أبيض
تصنيف الوثيقة: عام

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

يستخدم هذا البروتوكول على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

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

برتقالي – مشاركة محدودة

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

أخضر – مشاركة في نفس المجتمع

المستلم يمكنه مشاركة المعلومات مع آخرين في نفس الجهة أو جهة أخرى على علاقة معهم في نفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

قائمة المحتويات

مبادئ تصميم ضوابط الأمن السيبراني للأنظمة التشغيلية ٦
العلاقة بالمعايير الدولية الأخرى ٦
منهجية تصميم ضوابط الامن السيبراني للأنظمة التشغيلية (OTCC-1:2022) ٨
هيكلية المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية ١٠
العلاقة بين المكون الأساسي الخامس للضوابط الأساسية للأمن السيبراني مع ضوابط الأمن السيبراني للأنظمة التشغيلية ١١
تحديد مستويات الضوابط الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية ١٣
ربط المعايير الدولية مع الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022) ١٥

قائمة الجداول التوضيحية

جدول 1 : العلاقة بين المكون الأساسي الخامس للضوابط الأساسية للأمن السيبراني مع ضوابط الأمن السيبراني للأنظمة التشغيلية ١٢

قائمة الأشكال والرسوم التوضيحية

شكل 1 : تداخل نطاق الضوابط الأساسية للأمن السيبراني مع ضوابط الأمن السيبراني للأنظمة التشغيلية ٨
شكل 2 : علاقة المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية مع الضوابط الأساسية للأمن السيبراني ٩
شكل 3 : المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية ١٠
شكل ٤: خطوات تطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية ١٣

مبادئ تصميم ضوابط الأمن السيبراني للأنظمة التشغيلية

طورت ضوابط الأمن السيبراني للأنظمة التشغيلية لتوفّر ضوابط مخصصة للأنظمة التشغيلية وأنظمة التحكم الصناعي (OT/ICS)، حيث تعتبر هذه الضوابط امتدادًا للضوابط الأساسية للأمن السيبراني (ECC-1: 2018). ويجب على الجهات ذات العلاقة الالتزام بالضوابط الأساسية للأمن السيبراني أولًا، ثم الضوابط الإضافية المنصوص عليها في وثيقة ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022)

عند تطوير وثيقة ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022)، فقد تم تطبيق المبادئ التالية:

- أن تكون المتطلبات الأمنية المذكورة بوثيقة ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022) امتدادًا للضوابط الأساسية للأمن السيبراني.
- الاستفادة من الممارسات والتجارب الدولية في مجال الأنظمة التشغيلية وأنظمة التحكم الصناعي.
- مواءمة ضوابط الأمن السيبراني للأنظمة التشغيلية مع المعايير العالمية من أجل السماح للجهات بالاستفادة من الممارسات الدولية.

العلاقة بالمعايير الدولية الأخرى

خلال تطوير ضوابط الأمن السيبراني الخاصة بالأنظمة التشغيلية، تم استخدام عدة معايير دولية ذات علاقة بالأمن السيبراني للأنظمة التشغيلية وأنظمة التحكم الصناعي. وتمثلت المعايير التي استخدمت في تطوير هذه الضوابط فيما يلي:

- سلسلة معايير (ISA/IEC 62443) المتعلقة بأمن أنظمة التحكم والأتمتة الصناعية (IACS)، وتحديداً:
  - وثيقة متطلبات برنامج الأمن لمالكي الأصول (62443-2-1).
  - وثيقة معيار تقييم المخاطر الأمنية لتصميم النظام (62443-3-2).
  - وثيقة متطلبات أمان النظام ومستويات الأمان (62443-3-3).
- إطار عمل الأمن السيبراني الأمريكي (CYBERSECURITY FRAMEWORK "CSF") الصادر من المعهد الوطني للمعايير والتقنية (NIST).
- ضوابط الأمان والخصوصية لأنظمة المعلومات والمنظمات الفيدرالية (NIST SP 800-53)، الصادر من المعهد الوطني للمعايير والتقنية (NIST).
- دليل أمن أنظمة التحكم الصناعي (NIST SP 800-82) الصادر من المعهد الوطني للمعايير والتقنية (NIST).
- المعيار النرويجي لقطاع الغاز والطاقة (NOG 104) للإرشادات المتعلقة بالمتطلبات الأساسية لأمن

المعلومات لضبط عملية التحكم والسلامة ودعم أنظمة تقنية المعلومات والاتصالات.

- معيار حماية البنية التحتية الحساسة الصادر من منظمة الموثوقية الكهربائية لأمريكا الشمالية (NERC CIP).
- إطار النضج الخاص بقدرات الأمن السيبراني الصادر من وزارة الطاقة الأمريكية.

منهجية تصميم ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022)

العلاقة مع الضوابط الأساسية للأمن السيبراني (ECC-1:2018)

تعتبر ضوابط الأمـن السيبراني للأنظمة التشغيلية امـتـدادًا للضوابط الأساسية للأمن السيبراني (ECC-1:2018)، والتي تستهدف الأنظمة التشغيلية وأنظمة التحكم الصناعي الواقعة بالمرافق الصناعية الحساسة. يوضح الشكل 1 أدناه أن تنفيذ هذه الضوابط يبدأ بعد تنفيذ الضوابط الأساسية للأمن السيبراني والالتزام بها.

شكل 1 : تداخل نطاق الضوابط الأساسية للأمن السيبراني مع ضوابط الأمن السيبراني للأنظمة التشغيلية

تم مواءمة المكونات الأساسية والفرعية من الضوابط الأساسية للأمن السيبراني وضوابط الأمن السيبراني للأنظمة التشغيلية في هيكلية مماثلة. حيث يوجد أربع مكونات رئيسية من أصل خمس مكونات رئيسية من الضوابط الأساسية للأمن السيبراني في ضوابط الأمن السيبراني للأنظمة التشغيلية. بالإضافة إلى ذلك، فقد تم إضافة ضوابط خاصة بالأنظمة التشغيلية وأنظمة التحكم الصناعي إلى عشرين مكون فرعي من المكونات الفرعية للضوابط الأساسية للأمن السيبراني (تظهر باللون الرمادي الفاتح في الشكل 2). كما تم إضافة مكون فرعي جديد لوثيقة ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022) (تظهر باللون الأزرق الداكن في الشكل 2). كما تم تعديل مكونين فرعيين لتتوافق مع الأنظمة التشغيلية وأنظمة التحكم الصناعي (OT/ICS) (تظهر باللون الأزرق الفاتح في الشكل 2). وتوجد أربع مكونات فرعية من الضوابط الأساسية للأمن السيبراني لا تحتوي على ضوابط محددة للأنظمة التشغيلية وأنظمة التحكم الصناعي (OT/ICS) (تظهر باللون الرمادي في الشكل 2).

