

البرنامج التدريبي: التحول الرقمي ومهارات المستقبل





الهدف العام للبرنامج التدريبي:

يأتي هذا البرنامج لتمكين المشاركين من ممارسة دوره كمراجع بكفاءة أعلى من خلال الفهم المتقدم لأبعاد التحول الرقمي ودورها في تطوير أساليب المراجعة بما يعزز كفاءة الأداء والشفافية والمساءلة، وتحقيق أثر المراجعة الفعّال في بيئة العمل الحكومية.

محاوَر البرنامج:

01

الربط بين أبعاد برنامج التحول الوطني ودور المراجعة الرقمية في دعمها.

02

ترتيب المراحل الأساسية للتحول الرقمي المؤسسي وفق التسلسل المنطقي الصحيح.

03

نضج المنصات الرقمية الحكومية وفق المناظير الأربعة لمؤشر النضج.

04

تحديد المجال الرئيسي والهدف والضوابط المناسبة الخاصة بالأمن السيبراني.

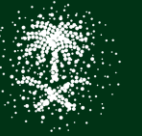
قياس المعرفة (التقييم القبلي)





المركز السعودي للمراجعة
المالية والرقابة على الأداء

الديوان العام للمحاسبة
GENERAL COURT OF AUDIT



اليوم الأول





المركز السعودي للمراجعة
المالية والرقابة على الأداء

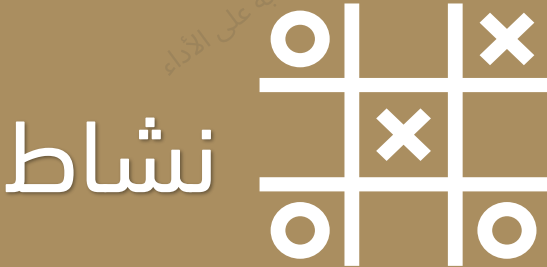
الديوان العام للمحاسبة
GENERAL COURT OF AUDIT



01

المحور الأول:

الربط بين أبعاد برنامج التحول الوطني ودور المراجعة الرقمية في دعمها



المركز السعودي
الديوان العام للمحاسبة
للمراجعة المالية والرقابة على الأداء

المركز السعودي
الديوان العام للمحاسبة
للمراجعة المالية والرقابة على الأداء

المركز السعودي
الديوان العام للمحاسبة
للمراجعة المالية والرقابة على الأداء

المركز السعودي
الديوان العام للمحاسبة
للمراجعة المالية والرقابة على الأداء

المركز السعودي
الديوان العام للمحاسبة
للمراجعة المالية والرقابة على الأداء

المركز السعودي
الديوان العام للمحاسبة
للمراجعة المالية والرقابة على الأداء

الديوان العام للمحاسبة
للمراجعة المالية والرقابة على الأداء

نشاط (1)

أن يربط المشارك بين أبعاد برنامج التحول الوطني ودور المراجعة الرقمية في دعمها.	هدف النشاط
زمن النشاط (20) دقيقة.	المدة الزمنية المتوقعة:
نشاط فردي	أسلوب النشاط

نشاط (1)

المطلوب:

اختر بُعدًا واحدًا ترى أنه الأكثر ارتباطًا بعملك أو مجالك، ثم عرّف بنفسك (اسمك ومسمّك الوظيفي)، وشارك زملاءك وجهة نظرك حول كيف يمكن للمراجعة الرقمية أن تدعم هذا البعد.

المعطيات:

أبعاد برنامج التحول الوطني:

1. تحقيق التميّز في الأداء الحكومي.
2. ضمان استدامة الموارد الحيوية.
3. تعزيز التنمية المجتمعية وتطوير القطاع غير الربحي.
4. الإسهام في تمكين القطاع الخاص.
5. التحول الرقمي.
6. تمكين فئات المجتمع من دخول سوق العمل ورفع جاذبيته.
7. تطوير الشراكات الاقتصادية.



كسر الجليد

المفهوم الشامل للتحول الرقمي في المؤسسات السعودية مفهوم التحول الرقمي:

يُعرّف **التحول الرقمي بأنه عملية مستمرة** تُمكن المنظمات من التكيف بمرونة مع ظروف السوق المتغيرة ومتطلبات الأعمال، وذلك من خلال اعتماد أحدث التقنيات لتحويل طريقة عملها وإشراك عملائها.

يتجاوز هذا المفهوم مجرد استخدام التقنية ليشمل **تحويل ثقافة الشركات** والمؤسسات والمنظمات، وتشجيع الموظفين على جميع المستويات على أداء واجباتهم بمرونة أكبر واستعداد لمشاركة المعلومات. هذا التحول **من التركيز على التقنية البحتة إلى التغيير الثقافي الشامل** يُعد عنصراً جوهرياً لنجاح المبادرات الرقمية. فالتبني الفعال للتقنيات يتطلب استعداداً ثقافياً داخل المنظمة، حيث أن مقاومة التغيير يمكن أن تعيق المبادرات بشكل كبير حتى مع توفر أحدث التقنيات. لذلك، **فإن الاستثمار في إدارة التغيير، والتدريب، وتعزيز عقلية "الرقمية أولاً" لا يقل أهمية، إن لم يكن أكثر، عن الاستثمار في التقنية نفسها.**



المفهوم الشامل للتحول الرقمي في المؤسسات السعودية

أبعاد برنامج التحول الوطني:



المفهوم الشامل للتحول الرقمي في المؤسسات السعودية أبرز النتائج التحول الرقمي:

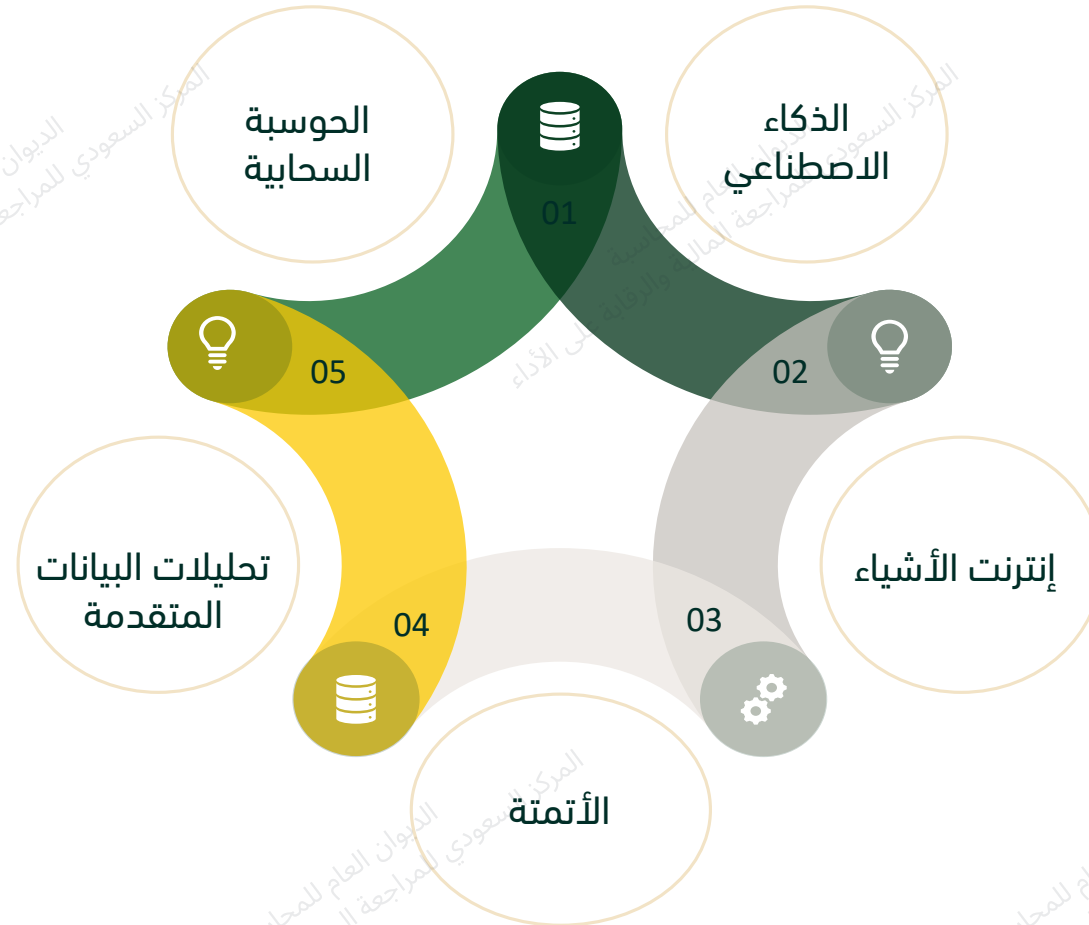
يهدف التحول الرقمي إلى تحقيق مجموعة من الأهداف المتعددة، بما في ذلك:

1. تطوير العمليات الداخلية.
2. تحسين تجربة العملاء.
3. تعزيز التعاون بين الموظفين.
4. تحقيق الاستدامة البيئية.
5. تطوير سلسلة التوريد.
6. تحقيق الميزة التنافسية.
7. الاستفادة الفعالة من تحليل البيانات.
8. زيادة الإنتاجية من خلال أتمتة العمليات وتبسيط الإجراءات.
9. تحسين اتخاذ القرارات عبر تحليل البيانات الضخمة.
10. تعزيز المرونة.
11. بناء سمعة قوية للمؤسسة من خلال تقديم خدمات مبتكرة وتجربة عملاء مميزة.



المفهوم الشامل للتحول الرقمي في المؤسسات السعودية

أبرز التقنيات التي تمكن هذا التحول:





المركز السعودي للمراجعة
المالية والرقابة على الأداء

الديوان العام للمحاسبة
GENERAL COURT OF AUDIT



استراحة

20 دقيقة

أبعاد التحول الرقمي ودوره في تطوير أساليب المراجعة في المملكة

تهدف منظومة شامل المحدثّة إلى **تمكين القيادة وحوكمة أعمال المراجعة** حيث تُعنى بإدارة وتنظيم عمليات المراجعة التي يجريها الديوان بموجب اختصاصه، وتبادل البيانات والمعلومات وتبليغ نتائج المراجعة واستقبال الردود آلياً مع الجهات المشمولة بمراجعة الديوان، **بما يسهم في رفع كفاءة الأعمال وتحسين جودة المخرجات ودعم اتخاذ القرار.**



ما هو الهدف من تطوير منظومة المراجعة الرقمية - شامل ؟

ما هي منظومة المراجعة الرقمية - شامل ؟

منظومة وطنية رقمية مبتكرة تُعزز كفاءة المراجعة من خلال تنفيذ أفضل المنهجيات والمعايير العالمية وتبني التقنيات الحديثة لتمكين التحول في أعمال المراجعة، **توفر المنظومة إجراءات مرقمة، ونماذج ذكية، وقنوات تواصل آمنة، وتحليلات متقدمة،** بالإضافة إلى تكامل فعال مع المنصات الحكومية الأخرى، مما يسهم في تحسين فعالية ودقة عمليات المراجعة.



01

قناة رسمية موحدة تضمن ضبط التواصل مع الديوان العام للمحاسبة



02

استجابة أسرع للملاحظات والطلبات ومتابعة لحالة المهام



03

توفير رؤية على نتائج المراجعة بما يدعم قياس الأداء وتحسينه



05

حوكمة واضحة للأدوار والصلاحيات وتوزيع المهام



06

تسريع الحصول على الموافقات والاعتمادات لطلبات المعاملات الأخرى

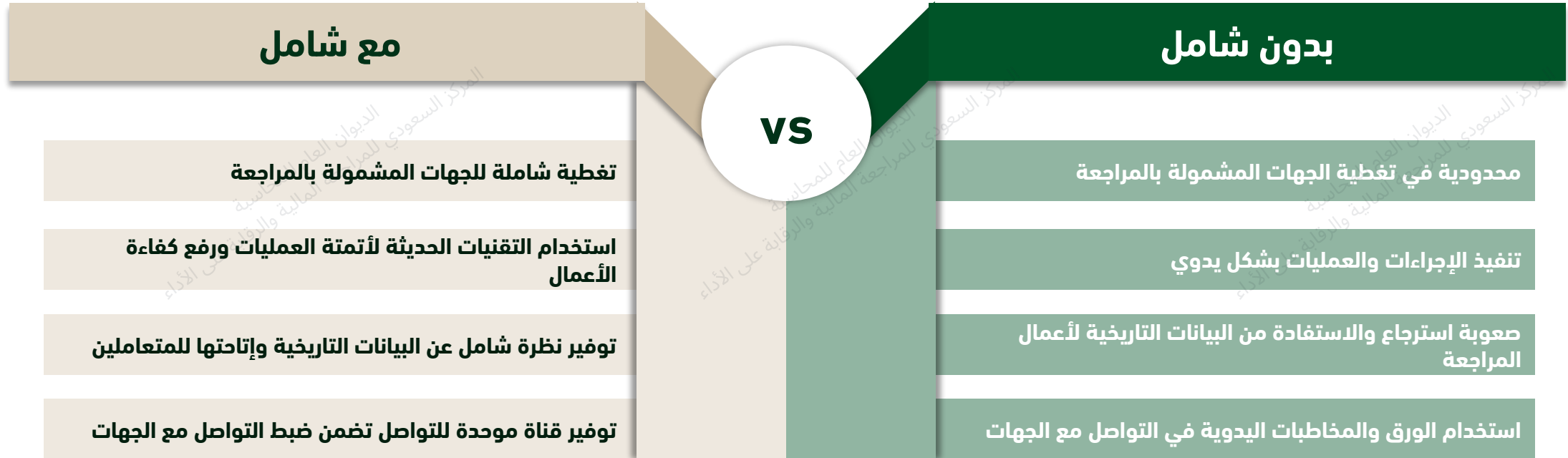


04

تنبيهات فورية لحالة الطلبات والمهام

أبعاد التحول الرقمي ودوره في تطوير أساليب المراجعة في المملكة

أثر تطوير منظومة المراجعة الرقمية "شامل" على أعمال المراجعة



القيمة المضافة من منظومة شامل:

التكامل الشامل مع المنصات الوطنية لتحسين آلية الحصول على البيانات وتحسين الخدمات

دعم اتخاذ القرار وتحسين جودة إعداد التقارير من خلال التحليلات المتقدمة

تعزيز الكفاءة والفعالية لأعمال المراجعة والتواصل مع الجهات

توفير تجربة موحدة ومتكاملة **للمستفيدين**

تعزيز الشفافية والمساءلة من خلال مراقبة جودة المخرجات ومتابعة التوصيات



المركز السعودي للمراجعة
المالية والرقابة على الأداء

الديوان العام للمحاسبة
GENERAL COURT OF AUDIT



02

المحور الثاني:

المراحل الأساسية للتحويل الرقمي المؤسسي وفق
التسلسل المنطقي الصحيح



نشاط (2)

هدف النشاط	أن يرتب المشاركون المراحل الأساسية للتحول الرقمي المؤسسي وفق التسلسل المنطقي الصحيح.
المدة الزمنية المتوقعة	زمن النشاط (10) دقائق.
أسلوب النشاط	نشاط فردي.