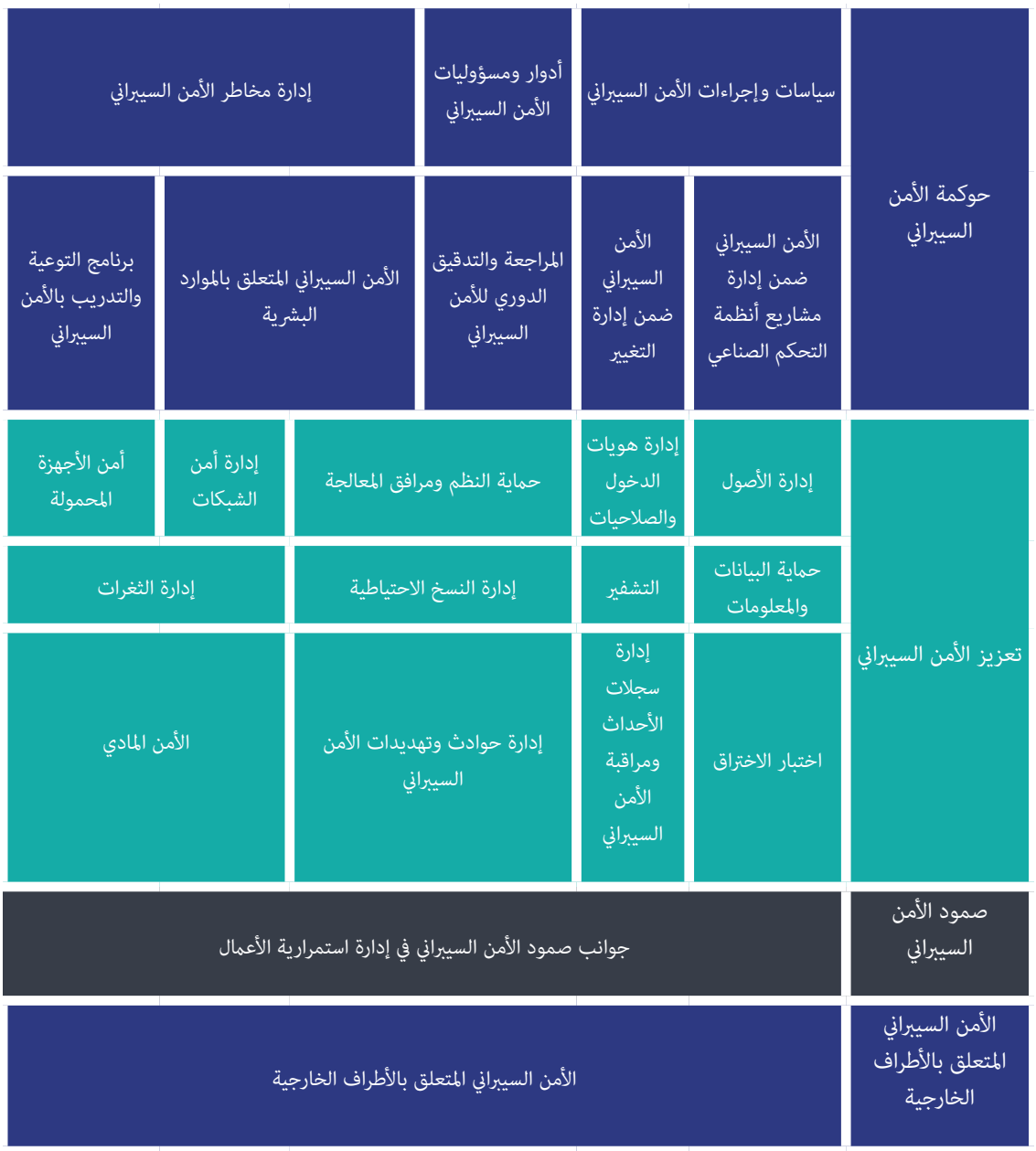
شكل 2 : علاقة المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية مع الضوابط الأساسية للأمن السيبراني

العلاقة مع ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019)

تنطبق ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022) على الأنظمة التشغيلية وأنظمة التحكم الصناعي الموجودة في المرافق الحساسة، على أن الأنظمة الحساسة الأخرى يجب عليها تطبيق ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1:2019) ، أما الأنظمة التشغيلية وأنظمة التحكم الصناعي المتواجدة بالمرافق الحساسة فيتم الإكتفاء في تطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022).

هيكلية المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية

يوضح الشكل 3 هيكلية المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية



شكل 3 : المكونات الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية

العلاقة بين المكون الأساسي الخامس للضوابط الأساسية للأمن السيبراني مع ضوابط الأمن السيبراني للأنظمة التشغيلية

يحتوي المكون الأساسي الخامس من الضوابط الأساسية للأمن السيبراني "حماية أنظمة التحكم الصناعي" على ضوابط عامة لتعزيز حماية بيئة الأنظمة التشغيلية وأنظمة التحكم الصناعي. كما أن ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1: 2022) تحدد ضوابط تفصيلية لحماية الأنظمة التشغيلية وأنظمة التحكم الصناعي.

الجدول التالي (جدول 1) يوضح علاقة متطلبات الأمن السيبراني الواردة في المكون الأساسي الخامس من الضوابط الأساسية للأمن السيبراني مع ضوابط الأمن السيبراني للأنظمة التشغيلية.