نشاط (2)

المطلوب:

رتّب مراحل التحول الرقمي المؤسسي بالترتيب الصحيح بدءًا من مرحلة الوعي حتى مرحلة الاستدامة والتحسين المستمر.

المعطيات:

المرحلة	الترتيب الصحيح
تطوير القدرات البشرية (Human Capacity Development)	
الوعي والاستراتيجية (Awareness & Strategy)	
التنفيذ والتوسع (Implementation & Scaling)	
التقنيات الناشئة والتطبيق العملي (Emerging Technologies & Practical Application)	
إعادة تصميم العمليات (Process Redesign)	
الاستدامة والتحسين المستمر (Sustainability & Continuous Improvement)	
التهيئة والبنية التحتية (Readiness & Infrastructure)	



نشاط جماعي

نشاط (2)

الحل:



الترتيب الصحيح

- 01 الوعي والاستراتيجية (Awareness & Strategy)
- 02 التهيئة والبنية التحتية (Readiness & Infrastructure)
- 03 إعادة تصميم العمليات (Process Redesign)
- 04 تطوير القدرات البشرية (Human Capacity Development)
- 05 التقنيات الناشئة والتطبيق العملي (Emerging Technologies & Practical Application)
- 06 التنفيذ والتوسع (Implementation & Scaling)
- 07 الاستدامة والتحسين المستمر (Sustainability & Continuous Improvement)



مراحل التحول الرقمي المؤسسي

لا يوجد إطار زمني محدد للتحول الرقمي؛ إنه عملية مستمرة تتطلب التزاماً طويلاً الأمد، ويمكن تقسيمها إلى مراحل قابلة للتحقيق مع أهداف قصيرة ومتوسطة وطويلة الأجل. يُعد التخطيط للتحول الرقمي الخطوة الأولى والأهم لضمان النجاح وتجنب هدر الموارد وعدم تحقيق الأهداف المرجوة.



مراحل التحول الرقمي المؤسسي

مراحل التحول الرقمي عادةً تمر بعدة خطوات مترابطة، تختلف تفاصيلها من مؤسسة إلى أخرى، لكنها غالبًا تتبع إطارًا مشتركًا:

1. الوعي والاستراتيجية (Awareness & Strategy)

- تحديد الرؤية (Vision Setting): لماذا تحتاج المؤسسة للتحول الرقمي؟ لتحسين تجربة العملاء؟ تقليل التكاليف؟ تعزيز الكفاءة؟
- تقييم الوضع الحالي (Current State Assessment): تحليل البنية التحتية التقنية، الثقافة المؤسسية، والعمليات.
- وضع خارطة طريق (Roadmap Development): صياغة استراتيجية شاملة بأهداف واضحة ومؤشرات أداء (KPIs).

في المملكة: يتجسد في استراتيجية الحكومة الرقمية (2030-2025)



مراحل التحول الرقمي المؤسسي

مراحل التحول الرقمي عادةً تمر بعدة خطوات مترابطة، تختلف تفاصيلها من مؤسسة إلى أخرى، لكنها غالبًا تتبع إطارًا مشتركًا:

2. التهيئة والبنية التحتية (Readiness & Infrastructure)

- تطوير البنية التحتية التقنية (Technology Infrastructure Upgrade): تحديث الشبكات، الأنظمة، وقواعد البيانات.
- اعتماد الحوسبة السحابية أو الهجينة (Cloud / Hybrid Adoption) : لزيادة المرونة والتوسع.
- الأمن السيبراني (Cybersecurity): إدماج ضوابط قوية لحماية البيانات والعمليات.

في المملكة: يتجسد في استراتيجية الحكومة الرقمية (2030-2025)



مراحل التحول الرقمي المؤسسي

مراحل التحول الرقمي عادةً تمر بعدة خطوات مترابطة، تختلف تفاصيلها من مؤسسة إلى أخرى، لكنها غالبًا تتبع إطارًا مشتركًا:

3. إعادة تصميم العمليات (Process Redesign):

- أتمتة العمليات (RPA – Process Automation): استخدام الروبوتات البرمجية.
- إعادة هندسة الإجراءات (BPR – Business Process Reengineering): بما يتماشى مع الأدوات الرقمية.
- التركيز على تجربة العميل (Customer Experience Focus): استخدام قنوات رقمية سلسلة وذكية.

في المملكة: مثل ما قامت به وزارة الداخلية عبر أتمتة خدمات الجوازات والإقامة.



مراحل التحول الرقمي المؤسسي

مراحل التحول الرقمي عادةً تمر بعدة خطوات مترابطة، تختلف تفاصيلها من مؤسسة إلى أخرى، لكنها غالبًا تتبع إطارًا مشتركًا:

4. تطوير القدرات البشرية (Human Capacity Development):

- التدريب وبناء المهارات الرقمية (Digital Skills Training): رفع وعي الموظفين.
- تغيير الثقافة المؤسسية (Cultural Change): تعزيز الابتكار والتجريب.
- إدارة التغيير (Change Management): لتقليل مقاومة الموظفين وضمان التبني السلس.

في المملكة: يتم دعمها عبر مبادرات مثل مهارات المستقبل وأكاديمية سدايا.



مراحل التحول الرقمي المؤسسي

مراحل التحول الرقمي عادةً تمر بعدة خطوات مترابطة، تختلف تفاصيلها من مؤسسة إلى أخرى، لكنها غالبًا تتبع إطارًا مشتركًا:

5. التقنيات الناشئة والتطبيق العملي (Emerging Technologies & Practical Application) :

- الذكاء الاصطناعي والتحليلات المتقدمة (AI & Advanced Analytics): لاستخراج رؤى جديدة من البيانات.
- البلوك تشين، إنترنت الأشياء، الواقع المعزز/الافتراضي (Blockchain, IoT, AR/VR): حسب طبيعة القطاع.
- التجريب والابتكار (Experimentation & Innovation): إنشاء مختبرات رقمية أو بيئات اختبارية (Sandboxes).

في المملكة: تُطبَّق في مشاريع مثل نيوم باستخدام إنترنت الأشياء والذكاء الاصطناعي.



مراحل التحول الرقمي المؤسسي

مراحل التحول الرقمي عادةً تمر بعدة خطوات مترابطة، تختلف تفاصيلها من مؤسسة إلى أخرى، لكنها غالبًا تتبع إطارًا مشتركًا:

6. التنفيذ والتوسع (Implementation & Scaling):

- إطلاق المشاريع الرقمية تدريجيًا (Pilot Projects): ثم توسيعها.
- قياس الأداء ومراجعة النتائج (Performance Measurement & Review): مقابل الأهداف.
- التوسع عبر المؤسسة (Enterprise-wide Scaling): تعميم الحلول الناجحة على الوحدات الأخرى.

في المملكة: نراه في تعميم تجربة أبشر على جميع مناطق المملكة.