رقم الضابط (الضوابط الأساسية)	بنود الضابط	الضوابط ذات العلاقة
٥-١-١	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي للجهة (OT/ICS).	١-١-١
٥-١-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي للجهة (OT/ICS).	١-١-١
٥-١-٣	بالإضافة إلى ما يمكن تطبيقه من الضوابط ضمن المكونات الأساسية رقم (١) و (٢) و (٣) و (٤) لحماية بيانات الجهة وخدماتها، فإن متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) يجب أن تغطي بحد أدنى ما يلي:	-
٥-١-٣-١	التقييد الحازم والتقسيم المادي والمنطقي عند ربط شبكات الإنتاج الصناعية (OT/ICS) مع الشبكات الأخرى التابعة للجهة، مثل: شبكة العمال الداخلية للجهة "Corporate Network".	٢-٤-١-١ ، ٢-٤-١-٢ ، ٢-٤-١-٣، ٢-٤-١-٦ ٢-٤-١-٩ ، ٢-٤-١-١٠ ، ٢-٤-١-١١ ٢-٤-١-١٢ ، ٢-٤-١-١٣
٥-١-٣-٢	التقييد الحازم والتقسيم المادي والمنطقي عند ربط الأنظمة أو الشبكات الصناعية مع شبكات خارجية، مثل: الإنترنت أو الدخول عن بعد أو الاتصال اللاسلكي.	٢-٤-١-٤ ، ٢-٤-١-٥ ٢-٤-١-٧ ، ٢-٤-١-٨
٥-١-٣-٣	تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني للشبكة الصناعية والاتصالات المرتبطة بها ما أمكن ذلك، والمراقبة المستمرة لها.	٢-١١-١، ٢-١١-٣

٥-١-٣-٤	عزل أنظمة معدات السلامة (Safety Instrumented Systems ‹SIS›)	٢-٤-١-٣
٥-١-٣-٥	التقييد الحازم لاستخدام وسائط التخزين الخارجية.	٢-٣-١-٨ ، ٢-٣-١-٩
٥-١-٣-٦	التقييد الحازم لتوصيل الأجهزة المحمولة على شبكة الإنتاج الصناعية.	٢-٥-١-١، ٢-٥-١-٢، ٢-٥-١-٣ ٢-٥-١-٤ ، ٢-٥-١-٥
٥-١-٣-٧	مراجعة إعدادات وتحصين الأنظمة الصناعية، وأنظمة الدعم والأجهزة الآلية الصناعية (Secure Confguration and Hardening) دورياً.	٢-٣-١-١ ، ٢-٣-١-٢ ، ٢-٣-١-٣، ٢-٣-١-٥ ، ٢-٣-١-٧، ٢-٤-١-١٥
٥-١-٣-٨	إدارة ثغرات الأنظمة الصناعية (OT/ICS Vulnerability Management).	٢-٩-١-١، ٢-٩-١-٢، ٢-٩-١-٣
٥-١-٣-٩	إدارة حزم التحديثات والصلاحيات الأمنية للأنظمة (OT/ICS Patch Management).	٢-٣-١-٣ ، ٢-٥-١-٢
٥-١-٣-١٠	إدارة البرامج الخاصة بالأمن السيبراني الصناعي للحماية من الفيروسات والبرمجيات المشبوهة والضارة.	٢-٢-١-٢، ٢-٣-١-١، ٢-٣-١-٦، ٢-١١-١-٥
٥-١-٤	يجب مراجعة متطلبات الأمن السيبراني لحماية أجهزة وأنظمة التحكم الصناعي (OT/ICS) للجهة دورياً.	١-١-٣ ، ١-٤-٢ ، ١-٥-٤ ، ١-٧-٢، ٢-١-٢ ، ٢-٢-٢ ، ٢-٣-٢ ، ٢-٤-٢، ٢-٥-٢، ٢-٦-٢، ٢-٧-٢، ٢-٨-٢، ٢-٩-٢، ٢-١٠-٢ ، ٢-١١-٢، ٢-١٢-٢ ، ٢-١٣-٢، ٣-١-٢ ، ٤-١-٢

جدول 1 : العلاقة بين المكون الأساسي الخامس للضوابط الأساسية للأمن السيبراني مع ضوابط الأمن السيبراني للأنظمة التشغيلية

تحديد مستويات الضوابط الأساسية والفرعية لضوابط الأمن السيبراني للأنظمة التشغيلية

نظرة عامة

يقدم هذا القسم إجراءات شاملة حول كيفية قيام الجهات بتحديد المستويات المناسبة للمرافق الحساسة المختلفة والتي تحتوي على أنظمة تشغيلية وأنظمة تحكم صناعي (OT/ICS). حيث يتم تحديد المستوى المناسب للمرافق بناءً على عدة معايير يتم مراعاتها لكي يتم التأكد من تحديد الضوابط المناسبة لكل مستوى.

منهجية تحديد المستويات

تتكون هذه المنهجية من خطوتين رئيسيتين:

- تحديد مستوى حساسية المرافق بناءً على نتائج أداة حصر وتحديد مستوى المرفق (OTCC-1:2022 FACILITY LEVEL IDENTIFICATION TOOL)
- تحديد الضوابط المناسبة لكل مرفق بناءً على حساسية الأنظمة التشغيلية والصناعية داخل المرفق.

شكل 4 : خطوات تطبيق ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022)

تحديد مستوى حساسية المرافق

هناك ثلاثة مستويات محددة في ضوابط الأمن السيبراني للأنظمة التشغيلية والتي تعتمد على درجة الأهمية والنتائج والآثار المحتملة على المرافق أو الأجهزة أو الأصول المختلفة والمتعلقة بالأجهزة والأنظمة التشغيلية و أنظمة التحكم الصناعي (OT/ICS). وذلك لكي يسمح للجهات بتكييف ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022) بشكل مناسب بناءً على حساسية الأنظمة التشغيلية والصناعية الخاصة بها.

- **المستوى الأول (م1):** مرافق ذات حساسية عالية على الأصول، والبيئة التشغيلية، لدى الجهة من

حيث الصحة، والسلامة، والبيئة.

- **المستوى الثاني (م2):** مرافق ذات حساسية متوسطة على الأصول، والبيئة التشغيلية، لدى الجهة من حيث الصحة، والسلامة، والبيئة.
- **المستوى الثالث (م3):** مرافق ذات حساسية منخفضة على الأصول، والبيئة التشغيلية، لدى الجهة من حيث الصحة، والسلامة، والبيئة.

في هذه المرحلة، تستخدم الجهة أداة (OTCC-1:2022 FACILITY LEVEL IDENTIFICATION TOOL) لتنظيم عملية الحصر وتحديد مستويات المرافق الحساسة والتي تحتوي على أنظمة تشغيلية وأنظمة التحكم الصناعي. تعتمد أداة حصر وتحديد مستوى المرفق على المعايير التالية:

1. التأثير السلبي على المتواجدين داخل و/أو خارج المرفق.
2. التأثير البيئي السلبي داخل و/أو خارج المرفق.
3. التأثير السلبي على الأمن الوطني.
4. التأثير السلبي على سمعة المملكة وصورتها العامة.
5. الكشف غير المصرح به عن البيانات المصنفة على أنها "سرّية للغاية" أو "سرّية".
6. إخلال بالإقتصاد الوطني.
7. التأثير السلبي على أعداد كبيرة من المستفيدين.
8. اعتمادية البنية التحتية الوطنية على المرفق.
9. اعتمادية المرفق على المرافق الأخرى.