مراحل التحول الرقمي المؤسسي

مراحل التحول الرقمي عادةً تمر بعدة خطوات مترابطة، تختلف تفاصيلها من مؤسسة إلى أخرى، لكنها غالبًا تتبع إطارًا مشتركًا:

7. الاستدامة والتحسين المستمر (Sustainability & Continuous Improvement):

- تحليل البيانات بشكل دوري (Data-Driven Decision Making) : لدعم القرارات.
- التطوير المستمر (Continuous Improvement): تحديث الأنظمة والعمليات باستمرار.
- تعزيز الابتكار (Innovation Embedding): كممارسة يومية.

في المملكة: تقاس بمؤشرات هيئة الحكومة الرقمية مثل مؤشر نضج الخدمات الرقمية.



مراحل التحول الرقمي المؤسسي

مراحل التحول الرقمي عادةً **تمر بعدة خطوات مترابطة**، تختلف تفاصيلها من مؤسسة إلى أخرى، لكنها غالبًا تتبع إطارًا مشتركًا:

يتضمن التخطيط الاستراتيجي للتحول الرقمي تحديد الأولويات بناءً على تأثيرها على الأعمال وقدرتها على تحقيق عوائد سريعة. كما يشمل بناء القدرات البشرية من خلال برامج تدريبية وتأهيلية لرفع كفاءة الموظفين. ومن الضروري تحديد الموارد البشرية والتقنية المطلوبة لتنفيذ المشاريع الرقمية، وتوقع التحديات المحتملة ووضع استراتيجيات للتخفيف من المخاطر. ويجب ضمان التنسيق بين مختلف الإدارات والأقسام في المؤسسة. يتطلب التخطيط الاستراتيجي أيضاً تحديد المبادرات والمشاريع الاستراتيجية اللازمة لتحقيق التحول الرقمي، مع وضع مؤشرات أداء واضحة، وتطوير نموذج لتحقيق التكامل مع الجهات الخارجية ذات العلاقة لضمان تحقيق الأهداف.



التحول الوطني والمراجعة المفهوم الشامل للتحول الرقمي في المؤسسات السعودية

كما أن دعم أطر الحوكمة الوطنية بالمرونة والتكرار السريع، مثل ضوابط الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني (NCA)، ومعايير سدايا (SDAIA) الخاصة بالبيانات والذكاء الاصطناعي، يضمن أن الابتكار الرقمي يتم في إطار من الامتثال والموثوقية.



المركز السعودي للمراجعة
المالية والرقابة على الأداء

الديوان العام للمحاسبة
GENERAL COURT OF AUDIT



اليوم الثاني



تصنيف الوثيقة: مقيد - Restricted



المركز السعودي للمراجعة
المالية والرقابة على الأداء

الديوان العام للمحاسبة
GENERAL COURT OF AUDIT



03

المحور الثالث:

نضج المنصات الرقمية الحكومية وفق المناظير الأربعة
لمؤشر النضج

النضج الرقمي المؤسسي في المملكة العربية السعودية

مؤشر نضج التجربة الرقمية

يُعد مؤشر نضج التجربة الرقمية مؤشراً سنوياً يهدف إلى قياس مدى نضج المنصات والخدمات الحكومية الرقمية، وتقديم التوصيات التي تساهم في رفع نضجها بما يتواءم مع الاستراتيجيات الوطنية.

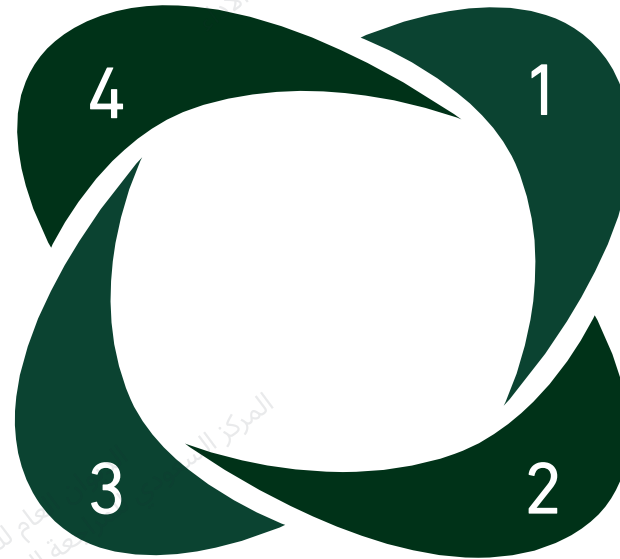
تسعى هيئة الحكومة الرقمية من خلال هذا المؤشر إلى تحقيق أهداف رئيسية مثل:

تأسيس ممارسات قياس نضج التجربة الرقمية بناءً على أفضل المعايير الدولية.

تعزيز التجربة الرقمية للمستفيدين ورفع رضاهم.

مواكبة التوجهات الاستراتيجية للحكومة الرقمية.

رفع نضج المنصات والخدمات الرقمية.



النضج الرقمي المؤسسي في المملكة العربية السعودية

النضج الرقمي في المملكة العربية السعودية أصبح معيارًا وطنيًا؛ إذ تستخدمه هيئة الحكومة الرقمية ليس فقط كأداة تقييم بل كوسيلة لبناء هوية رقمية سعودية مميزة.

الخدمات مثل مدرستي وصحتي وأبشر لا تُستخدم كمنصات فقط بل كنماذج وطنية للفخر أمام المجتمع الدولي.

كما أن إدراج معايير مثل رضا المستفيد وإمكانية الوصول لذوي الإعاقة يعكس التزامًا بالهوية السعودية الشاملة التي تراعي جميع شرائح المجتمع.



صحتي
Sehhaty



توكلنا
Tawakkalna



النضج الرقمي المؤسسي في المملكة العربية السعودية

يركز المؤشر على أربعة مناظير رئيسية لقياس نضج التجربة الرقمية:



النضج الرقمي المؤسسي في المملكة العربية السعودية

مؤشر نضج التجربة الرقمية للخدمات الحكومية في السعودية

التفاصيل	المعيار / الخاصية
الجهة المسؤولة	هيئة الحكومة الرقمية DGA – Digital Government Authority.
الأهداف الرئيسية	مواكبة التوجهات الاستراتيجية للحكومة الرقمية، رفع نضج المنصات والخدمات الرقمية الحكومية، تعزيز التجربة الرقمية للمستخدمين ورفع رضاهم، تأسيس ممارسات قياس نضج التجربة الرقمية بناءً على أفضل المعايير الدولية، تسريع التحول الرقمي للمنصات والخدمات الرقمية الحكومية، الاستفادة من المنصات والخدمات الرقمية ذات النضج العالي كنماذج وطنية.
المناظير الرئيسية للقياس	رضا المستخدم، تجربة المستخدم، التعامل مع الشكوى، التقنيات والأدوات.
معايير اختيار المنصات المشمولة	تنوع القطاعات التي تخدمها المنصة، تأثير المنصة في المؤشرات الدولية، أهمية المنصة في القطاع الذي تخدمه، حجم الخدمات والعمليات على المنصة، عدد المستخدمين من المنصة وتنوع شرائحهم، حجم التفاعل على المنصة في منصات التواصل الاجتماعي، ارتباط المنصة بأهم رحلات الحياة التي يحتاجها مختلف المستخدمين في المملكة.
أمثلة على المنصات الحكومية المشمولة	أبشر، صحتي، مدرستي، منصات التعليم عن بعد.



المركز السعودي للمراجعة
المالية والرقابة على الأداء

الديوان العام للمحاسبة
GENERAL COURT OF AUDIT



04

المحور الرابع:

تحديد المجال الرئيسي والهدف والضوابط المناسبة الخاصة
بالأمن السيبراني



نشاط (3)

أن يحدد المشارك المجال الرئيسي والهدف والضوابط المناسبة الخاصة بالأمن السيبراني من خلال تحليل سيناريوهات واقعية.	هدف النشاط
زمن النشاط (15) دقيقة.	المدة الزمنية المتوقعة
سيناريو.	أسلوب النشاط

المطلوب:

- قم بالاختيار المجال المناسب للسيناريو من الجدول أدناه وأذكر الآتي :
- المجال الرئيسي الذي يندرج تحته السيناريو.
 - الهدف المرتبط به وفق ما تفهمه من الموقف.
 - الضوابط أو الممارسات المقترحة لضمان تحسين الأداء أو معالجة التحدي المعروض.

المعطيات:

سيناريو	حدث انقطاع كامل في أحد مراكز البيانات الحكومية بسبب عطل في نظام التبريد، مما تسبب في توقف الخدمات الرقمية لمدة 6 ساعات. تبين لاحقاً أن خطة استمرارية الأعمال لم تُحدَّث منذ عامين، وأن اختبارات الاسترداد من الكوارث لم تُنفذ مؤخراً.
المجالات	تعزيز الأمن السيبراني
	حوكمة الأمن السيبراني
	صمود الأمن السيبراني
المجالات	الأمن السيبراني المتعلق بالأطراف الخارجية



سيناريو

أمثلة إضافية

الحل:



سيناريو (3)

حدث انقطاع كامل في أحد مراكز البيانات الحكومية بسبب عطل في نظام التبريد، مما تسبب في توقف الخدمات الرقمية لمدة 6 ساعات. تبين لاحقًا أن خطة استمرارية الأعمال لم تُحدَّث منذ عامين، وأن اختبارات الاسترداد من الكوارث لم تُنفذ مؤخرًا.

العنصر	الإجابة
المجال الرئيسي	صمود الأمن السيبراني.
الهدف الرئيسي	ضمان استمرارية الخدمات الحيوية واستعادة الأنظمة بسرعة عند الأزمات.
الضوابط المناسبة	تحديث خطة استمرارية الأعمال واختبارها دوريًا. إنشاء مركز تعافٍ احتياطي فعال. توثيق آلية الاستجابة للحوادث والأزمات.

معايير مراجعة البنية التحتية الرقمية والأنظمة الحكومية في السعودية

تضع المملكة العربية السعودية أطراً تنظيمية صارمة لضمان أمن وموثوقية بنيتها التحتية الرقمية وأنظمتها الحكومية، وذلك من خلال جهود هيئات رئيسية مثل:

- الهيئة الوطنية للأمن السيبراني (NCA)

- هيئة الحكومة الرقمية (DGA)

بالإضافة إلى معايير أخرى ذات صلة.



الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

هيئة
الحكومة
الرقمية
Digital
Government
Authority



الهيئة الوطنية للأمن السيبراني

عن الهيئة الوطنية للأمن السيبراني – NCA



الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

صدر الأمر الملكي الكريم رقم (6801) بتاريخ 1439/2/11هـ، بالموافقة على تنظيم الهيئة الوطنية للأمن السيبراني وارتباطها بمقام خادم الحرمين الشريفين -حفظه الله-، لتكون الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه، وتهدف إلى تعزيزه حماية للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية.

ولا يخلي ذلك أي جهة عامة أو خاصة أو غيرها من مسؤوليتها تجاه أمنها السيبراني بما لا يتعارض مع اختصاصات ومهام الهيئة الواردة في تنظيمها.

الرؤية

فضاء سيبراني سعودي آمن وموثوق يمكّن النمو والازدهار.

الرسالة

نعزز الأمن السيبراني في المملكة؛ لتقلي المخاطر وتعزيز الثقة وتمكين النمو.

القيم



الاعتراف



الإتقان



الشغف



اليقظة

نهج المملكة العربية السعودية في بناء الأمن السيبراني

التنفيذ

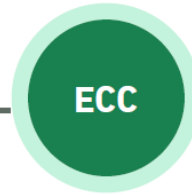
تطوير وتنفيذ
برامج ومبادرات
وطنية للتدريب،
وتنظيم الحكومة،
وتعزيز القدرات
الوطنية.



2020

الضوابط

إصدار الضوابط
الأساسية للأمن
السيبراني (ECC)
والزام الجهات
الوطنية بتنفيذها.



2018

التأسيس

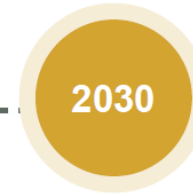
تأسيس الهيئة
الوطنية للأمن
السيبراني بمرسوم
ملكي كجهة مركزية
منظمة.



2017

الرؤية

إطلاق رؤية 2030
وتضمن الأمن
السيبراني ضمن
محاورها
الاستراتيجية.



2016

البداية

مبادرات أولية
للمحماية السيبرانية
وتنفيذ مراكز أمن
المعلومات لدى
جهات حكومية
وحساسة.



2015

نهج المملكة العربية السعودية في بناء الأمن السيبراني

الاستراتيجية

اعتماد
الاستراتيجية
الوطنية للأمن
السيبراني وتنفيذ
المرحلة الأولى من
المشاريع الوطنية.



2021

التقدم

تطوير ضوابط
ومقاييس متقدمة
(مثل الأمن
السيبراني الصناعي،
والسحابي).



2022-
2023

التفوق

تحقيق المركز الأول
عالمياً على مؤشر
الأمن السيبراني،
وتعزيز الابتكار
وتطبيق الذكاء
الاصطناعي.



2024

العقوبات

إقرار العقوبات على
الجهات غير المنفذة
للضوابط وتعزيز مبدأ
المحاسبة وضبط
الامتثال.



2024

القادم

التركيز على الأمن
السيبراني التنبئي،
تطوير القدرات
الوطنية، والحفاظ على
الإنجازات و المكانة
التي حققتها المملكة.



المستقبل

الهيئة الوطنية للأمن السيبراني

1.1. ضوابط الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني

تسعى إدارة الأمن
السيبراني بتحقيق الالتزام
الكامل بالضوابط
والتشريعات الصادرة من
الهيئة الوطنية للأمن
السيبراني وهي كالتالي:

ضوابط الأمن السيبراني الأساسية (ECC)

هي الضوابط التي **تمثل الحد الأدنى** من المتطلبات والمعايير الأساسية والشاملة لضمان الحماية الأساسية للأصول الرقمية والمعلوماتية للديوان.

01

ضوابط الأنظمة الحساسة (CSCC)

هي الضوابط الإضافية الموجهة **لحماية المعلومات أو الأنظمة الأكثر حساسية**، والتي تتطلب مستوى أعلى من الحماية نظرًا لأهميتها أو حساسيتها.

02

ضوابط حسابات التواصل (OSMAC)

هي ضوابط تهدف إلى تنظيم **استخدام حسابات التواصل الاجتماعي**، وتعزيز الأمان السيبراني، وحماية البيانات، وضمان المسؤولية في التعامل مع المعلومات.