في حال أمتلكت الجهة أنظمة تحكم صناعي ذات مستويات مختلفة في نفس المرفق، فيتم تحديد مستوى المرفق بناءً على مستوى النظام الأعلى حساسية.

تحديد الضوابط المناسبة

بمجرد أن تحدد الجهة مستوى حساسية المرفق بناءً على المعايير المحددة أعلاه، فإنه يجب عليها الإلتزام بالضوابط التي يجب تطبيقها بناءً على مستوى حساسية كل مرفق. فعندما يكون لدى الجهة عدد من المرافق الحساسة المختلفة والمنفصلة والمعزولة والتي تحتوي على أنظمة التحكم الصناعي (OT/ICS) فستختلف المستويات تباعاً لذلك وبالتالي ستختلف قابلية تطبيق الضوابط على مرافق الجهة.

يرتبط كل ضابط أساسي أو فرعي من ضوابط الأمن السيبراني للأنظمة التشغيلية بمستوى معين. لذلك، سيحدد كل مستوى يتم تعيينه للمرافق، مجموعة من الضوابط التي يجب تطبيقها لتحقيق الالتزام بوثيقة ضوابط الأمن السيبراني للأنظمة التشغيلية. يتعين على الجهات التي لديها مرافق مصنفة على أنها (م1) تنفيذ جميع الضوابط الأساسية والفرعية المذكورة في وثيقة ضوابط الأمن السيبراني للأنظمة التشغيلية على تلك المرافق. ويتعين على الجهات التي لديها مرافق مصنفة على أنها (م2) تنفيذ ضوابط المستوى الثاني والثالث على تلك المرافق. بالنسبة للجهات التي لديها مرافق مصنفة على أنها (م3) فإنها مطالبة بتنفيذ ضوابط المستوى الثالث كحد أدنى. في حال عدم تطلب تطبيق ضابط رئيسي أو فرعي بناء على مستوى المرفق، تشجع الهيئة الجهة على تطبيق ذلك الضابط.

ربط المعايير الدولية مع ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022)

في حال وجود تعارض بين ضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022) والتشريعات الوطنية والعالمية الأخرى المشار إليها في هذه الوثيقة، فيجب أن تكون الأولوية لضوابط الأمن السيبراني للأنظمة التشغيلية (OTCC-1:2022).

١ حوكمة الأمن السيبراني

١-١	سياسات وإجراءات الأمن السيبراني							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
١-١-١	ORG 1.1, ORG 2.4	ZCR 6.1	-	ID.GV-1, ID.GV-2	PL-2	ISBR 8	003-R1, 003-R2	CPM-1, CPM-2c, CPM-2e, CPM-3b
١-١-٢	CM 1.2	-	SR 7.6	PR.IP-3	CM-3, MA-1, SA-10	ISBR 6	002-R1, 002-R2, 003-R1, 003-R2	ACM-1c, ACM-2a,
١-١-٣	ORG 1.6, ORG 2 (all)	ZCR 5.1, ZCR 6.6, ZCR 4.1, ZCR 7.1, ZCR 6.8	-	ID.GV-4, ID.RA-5, ID.BE (All), ID-GV-4, ID.RA-4	SA-11 (2), RA-3, PM-11, PL-2, PM-9	ISBR 13, ISBR 1, ISBR 2	002-R1, 002-R2, 003-R1, 003-R2	ISC-1 (all), CPM-2g RM-3e

١-٢	أدوار ومسؤوليات الأمن السيبراني							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
١-٢-١								
١-١-٢-١	ORG 1.3, ORG 1.5	-	-	ID.AM-6, ID.GV-2, PR.AT-4	PS-1, PM-1, PM-2	ISBR 1, ISBR 3	002-R2, 003-R1, 003-R3, 003-R4	WM-1d, WM-1c
١-١-٢-٢	ORG 1.3, ORG 1.5	-	-	ID.AM-6, ID.GV-2, PR.AT-4	PS-1, PM-1, PM-2	ISBR 1, ISBR 3	002-R2, 003-R1, 003-R3, 003-R4	WM-1d, WM-1c

١-٣	إدارة مخاطر الأمن السيبراني							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1

١-٣-١								
١-١-٣-١	ORG 2.1	ZCR 3.3, ZCR 5.3, ZCR 7.1	-	ID.RM-1, ,ID.RM-3	RA-1, PM-1	ISBR 2	-	RM-3e
٢-١-٣-١	ORG 2.1, ORG 2.4, AVAIL 1.2, AVAIL 1.2, NET 1.5	ZCR 5.1, ZCR 5.3, ZCR 5.4, ZCR 5.5, ZCR 5.7, ZCR 5.10, ZCR 5.11, ZCR 5.13, ZCR 6.1, ZCR 6.6	-	ID.RA-4	RA-3, SA-11 (2), SA-15 (4), PM-16,	ISBR 5	002-R1, 008-R1	TVM-1d, TVM-1g, RM-2e, RM-1c
٣-١-٣-١	ORG 2.1	ZCR 5.13	-	ID.RA-6	RA-3	ISBR 2	-	-
٤-١-٣-١	ORG 2.1	ZCR 5.13	-	ID.GV-4	-	-	-	RM-2a, RM-1c
٥-١-٣-١	COMP 3.5	-	-	PR.IP-3	-	ISBR 10	003-R1, 003-R2, 010-R1, 010-R2	COMP 3.5
٦-١-٣-١	-	-	-	-	PL-8, PL-2	ISBR 6	-	CPM-3b,
٧-١-٣-١	-	-	-	-	PL-8, PL-2	ISBR 6	-	CPM-3b,
٤-١	**الأمن السيبراني ضمن إدارة مشاريع أنظمة التحكم الصناعي**							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
١-٤-١								
١-١-٤-١	ORG 2.3, ORG 1.6	-	SR 3.3	ID.SC-4	CA-1, CM-4 (2) SA-1, SA-3, SA-4, SA-8, SA-11, SA-12	ISBR 8	-	CPM-4b
٢-١-٤-١	ORG 2.3, ORG 1.6	-	SR 7.6	-	-	ISBR 12	-	CPM-4b
٣-١-٤-١	-	-	-	PR.IP-9	CP-2 CP-3	-	-	-
٤-١-٤-١	-	-	-	ID.GV-4	PM-7	-	-	-
٢-٤-١	ORG 2.4	-	-	-	CM-7 (1)	ISBR 8	-	-
٥-١	**الأمن السيبراني ضمن إدارة التغيير**							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
١-٥-١	CM 1.4	-	-	PR.IP-3	CM-3	ISBR 10	003-R1, 003-R2	ACM-4a
٢-٥-١	CM 1.4	-	-	PR.IP-3	CM-3	ISBR 10	003-R1, 003-R2	ACM (all)
٣-٥-١								