03

ضوابط الأمن السيبراني للبائانات (DCC)

تهدف إلى **حماية البائانات** من التهديدات السيبرانية. تشمل الضوابط تنظيم الوصول إلى البائانات، وتخزينها، ونقلها، لضمان سرية البائانات وسلامتها واستمرارية الوصول إليها بشكل آمن.

04

ضوابط الأمن السيبراني للعمل عن بعد (TCC)

تهدف إلى ضمان الأمان السيبراني **أثناء العمل عن بعد**. تشمل الضوابط حماية الأجهزة والشبكات، تأمين البائانات، وضمان استخدام تقنيات موثوقة لتفادي المخاطر والهجمات الإلكترونية.

05

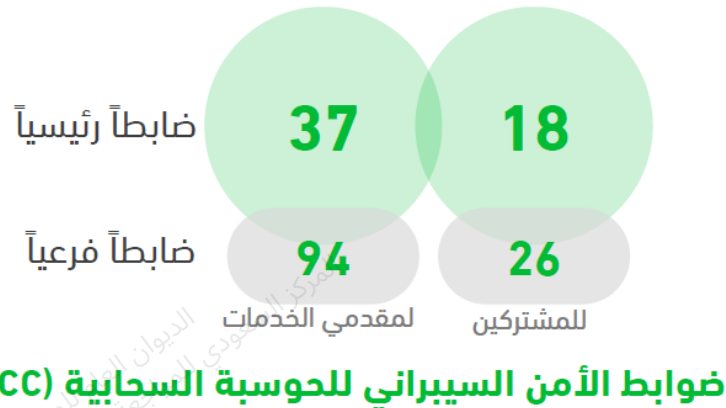
ضوابط الحوسبة السحابية (CCC)

تهدف إلى ضمان الأمان وحماية البائانات عند استخدام الخدمات السحابية. تشمل الضوابط تأمين الوصول إلى البائانات، وضمان الامتثال للمعايير الأمنية أثناء تخزين ومعالجة البائانات في السحابة.

06

الهيئة الوطنية للأمن السيبراني

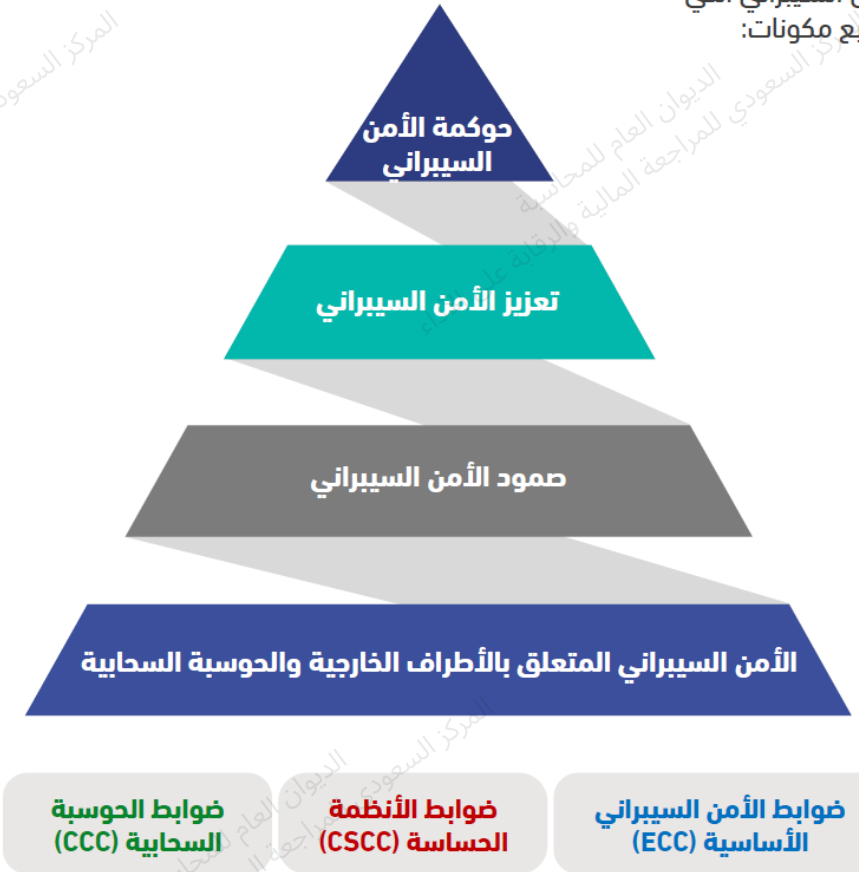
1.2. ضوابط الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني



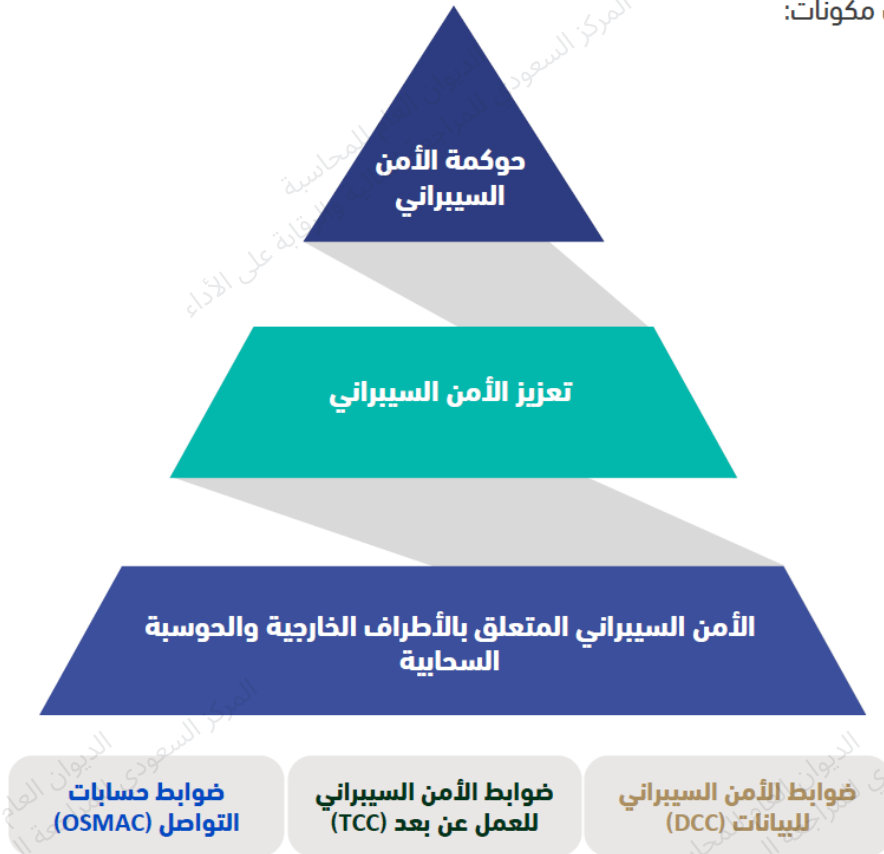
الهيئة الوطنية للأمن السيبراني

2.1. مكونات ضوابط الأمن السيبراني

ضوابط الأمن السيبراني التي تتكون من أربع مكونات:



ضوابط الأمن السيبراني التي تتكون من ثلاث مكونات:



الهيئة الوطنية للأمن السيبراني

2.2. مثال على مكونات ضوابط الأمن السيبراني

إدارة الأمن السيبراني Cybersecurity Management	٣-١	إستراتيجية الأمن السيبراني Cybersecurity Strategy	١-١	١ - حوكمة الأمن السيبراني Cybersecurity Governance
أدوار ومسؤوليات الأمن السيبراني Cybersecurity Roles and Responsibilities	٤-١	سياسات وإجراءات الأمن السيبراني Cybersecurity Policies and Procedures	٣-١	
الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية Cybersecurity in Information Technology Projects	٦-١	إدارة مخاطر الأمن السيبراني Cybersecurity Risk Management	٥-١	
المراجعة والتدقيق الدوري للأمن السيبراني Cybersecurity Periodical Assessment and Audit	٨-١	الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني Cybersecurity Regulatory Compliance	٧-١	
برنامج التوعية والتدريب بالأمن السيبراني Cybersecurity Awareness and Training Program	١٠-١	الأمن السيبراني المتعلق بالموارد البشرية Cybersecurity in Human Resources	٩-١	٢ - تعزيز الأمن السيبراني Cybersecurity Defence
إدارة هويات الدخول والصلاحيات Identity and Access Management	٣-٢	إدارة الأصول Asset Management	١-٢	
حماية البريد الإلكتروني Email Protection	٤-٢	حماية الأنظمة وأجهزة معالجة المعلومات Information System and Processing Facilities Protection	٣-٢	
أمن الأجهزة المحمولة Mobile Devices Security	٦-٢	إدارة أمن الشبكات Networks Security Management	٥-٢	
التشفير Cryptography	٨-٢	حماية البيانات والمعلومات Data and Information Protection	٧-٢	
إدارة الثغرات Vulnerabilities Management	١٠-٢	إدارة النسخ الاحتياطية Backup and Recovery Management	٩-٢	
إدارة سجلات الأحداث ومراقبة الأمن السيبراني Cybersecurity Event Logs and Monitoring Management	١٢-٢	اختبار الاختراق Penetration Testing	١١-٢	
الأمن المادي Physical Security	١٤-٢	إدارة حوادث وتهديدات الأمن السيبراني Cybersecurity Incident and Threat Management	١٣-٢	
حماية تطبيقات الويب Web Application Security	١٥-٢		١٥-٢	
جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience aspects of Business Continuity Management (BCM)	١-٣		١-٣	
الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity	٢-٤	الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	١-٤	٣ - صمود الأمن السيبراني Cybersecurity Resilience
				٤ - الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud

مكونات ضوابط الأمن السيبراني الأساسية (ECC)

مكونات فرعية تابعة

مكونات أساسية

جوانب صمود الأمن السيبراني في إدارة استمرارية الأعمال Cybersecurity Resilience aspects of Business Continuity Management (BCM)	١-٣	٣ - صمود الأمن السيبراني Cybersecurity Resilience
الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة Cloud Computing and Hosting Cybersecurity	٢-٤	٤ - الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية Third-Party and Cloud Computing Cybersecurity
الأمن السيبراني المتعلق بالأطراف الخارجية Third-Party Cybersecurity	١-٤	

الهيئة الوطنية للأمن السيبراني

2.3. مثال على أحد ضوابط الأمن السيبراني

مكون فرعي

ضابط رئيسي

ضوابط فرعية تابعة

الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية (Third-Party and Cloud Computing Cybersecurity)	
١-٤	الأمن السيبراني المتعلق بالأطراف الخارجية
الهدف	ضمان حماية أصول الجهة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية (بما في ذلك خدمات الإسناد للأمن السيبراني أو لتقنية المعلومات "Outsourcing" والخدمات المدارة "Managed Services"). وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-١-٤	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني ضمن العقود والاتفاقيات مع الأطراف الخارجية للجهة.
٢-١-٤	يجب أن تغطي متطلبات الأمن السيبراني ضمن العقود والاتفاقيات (مثل اتفاقية مستوى الخدمة SLA) مع الأطراف الخارجية التي قد تتأثر بإصابتها ببيانات الجهة أو الخدمات المقدمة لها بحد أدنى ما يلي: ١-٢-١-٤ بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الآمن من قبل الطرف الخارجي لبيانات الجهة عند انتهاء الخدمة. ٢-٢-١-٤ إجراءات التواصل في حال حدوث حادثة أمن سيبراني. ٣-٢-١-٤ إلزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.
٣-١-٤	يجب أن تغطي متطلبات الأمن السيبراني مع الأطراف الخارجية التي تقدم خدمات الإسناد للأمن السيبراني أو لتقنية المعلومات، أو الخدمات المدارة بحد أدنى ما يلي: ١-٣-١-٤ إجراء تقييم لمخاطر الأمن السيبراني، والتأكد من وجود ما يضمن السيطرة على تلك المخاطر، قبل توقيع العقود والاتفاقيات أو عند تغيير المتطلبات التشريعية والتنظيمية ذات العلاقة. ٢-٣-١-٤ أن تكون مراكز عمليات خدمات الأمن السيبراني المدارة للتشغيل والمراقبة، والتي تستخدم طريقة الوصول عن بعد، موجودة بالكامل داخل المملكة.
٤-١-٤	يجب مراجعة متطلبات الأمن السيبراني مع الأطراف الخارجية دورياً.

الهيئة الوطنية للأمن السيبراني

3. الدعم المقدم من الهيئة الوطنية للأمن السيبراني

تقدم **الهيئة الوطنية للأمن السيبراني** الدعم للجهات لتعزيز الأمن السيبراني وذلك عبر تقديم الدعم والإرشاد:

إنشاء ضوابط الأمن السيبراني المتعلقة بأهم المجالات

إنشاء إرشادات تطبيق ضوابط الأمن السيبراني.

تقديم أدوات مساعدة ونماذج لوثائق الحوكمة مثل: سياسات، إجراءات معايير وخطط

التقييم الدوري للجهات لحالة تطبيق ضوابط الأمن السيبراني.

التوعية والتدريب لكوادر الأمن السيبراني الوطنية.

تنظيم حملات ومبادرات توعوية للجهات ومنسوبيها.

الدعم في حالة الحوادث السيبرانية والطوارئ.

تقديم المعلومات بما يتعلق بالتهديدات والحوادث.

وتقدم هذه القنوات من خلال قنوات التواصل المباشر مع الهيئة مثل منصة **حصين** أو ضابط الاتصال لكل جهة.



الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

الدليل الإرشادي لتطبيق الضوابط
الأساسية للأمن السيبراني

Guide to Essential Cybersecurity Controls
Implementation (GECC – 1 : 2023)

إشارة المشايخة لـ
تصنيف الوثيقة: عام

نموذج السياسة العامة للأمن السيبراني

أعلى تصنيف

التاريخ
الإصدار
الترخيص

مستند ذات الصلة
مستند ذات الصلة
مستند ذات الصلة

مستند ذات الصلة
مستند ذات الصلة
مستند ذات الصلة
مستند ذات الصلة
مستند ذات الصلة
مستند ذات الصلة
مستند ذات الصلة
مستند ذات الصلة
مستند ذات الصلة
مستند ذات الصلة

الهيئة الوطنية للأمن السيبراني تطلق
المعرض المتنقل للتوعية
بالأمن السيبراني

المملكة تحقق المرتبة الأولى عالمياً في مؤشر الأمن السيبراني

وفق الكتاب السنوي للتنافسية العالمية لعام 2024





المركز السعودي للمراجعة
المالية والرقابة على الأداء

الديوان العام للمحاسبة
GENERAL COURT OF AUDIT



استراحة

20 دقيقة

معايير مراجعة البنية التحتية الرقمية والأنظمة الحكومية في السعودية

ضوابط حوكمة تقنية المعلومات هيئة الحكومة الرقمية - DGA

تهدف هيئة الحكومة الرقمية إلى تعزيز الأداء الرقمي في الجهات الحكومية، ورفع جودة الخدمات، وتحسين تجربة المستفيد، بما يتوافق مع رؤية المملكة 2030، وتعد الهيئة المرجع الوطني المختص في هذا الشأن. أعدت الهيئة "ضوابط حوكمة تقنية المعلومات في الحكومة الرقمية" **لدعم حوكمة الإدارات المشرفة على تقنية المعلومات في الجهات الحكومية والإطار التنظيمي التابع لها، وتوحيد السياسات والإجراءات، ومتابعة الالتزام بها.**

تتمثل الأهداف الرئيسية لضوابط حوكمة تقنية المعلومات في: التخطيط والتنظيم لحوكمة تقنية المعلومات ومواءمتها مع استراتيجيات الجهة، وتطبيق المبادئ والممارسات السليمة لتنفيذ وتشغيل عمليات حوكمة تقنية المعلومات، والمراقبة والتقييم لمتطلبات حوكمة تقنية المعلومات الداخلية والخارجية للجهة، وتقديم الدعم لحوكمة تقنية المعلومات وعمليات تشغيلها.

تستند هذه الضوابط إلى مبادئ أساسية للإطار التنظيمي لأعمال الحكومة الرقمية، منها: **طلب بيانات المستخدم لمرة واحدة، الرقمنة أولاً، الأجهزة الذكية أولاً، الرقمنة افتراضياً، الحكومة الرقمية منصة شاملة، الرقمنة في التصميم، الإتاحة افتراضياً، وسهولة تطوير السياسات.**



معايير مراجعة البنية التحتية الرقمية والأنظمة الحكومية في السعودية

ضوابط حوكمة تقنية المعلومات هيئة الحكومة الرقمية - DGA

تتضمن ضوابط حوكمة تقنية المعلومات خمسة مستويات رئيسية:

1. **إدارة تقنية المعلومات:** تهدف إلى تمكين الإدارة العليا المسؤولة عن مستوى نضج حوكمة تقنية المعلومات وفعاليتها.
2. **تخطيط تقنية المعلومات:** تهدف إلى التأكيد على ضمان إدارة عمليات مخاطر تقنية المعلومات بفاعلية، بالإضافة إلى كفاءة نموذج الحوكمة والاستراتيجيات الخاصة بتقنية المعلومات.
3. **بناء وتطوير وتنفيذ أنظمة تقنية المعلومات:** تهدف إلى تحديد التغييرات المتعلقة بأصول المعلومات والخدمات الرقمية وتصميمها واختبارها وتنفيذها لتقليل تأثير المخاطر المتعلقة بإدارة التغيير.
4. **تحقيق القيم المضافة من تقنية المعلومات:** تهدف إلى تحقيق المنافع من بيئة تقنية المعلومات لدى الجهة، ودعم أهداف الحكومة الرقمية بتنفيذ الإدارة الفعالة والمراجعة المستمرة.
5. **مراقبة الأداء والتحسين المستمر:** تهدف إلى مراقبة الأداء وفعاليتها كفاءة الخدمات الرقمية والتقنية، وضمان عملية التحسين المستمر عن طريق قياس الأداء والمراجعات الداخلية.



معايير مراجعة البنية التحتية الرقمية والأنظمة الحكومية في السعودية

ضوابط حوكمة تقنية المعلومات هيئة الحكومة الرقمية - DGA

تتضمن هذه الضوابط أيضاً معايير لحوكمة وإدارة البيانات، تشمل تطبيق الأنظمة والمعايير المتعلقة بالبيانات الحكومية وآلية تطويرها، وحوكمة وإدارة البيانات، واستخدام وإتاحة البيانات، والبيانات المفتوحة.

كما تشمل ضوابط إدارة العمليات، وسياسات وإجراءات تقنية المعلومات، وتحديد الأدوار والمسؤوليات، وإدارة مخاطر تقنية المعلومات، وإدارة الكفاءات والقدرات لتقنية المعلومات. وتطبق هذه المتطلبات على جميع الجهات الحكومية التي تقدم خدمات ومنتجات رقمية، والجهات المشغلة لخدمات تقنية المعلومات ومزودي الخدمات الرقمية.

هذه المعايير ليست نظرية بل تُطبق ميدانياً في السوق السعودي. **فالهئية الوطنية للأمن السيبراني تقوم بتدقيق دوري عبر منصة حصين لضمان التزام الجهات الحكومية. بينما هيئة الحكومة الرقمية توّجّد سياسات الحوكمة عبر ضوابط تقنية المعلومات.**

هذه الأطر التنظيمية تعكس الهوية السعودية القائمة على الحوكمة الرشيدة وتضمن أن أي مؤسسة سعودية تتحول رقمياً تفعل ذلك في إطار يوازن بين الأمن، الشفافية، وخدمة المواطن.





نشاط (4)

هدف النشاط	أن يطور المشاركون توصيات واقعية لتحسين وتطوير مبادرات التحول الرقمي.
المدة الزمنية المتوقعة	زمن النشاط (10) دقيقة.
أسلوب النشاط	نشاط جماعي.

المطلوب:

قم بتعبئة الجدول الموجود أدناه بكتابة التوصيات المقترحة ليتم مشاركتها مع منظمة الأربوساي

جدول التوصيات المقترحة:

التوصية 1	بناء القدرات والابتكار الآمن: تطوير برامج تدريب مستمرة في المهارات الرقمية والذكاء الاصطناعي وتحليل البيانات والأمن السيبراني، مع التوسع الآمن في التقنيات الناشئة وتبادل الخبرات بين الأجهزة الرقابية في منظمة الأربوساي.
التوصية 2	استقلال الأمن السيبراني: إنشاء إدارة مستقلة للأمن السيبراني وفصلها تنظيميًا وإداريًا عن تقنية المعلومات والتحول الرقمي؛ لضمان استقلالية الرقابة والحد من تعارض المصالح.
التوصية 3	التحول والنضج الرقمي: إعداد خارطة طريق للتحويل الرقمي تبدأ بقياس النضج وتحديد الفجوات والأولويات، مع أتمتة العمليات وقياس أثر المبادرات والتحسين المستمر.
توصية 4	تجهيز دليل لتقييم تقنية المعلومات استناداً لآطار عمل (COBIT) قبل التدقيق لنشر الوعي في الجهات الخاضعة للرقابة.
توصية 5	تفعيل دور الرقابة الداخلية للتدقيق على تقنية المعلومات والأمن السيبراني.
توصية 6	اعتماد سياسة واضحة لحوكمة وأخلاقيات استخدام الذكاء الاصطناعي وتحليل البيانات في العمل الرقابي، مع ضمان أعلى معايير سرية وحماية البيانات الحكومية والمواطنين.



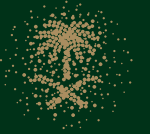
التوصيات





المركز السعودي للمراجعة
المالية والرقابة على الأداء

الديوان العام للمحاسبة
GENERAL COURT OF AUDIT



شكرا