١-٣-٥-١	CM 1.4	-	-	PR.IP-3	CM-4	ISBR 10	003-R1, 003-R2, 010-R1, 010-R2	ACM-3a
٢-٣-٥-١	CM 1.4	-	-	PR.IP-3	CM-3(2)	ISBR 10	003-R1, 003-R2, 010-R1, 010-R2	ACM-4d
٣-٣-٥-١	CM 1.4	-	-	PR.IP-3	IR-4 (2)	ISBR 10	003-R1, 003-R2, 010-R1, 010-R2	-
٤-٣-٥-١	CM 1.4	-	-	PR.IP-3	IR-4 (2)	ISBR 10	003-R1, 003-R2, 010-R1, 010-R2	-
٥-٣-٥-١	CM 1.4	-	SR 7.6 RE(1)	PR.IP-3	CM-2(2)	ISBR 10	010-R1, 010-R2	ACM-2d
٤-٥-١	CM 1.4, ORG 2.4	-	-	PR.IP-3	CM-3	ISBR 10	003-R1, 003-R2, 010-R1, 010-R2	ACM-4g
٦-١	**المراجعة والتدقيق الدوري للأمن السيبراني**							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
١-٦-١	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	-	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12	PR.PT-1	AU*	-	-	-
٢-٦-١	3.1.18	-	-	PR.PT-1	AU*	-	-	-
٧-١	**الأمن السيبراني المتعلق بالموارد البشرية**							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
١-٧-١	USER 1.2, USER 1.4	-	-	-	PS-3	-	004-R3, 004-R4, 004-R5	WM-2a, WM-2c
٢-٧-١	-	-	-	PR.IP-11	PS-1	-	-	-
٨-١	**برنامج التوعية والتدريب بالأمن السيبراني**							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
١-٨-١	ORG 1.4	-	-	PR.AT-1, PR.AT-2, PR.AT-5	PR.AT-1	ISBR 5	004-R1, 004-R2	WM-3a, WM-3d
٢-٨-١								
١-٢-٨-١	ORG 1.5	-	-	PR.AT-2, PR.AT-5	PR-AT-3	ISBR 5	004-R1, 004-R2	WM-3i
٢-٢-٨-١	ORG 1.5	-	-	PR.AT-2, PR.AT-5	PR-AT-3	ISBR 5	004-R1, 004-R2	WM-3i

٢-١	إدارة الأصول							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
٢-١-١								
٢-١-١-١	CM 1.1	-	SR 1.2	ID.AM-1	CM-8	ISBR 17	002-R1, 002-R2, 003-R1, 003-R2	-
٢-١-١-٢	CM 1.1	-	SR 1.2	ID.AM-1	CM-8	ISBR 17	002-R1, 002-R2, 003-R1, 003-R2	-
٢-١-١-٣	AVAIL 2.4, USER 1.5	-	SR 2.1 RE(1), SR 7.7	PR.AC-4	CP-9 (3), CM-8 (7)	ISBR 17	002-R2, 003-R1, 003-R2	-
٢-١-١-٤	ORG 1.3	-	SR 2.1	ID.GV-2	CM-9 (1)	ISBR 3	002-R2	-
٢-١-١-٥	CM 1.1	-	SR 1.2	ID.AM-1	CM-8	ISBR 17	002-R1, 002-R2, 003-R1, 003-R2	-
٢-١-٢	CM 1.1	-	SR 1.2	ID.AM-1	CM-8	ISBR 17	002-R1, 002-R2, 003-R1, 003-R2	-

٢-٢	إدارة هويات الدخول والصلاحيات							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
2-2-1								
٢-٢-١-١	-	-	SR 1.1, SR 2.1	-	-	-	007-R5	-
٢-٢-١-٢	USER 1.2	-	SR 1.2	PR.AC-7	AC-2 (1)	ISBR 19	007-R5	IAM-1a
٢-٢-١-٣	USER 1.2	-	SR 1.2	PR.AC-1	AC-2 (2)	ISBR 19	007-R5	IAM-1c
٢-٢-١-٤	USER 1.16	-	SR 2.5, SR 2.6	-	AC-11, AC-12, SI-14	-	003-R1, 005-R1, 005-R2	-
٢-٢-١-٥	-	-	-	-	AC-2 (1)	ISBR 19	-	-
٢-٢-١-٦	USER 2.3, USER 2.4	-	SR 2.1 RE(3), SR 2.1 RE(4)	-	AC-3 (2)	ISBR 19	007-R5	-
٢-٢-١-٧	NET 1.1	ZCR 2.1, 3.1, 4.1	SR 5.2	PR.AC-3	SC-1, SC-7	ISBR 4	005-R2	CPM-3 (all)
٢-٢-١-٨	USER 1.2	-	SR 1.4	PR.AC-1	IA-5	-	007-R5	IAM-1a
٢-٢-١-٩	DATA 1.2	-	SR 1.7	PR.DS-1, PR.DS-2	AC-21	-	011-R1, 011-R2	-
٢-٢-١-١٠	-	-	SR 4.1 RE(1)	PR.AC-1	-	ISBR 19	007-R5, 010-R1	IAM-1d

٢-١-٢-١١	USER 1.2	-	-	PR.AC-1	AC-2 (2)	ISBR 19	007-R5	IAM-1c
٢-٢-٢	USER 1.2	-	SR 1.2	R.AC-1	-	-	-	-
٢-٣	**حماية النظم ومرافق المعالجة**							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
٢-٣-١								
٢-٣-١-١	COMP 1.1, COMP 2.2	-	SR 3.2, SR 5.2	DE.CM-4	SI-3	ISBR 13	007-R3, 007-R4, 010-R1, 010-R2	SA-2b, SA-2e, SA-2j
٢-٣-١-٢	COMP 1.1, USER 1.5, COMP 3	-	-	PR.PT-3	CM-6, CM-7	ISBR 6	007-R2	TVM-2c
٢-٣-١-٣	COMP 1.1, USER 1.5, COMP 3	-	-	PR.PT-3	CM-6, CM-7	ISBR 6	007-R2	TVM-2c
٢-٣-١-٤	-	-	SR 7.7	PR.IP-1	CM-7	-	-	-
٢-٣-١-٥	DATA 1.3	-	SR 5.2 RE(3)	-	AU-5 (4), CP-12	-	010-R1, 010-R2	-
٢-٣-١-٦	-	-	SR 7.7 SR 3.2	PR.IP-1	CM-7	-	-	-
٢-٣-١-٧	NET 1.3, COMP 1.1, COMP 3.3, EVENT 1.1, EVENT 1.5	ZCR 3.1, ZCR 3.3	SR 5.1 RE(3), SR 2.1 RE(1)	PR.IP-3, PR.AC-4	SA-17 (7)	ISBR 6	005-R1, 010-R1, 010-R2	SA-4a, IAM-2d,
٢-٣-١-٨	COMP 1.2, COMP 2.1	-	SR 3.2 RE(1)	PR.PT-2, DE.CM-4	MA-3 (2), MP (all)	ISBR 13	004-R2, 007-R1, 007-R3, 007-R4, 010-R4	IAM-1a, IAM-2a
٢-٣-١-٩	COMP 1.2, COMP 2.1	-	SR 3.2 RE(1)	PR.PT-2, DE.CM-4	MA-3 (2), MP (all)	ISBR 13	004-R2, 007-R1, 007-R3, 007-R4, 010-R4	IAM-1a, IAM-2a
٢-٣-١-١٠	-	-	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12	PR.PT-1	AU-1*	-	001-R4 002-R4 003-R4	-
٢-٣-٢-١١	ORG 2.2	-	SR 2.8	DE.CM-4	CA-7	ISBR 13	007-R4	SA-2d
٢-٣-٢-١٢	ORG 2.2	-	SR 2.8	DE.AE-7	CA-7	ISBR 13	007-R4	SA-2b
٢-٣-٢-١٣	EVENT 1.7	-	SR 2.8 RE(1)	DE.AE-3	AU-6 (4)	ISBR 2	007-R4	SA-1c, SA-1e
٢-٣-٢	COMP 1.1, COMP 2.2	-	SR 3.2, SR 5.2	DE.CM-4	SI-3	ISBR 13	007-R3, 007-R4, 010-R1, 010-R2	SA-2b, SA-2e, SA-2j
٢-٤	**إدارة أمن الشبكات**							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1

								٢-٤-١
SA-2b, SA-2e, SA-2j	005-R1, 006-R1	ISBR 4	AC-17, SC-7	PR.AC-5, PR.PT-4	SR 5.1 (all), SR 5.2 (all)	-	NET 1.1	٢-٤-١-١
CPM-3 (all)	005-R1, 006-R1	ISBR 4	SC-7	PR.AC-5, PR.PT-4	SR 5.1 (all), SR 5.2 (all)	ZCR 3.2	NET 1.1, NET 1.3	٢-٤-١-٢
CPM-3 (all)	002-R1, 005-R1, 006-R1	ISBR 4	SC-7	PR.AC-5, PR.PT-4	SR 5.1 (all), SR 5.2 (all)	ZCR 3.3	NET 1.3	٢-٤-١-٣
CPM-3 (all)	-	ISBR 4	AC-18 (all), SI-4 (14)	PR.AC-5, PR.PT-4	SR 5.1 (all), SR 5.2 (all)	ZCR 3.5	NET 2 (ALL)	٢-٤-١-٤
CPM-3 (all)	-	ISBR 4	AC-18 (all)	PR.AC-5, PR.PT-4	SR 1.6, SR 5.1 (all), SR 5.2 (all)	ZCR 3.5	NET 2.2, NET 1.6	٢-٤-١-٥
CPM-3 (all)	005-R1, 007-R1	ISBR 4	MA-4 (4), SC-7 (5)	PR.AC-5	SR 1.6, SR 5.1 (all), SR 5.2 (all)	ZCR 3.6	NET 1.7	٢-٤-١-٦
CPM-3 (all)	003-R1, 005-R1, 005-R2	-	AC-11, AC-12, SI-14	-	SR 2.5, SR 2.6	-	USER 1.16	٢-٤-١-٧
-	005-R1	ISBR 4	MA-4 (4), SC-7	PR.AC-3, PR.AC-5, PR.PT-4	SR 5.1 (all), SR 5.2 (all)	-	NET 3 (ALL)	٢-٤-١-٨
CPM-3 (all)	005-R2	ISBR 4	MA-4 (4), SC-7, SC-7 (8)	PR.AC-3, PR.AC-5, PR.PT-4	SR 1.6, SR 5.1 (all), SR 5.2 (all)	ZCR 3.2	NET 3 (ALL)	٢-٤-١-٩
CPM-3 (all)	005-R2	ISBR 4	MA-4 (4), SC-7, SC-7 (8)	PR.AC-3, PR.AC-5, PR.PT-4	SR 1.6, SR 5.1 (all), SR 5.2 (all)	ZCR 3.2	NET 3 (ALL)	٢-٤-١-١٠
CPM-3 (all)	005-R2	ISBR 4	MA-4 (4), SC-7, SC-7 (8)	PR.AC-3, PR.AC-5, PR.PT-4	SR 1.6, SR 5.1 (all), SR 5.2 (all)	ZCR 3.2	NET 3 (ALL)	٢-٤-١-١١
CPM-3 (all)	005-R2	ISBR 4	MA-4 (4), SC-7, SC-7 (8)	PR.AC-3, PR.AC-5, PR.PT-4	SR 1.6, SR 5.1 (all), SR 5.2 (all)	ZCR 3.2	NET 3 (ALL)	٢-٤-١-١٢
CPM-3 (all)	005-R1	ISBR 4	MA-4 (4), SC-7	PR.AC-3, PR.AC-5, PR.PT-4	SR 5.1 (all), SR 5.2 (all)	-	NET 3 (ALL)	٢-٤-١-١٣
CPM-3 (all)	005-R1	ISBR 4	MA-4 (4), SC-7	PR.AC-3, PR.AC-5, PR.PT-4	SR 5.1 (all), SR (5.2 (all	-	NET 3 (ALL)	٢-٤-١-١٤
CPM-3 (all)	005-R1	ISBR 11	CA-9, SI-4, CA-3	ID.AM-3, DE.AE-1	-	ZCR 6.3	NET 1.2	٢-٤-١-١٥
CPM-3 (all)	005-R1	ISBR 11	CA-9, SI-4, CA-3	ID.AM-3, DE.AE-1	-	ZCR 6.3	NET 1.2	٢-٤-١-١٦
CPM-3 (all)	005-R1, 006-R1	ISBR 4	AC-17, SC-7	PR.AC-5, PR.PT-4	SR 5.1 (all), SR 5.2 (all)	-	NET 1.1	٢-٤-٢
							أمن الأجهزة المحمولة	٢-٥

رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
٢-٥-١								
٢-٥-١-١	-	-	SR 2.3	PR.AC-7	ISBR 6	ISBR 4	007-R3, 007-R4, 010-R3, 010-R4	-
٢-٥-١-٢	NET 2 (all), NET 1.7, NET 1.8 COMP 1.2, COMP 2.1	-	SR 2.3 (all), SR 2.2, SR 2.2 RE(1)	PR.AC-7, ,DE.CM-7	ISBR 6	ISBR 6 ISBR 13	007-R3, 007-R4, 010-R3, 010-R5 010-R6	-
٢-٥-١-٣	-	-	SR 2.3	PR.AC-3	AC-19	ISBR 6	-	-
٢-٥-١-٤	-	-	SR 2.3	-	AC-19	ISBR 6	-	-
٢-٥-١-٥	-	-	SR 4.2	-	AC-19	ISBR 6	-	-
٢-٥-٢	NET 2 (all), NET 1.7, NET 1.8 COMP 1.2, COMP 2.1	-	SR 2.3	PR.AC-7	AC-19	ISBR 6	007-R3, 007-R4, 010-R3, 010-R4	-

٢-٦ حماية البيانات والمعلومات

رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
٢-٦-١								
٢-٦-١-١	DATA 1.2	-	SR 4.1 RE(1)	PR.DS-1, PR.DS-2	AC-21	-	011-R1, 011-R2	-
٢-٦-١-٢	-	-	SR 3.4 SR 4.1	PR.DS-1, PR.DS-2	-	-	-	-
٢-٦-١-٣	DATA 1.6	-	SR 4.2 (all)	ID.GV-4	MP-6	-	011-R1, 011-R2	-
٢-٦-١-٤	,4.3.3.3.9 4.3.4.4.1	-	SR 4.2	PR.DS-7 PR.DS-3	CM-8, MP-6, PE-16 CM-2	-	-	-
٢-٦-٢	DATA 1.2	-	SR 4.1 , 4.2	PR.DS-1, PR.DS-2	AC-21	-	011-R1, 011-R2	-

٢-٧ التشفير

رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
٢-٧-١	DATA 1.7	-	SR 3.1 (all), SR 4.1 (all), SR 4.3	PR.DS-1, PR.DS-2	SC-13	-	-	-
٢-٧-٢	DATA 1.7	-	SR 3.1 (all), SR 4.1 (all), SR 4.3	PR.DS-1, PR.DS-2	SC-13	-	-	-

٢-٨ إدارة النسخ الاحتياطية

رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
٢-٨-١								
٢-٨-١								
٢-٨-١-١	AVAIL 2.4	-	-	PR.IP-4	CP-9 (3)	ISBR 15	009-R1	-
٢-٨-١-٢	AVAIL 2.1	-	SR 7.3	PR.IP-4	CP-9	ISBR 17	009-R1	-
٢-٨-١-٣	AVAIL 2.1	-	SR 7.3	PR.IP-4	CP-9	ISBR 17	009-R1	-
٢-٨-١-٤	AVAIL 2.1	-	SR 7.3	PR.IP-4	CP-6	-	009-R1	-
٢-٨-٢	AVAIL 2.4	-	-	PR.IP-4	CP-9 (3)	ISBR 15	009-R1	-
٢-٩	**إدارة الثغرات**							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
٢-٩-١								
٢-٩-١-١	ORG 2.2, EVENT 1.9	ZCR 5.13	-	ID.RA-1, PR.IP-12	RA-3, RA-5	ISBR 6, ISBR 10, ISBR 12	010-R3	TVM-2 (all)
٢-٩-١-٢	EVENT 1.9	ZCR 5.13	SR 3.3	PR.IP-12	CA-5	ISBR 13	010-R3	TVM-2f
٢-٩-١-٣	ORG 2.1	-	-	-	RA-5	-	003-R1, 010-R3	-
٢-٩-٢	EVENT 1.9	ZCR 5.13	SR 3.3	PR.IP-12	CA-5	ISBR 13	010-R3	TVM-2f
٢-١٠	**اختبار الاختراق**							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
٢-١٠-١								
٢-١٠-١-١	-	-	-	-	CA-8	-	010-R2	TVM-2e
٢-١٠-١-٢	-	-	-	-	CA-8	-	-	TVM-2e
٢-١٠-١-٣	-	-	-	-	CA-8	-	010-R2	TVM-2e
٢-١٠-١-٤	-	-	-	-	CA-8	-	010-R2	TVM-2e
٢-١٠-٢	-	-	-	-	CA-8	-	010-R2	TVM-2e
٢-١١	**إدارة سجلات الأحداث ومراقبة الأمن السيبراني**							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
٢-١١-١								
٢-١١-١-١	EVENT 1.1, EVENT 1.2, EVENT 1.5	-	SR 2.8, SR 6.1	PR.PT-1, DE.AE-3, DE.CM-1	AU-2	ISBR 16	007-R4	SA-1a, SA-1b
٢-١١-١-٢	-	-	SR 2.10	DE.DP-3	AU-5	-	007-R4	-
٢-١١-١-٣	EVENT 1.7	-	SR 6.2	DE.AE-2	CA-7	ISBR 2	007-R4	SA-2a
٢-١١-١-٤	-	SR 2.8	DE.CM-3	CA-7	ISBR 13	007-R4	SA-2b	-
٢-١١-١-٥	ORG 2.2	-	SR 2.8	DE.CM-4	CA-7	ISBR 13	007-R4	SA-2d
٢-١١-١-٦	ORG 2.2	-	SR 2.8	DE.CM-7	CA-7	ISBR 13	010-R2	SA-2b

SA-2b	005-R2	ISBR 18	SI-4	DE.CM-7	SR 2.8	-	ORG 2.2	٢-١-١١-٧
SA-1a, SA-1b	007-R4	ISBR 16	AU-2	PR.PT-1, DE.AE-3, DE.CM-1	SR 2.8, SR 6.1	-	EVENT 1.1, EVENT 1.2, EVENT 1.5	٢-١-١١-٨
SA-2b	007-R4	ISBR 13	CA-7	DE.CM-4	SR 2.8	-	ORG 2.2	٢-١-١١-٩
SA-2b	007-R4	ISBR 13	CA-7	DE.CM-4	SR 2.8	-	ORG 2.2	٢-١١-١-١٠
SA-1a, SA-1b	007-R4	ISBR 16	AU-2	PR.PT-1, DE.AE-3, DE.CM-1	SR 2.8, SR 6.1	-	EVENT 1.1, EVENT 1.2, EVENT 1.5	٢-١١-٢
								٢-١٢ إدارة حوادث وتهديدات الأمن السيبراني
المعايير								رقم الضابط
62443-2-1	62443-3-2	62443-3-3	NIST CSF	NIST SP800-53/82	NOG 104	NERC CIP	DOE C2M2	
								٢-١٢-١
IR-3f	008-R1, 008-R2, 008-R3	ISBR 16	IR-1, IR-8	RS.RP (all)	-	-	EVENT 1.8	٢-١٢-١-١
IR-3h	008-R3	ISBR 16	IR-4	RS.AN-2, RS.AN-3	-	-	EVENT 1.7	٢-١٢-١-٢
IR-4b	009-R1, 009-R2, 009-R3	ISBR 15	IR-4, IR-1	RS.RP (all)	-	-	EVENT 1.8, AVAIL 2.5	٢-١٢-١-٣
IR-3c	008-R1, 009-R1	ISBR 16	IR-8	RS.CO (all)	-	-	EVENT 1.8	٢-١٢-١-٤
IR-4c	008-R1, 008-R2, 008-R3	-	-	-	-	-	-	٢-١٢-١-٥
EDM-2e, CPM-2f, CPM-4b	-	-	CM-9, SA-3, SA-4 (3), SA-8, SA-15	PR.IP-2	-	-	ORG 2.3	٢-١٢-١-٦
-	-	-	IR-3	PR.IP-10	SR 3.3	-	-	٢-١٢-١-٧
TVM-1a, TVM-1e, TVM-1f, TVM-1j	-	ISBR 5, ISBR 13	SA-12 (8)	ID.RA-2	-	ZCR 5.1, ZCR 6.6	-	٢-١٢-١-٨
TVM-1a, TVM-1e, TVM-1f, TVM-1j	008-R1, 008-R2, 008-R3	ISBR 16	IR-1, IR-8	RS.RP (all)	-	-	EVENT 1.8	٢-١٢-٢
								٢-١٣ الأمن المادي
المعايير								رقم الضابط
62443-2-1	62443-3-2	62443-3-3	NIST CSF	NIST SP800-53/82	NOG 104	NERC CIP	DOE C2M2	
								٢-١٣-١
-	-	-	PE-2	DE.CM-7	-	-	ORG 3.1	٢-١٣-١-١
-	-	-	PE-3	DE.CM-7	-	-	ORG 3.1	٢-١٣-١-٢
-	-	-	PE-3	DE.CM-7	-	-	ORG 3.1	٢-١٣-١-٣
-	006-R1	-	PE-6, PE-6, PE-6 (1), PE-6 (3), PE-6 (4)	DE.CM-7	-	-	ORG 3.1	٢-١٣-١-٤

٢-١٣-١-٥	ORG 3.1	-	-	-	-	-	-	-
٢-١٣-١-٦	ORG 3.1	-	-	-	PE-8	-	-	-
٢-١٣-١-٧	-	-	-	DE.CM-6	MA-2	-	-	-
٢-١٣-١-٨	ORG 3.1	-	-	PR.AT-5	AT-2 PM-13	-	-	-
٢-١٣-١-٩	ORG 3.1	-	-	PR.AT-5	AT-2 PM-13	-	-	-
٢-١٣-٢	-	-	-	-	PE-1	-	-	-

٣ صمود الأمن السيبراني

٣-١	جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
٣-١-١								
٣-١-١-١	AVAIL 2.1	-	SR7.4	PR.IP-4	CP-9	ISBR 9	009-R1	IR-4c
٣-١-١-٢	AVAIL 1.1, AVAIL 1.2	-	SR 7.2, SR 7.3	PR.IP-4, PR.DS-4	CP-9 (6), PE-9 (1)	-	005-R1, 006-R1, 009-R1	IR-4c
٣-١-١-٣	AVAIL 1.1	-	-	PR.IP-9	PR.IP-9, CP-2 (5)	-	009-R1	IR-4c, IR-4e, IR-4h
٣-١-١-٤	AVAIL 1.1	ZCR 5.3, ZCR 5.4	SR 7.4	PR.IP-9	CP-6, CP-6 (1), CP-6 (2), CP-6 (3), CP-7, CP-7 (1), CP-7 (2), CP-7 (3), CP-7 (4)	ISBR 7	009-R1, 009-R2, 009-R3	IR-2a, IR-2d, IR-4a
٣-١-١-٥	AVAIL 1.2	-	SR 7.4, SR 7.5	PR.PT-5, PR.DS-4	SI-13 (4), (SI-13 (5	-	002-R1, 008-R2, 009-R2	-
٣-١-١-٦	-	-	-	PR.IP-10	CP-3 (1), CP-3 (2), CP-4 (3)	-	008-R2, 009-R2	-
٣-١-٢	AVAIL 2.1	-	SR7.4	PR.IP-4	CP-9	ISBR 9	009-R1	IR-4c

٤ الأمن السيبراني المتعلق بالأطراف الخارجية

٤-١	الأمن السيبراني المتعلق بالأطراف الخارجية							
رقم الضابط	المعايير							
	DOE C2M2	NERC CIP	NOG 104	NIST SP800-53/82	NIST CSF	62443-3-3	62443-3-2	62443-2-1
٤-١-١								
٤-١-١-١	ORG 1.6	ZCR 5.12	-	ID.SC-1, ID.SC-3	SA-12	ISBR 8	013-R1, 013-R2	-
٤-١-١-٢	ORG 1.6	-	-	ID.SC-2	IR-6 (3), PS-7, UL-2	-	013-R1, 013-R2	-
٤-١-١-٣	ORG 2.3	-	-	PR.IP-2	CM-9, SA-3, SA-4 (3), SA-8, SA-15	-	-	EDM-2e, CPM-2f, CPM-4b
٤-١-١-٤	-	-	SR 6.1	ID.SC-4	-	-	-	-
٤-١-٢	ID.SC-1	-	SR 6.1	ID.SC-4	-	-	-	-

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority