وزارة النقل والاتصالات وتقنية المعلومات
Ministry of Transport, Communications and Information Technology

الدليل الاسترشادي لسياسة إدارة مخاطر تقنية المعلومات

فبراير 2026 م

نصل العالم
Connecting the world

@mtcitoman

جدول المحتويات

1.المقدمة

تعد إدارة مخاطر تقنية المعلومات من الركائز الأساسية للحفاظ على سلامة وأمن الأصول الرقمية في الوحدات الحكومية، يهدف هذا الدليل إلى توفير هيكل منهجي شامل يمكن من التعرف المبكر على المخاطر المرتبطة بتقنية المعلومات وتقييمها، ثم اتخاذ الإجراءات الوقائية المناسبة للحد من تأثيرها على سير الأعمال. كما يسعى الدليل إلى تعزيز الوعي المؤسسي بأهمية المخاطر التقنية، ورفع مستوى الجاهزية للتعامل مع المخاطر.

2.الاهداف

1. توضيح منهجية تطبيق سياسة ادارة مخاطر تقنية المعلومات.
2. التوافق مع المعايير والممارسات الدولية وأفضل النماذج في مجال ادارة المخاطر.
3. تطوير استراتيجيات واجراءات فعالة للحد من المخاطر ومعالجتها
4. حماية سرية وسلامة توافر البيانات والأصول الرقمية.
5. دعم اتخاذ القرارات المستندة الى تقييم المخاطر لتحسين الأداء التشغيلي والاستراتيجي.

3.الغرض

توفير دليل استرشادي عملي يسهم في تطبيق إدارة مخاطر تقنية المعلومات بفعالية في الوحدات الحكومية، مع دعم الجاهزية المؤسسية للتصدي السريع للحوادث الأمنية وضمان استمرارية الخدمات.

4.المبادئ العامة

تطبق سياسة إدارة المخاطر في الجهات المشموله استنادا الى المبادئ التالية:

1. التكامل: تدمج إدارة المخاطر ضمن استراتيجية تقنية المعلومات للوحدة.
2. الاستباقية: تمارس إدارة المخاطر بطريقة وقائية لتقيل الأثر قبل وقوع المخاطر.
3. الواقعية: تقيم المخاطر بناءا على تحليل موضوعي مبني على بيانات دقيقة.
4. التناسب: تحدد الضوابط والاجراءات بما يتناسب مع درجة الخطورة
5. التحسين المستمر: تراجع إدارة المخاطر وتحدث بصفة مستمرة لضمان فعاليتها ومواكبتها للتغيرات.

5.الهيكل الحوكمي للدليل الاشترشادي:

5.1تحديد الأدوار والمسؤوليات

- **الإدارة العليا:**
  - اعتماد سياسة إدارة المخاطر والإشراف على تنفيذها.
  - تخصيص الموارد اللازمة لإدارة المخاطر.
  - مراجعة تقارير المخاطر واتخاذ القرارات الاستراتيجية اللازمة.
  - تعزيز ثقافة الوعي بأهمية إدارة المخاطر في الوحدة.
  - تعيين نقطة اتصال رسمية مع الجهات الوطنية المعنية بالأمن السيبراني وإدارة المخاطر التقنية.
- **فريق إدارة المخاطر:**
  - التعرف المستمر على المخاطر التقنية وتقييمها وتصنيفها.
  - تطوير خطط الاستجابة وإجراءات التخفيف من المخاطر.
  - متابعة تنفيذ ضوابط وتقنيات إدارة المخاطر.
  - إعداد تقارير دورية للإدارة العليا حول حالة المخاطر والإجراءات المتخذة.
- **فريق تقنية المعلومات:**
  - تنفيذ الضوابط التقنية الموصى بها لمعالجة المخاطر المحددة.
  - مراقبة الأنظمة والتطبيقات لاكتشاف أي ثغرات أو تهديدات.
  - دعم عمليات التقييم الفني للحوادث الأمنية.

نموذج جدول الأدوار والمسؤوليات لإدارة مخاطر تقنية المعلومات ((RACI Matrix))

النشاط/المسؤولية	فريق إدارة المخاطر	فرق تقنية المعلومات	الإدارة العليا	الجهات الوطنية المختصة
تحديد وتقييم المخاطر	مسؤول	مستشار	إعلام	-
تطوير خطط التخفيف	مسؤول	مشارك	إعلام	-
تنفيذ الضوابط التقنية	مستشار	مسؤول	إعلام	-
مراقبة الحوادث والتهديدات	مشارك	مسؤول	إعلام	-
تصعيد المخاطر الحرجة	مسؤول	مشارك	مشارك	-
اتخاذ قرارات استراتيجية	إعلام	إعلام	مسؤول	-

التنسيق مع الجهات الوطنية المختصة	إعلام	إعلام	مشارك	مسؤول

5.2آليات التبليغ عن المخاطر ذات الأولوية

- وضع آلية واضحة لتصنيف المخاطر حسب أولويتها بناءا على تأثيرها واحتمالية حدوثها.
- تحديد نظام داخلي للتبليغ عن المخاطر الحرجة (مثل منصة إلكترونية أو نموذج تقارير موحدة) بشكل فوري إلى الجهات المختصة داخل الوحدة.
- تحديد مستويات التصعيد بدءا من فريق إدارة المخاطر مروراً بفرق تقنية المعلومات وصولا إلى الإدارة العليا والجهات الوطنية المختصة.
- اعتماد نماذج وتقارير موحدة لتوثيق وتقييم المخاطر والإجراءات المتخذة.

نموذج اجراءات تصعيد والتبليغ عن المخاطر

رقم البلاغ	تاريخ البلاغ	وصف المخاطر	مستوى الخطورة	الإجراءات المتخذة	المسؤول عن المعالجة	تاريخ الاستجابة	الحالة
1	2025-08-12	اختراق نظام البريد الإلكتروني	حرِج	عزل النظام، تغيير كلمات المرور	فريق تقنية المعلومات	2025-08-12	جاري المعالجة
2	2025-08-11	تأخر تحديث نظام الحماية	متوسط	جدولة التحديث فورا	فريق إدارة المخاطر	2025-08-12	تم التنفيذ
3	2025-08-10	فقدان بيانات غير مصنفة	عالي	استعادة النسخة الاحتياطية	فريق تقنية المعلومات	2025-08-11	تحت المراجعة

5.3آليات التنسيق مع الجهات الوطنية المختصة

- تبادل المعلومات والتقارير المتعلقة بالتهديدات الأمنية والمخاطر التقنية.
- المشاركة في المبادرات الوطنية وبرامج التوعية والتدريب لتعزيز القدرات المؤسسية.
- الالتزام بالمتطلبات واللوائح الوطنية ذات الصلة، وضمان تحديث السياسات والإجراءات وفقًا للتوجيهات الحكومية.

6.تصنيف الأصول التقنية

6.1فئات الأصول التقنية

- الأصول المادية (Hardware) :
تشمل أجهزة الحاسوب، الخوادم، أجهزة الشبكة، وحدات التخزين، وأجهزة الاتصال.
- الأصول البرمجية (Software) :
تشمل أنظمة التشغيل، تطبيقات المؤسسة، البرامج الوسيطة، والأدوات البرمجية.
- البيانات (Data) :
تشمل قواعد البيانات، الملفات الإلكترونية، المعلومات الحساسة، وبيانات العملاء.
- الشبكات (Network):
تشمل البنية التحتية للشبكات، أجهزة التوجيه(Routers) ، الجدران النارية(Firewalls) ، ونقاط الوصول
- الخدمات التقنية (Services) :
تشمل خدمات الاستضافة، الخدمات السحابية، قواعد البيانات المستضافة، وخدمات الدعم الفني.

6.2معايير تصنيف الأصول التقنية

يتم تصنيف الأصول بناءا على معايير مثل:

- الأهمية :مدى تأثير فقدان أو تلف الأصل على الأعمال.
- الحساسية :درجة حساسية المعلومات أو البيانات المرتبطة بالأصل.
- القابلية للاستبدال :مدى سهولة استبدال الأصل أو استعادته.
- الاعتمادية :مدى اعتماد العمليات الحيوية على الأصل.
- القيمة المالية :التكلفة المالية للأصل أو تكلفة استبداله.

نموذج لمستويات تصنيف الأصول التقنية

الفئة	الوصف	أمثلة
أصول حرجة	أصول تؤثر بشكل مباشر على استمرارية الأعمال وسلامة البيانات الحساسة	أنظمة الدفع الإلكتروني، قواعد بيانات العملاء
أصول حساسة	أصول تحتوي على معلومات سرية تتطلب حماية عالية	بيانات الموظفين، تطبيقات داخلية حساسة
أصول مهمة	أصول تدعم العمليات الأساسية لكنها أقل حساسية	الخوادم الأساسية، برامج الإنتاج
أصول عادية	أصول ذات تأثير منخفض على الأعمال ولا تحتوي على معلومات حساسة	الحواسيب المكتبية العامة، البرامج العامة

6.3خطوات عملية لتصنيف الأصول التقنية

1. جرد الأصول :إعداد قائمة شاملة بكل الأصول التقنية في الوحدة.
2. تقييم الأصول :تقييم كل أصل وفق المعايير السابقة (الأهمية، الحساسية، القيمة).
3. تعيين فئة التصنيف :وضع كل أصل ضمن إحدى فئات التصنيف.
4. توثيق النتائج :إنشاء سجل مركزي لتصنيف الأصول مع تحديث دوري.
5. تطبيق الضوابط الأمنية :تحديد الإجراءات الأمنية المناسبة لكل فئة حسب درجة التصنيف.

نموذج جرد وتصنيف الأصول التقنية

رقم الأصل	اسم الأصل	نوع الأصل	وصف مختصر	القيمة المالية	الحساسية (منخفض، متوسط عالي)	الأهمية (حرجة، مهمة، عادية)	الموقع /القسم	المسؤول عن الأصل	الاجراءات
001	خادم قواعد البيانات	مادي/برمجي	خادم يستضيف قاعدة بيانات العملاء	50,000 ريال	عالي	حرجة	مركز البيانات	فريق تقنية المعلومات	يتطلب حماية عالية
002	تطبيق الحضور والانصراف	برمجي	نظام داخلي لإدارة حضور الموظفين	10,000 ريال	متوسط	مهمة	قسم الموارد البشرية	مدير النظام	تحديث شهري
003	شبكة الإنترنت الداخلية	شبكة	LANتربط جميع أجهزة الشركة	30,000 ريال	متوسط	مهمة	مركز الشبكات	مسؤول الشبكة	صيانة دورية

7.منهجية ادارة المخاطر

1. تحديد الأصول التقنية

- اختيار الأصول المستهدفة للتحليل بناءا على نتائج جرد وتصنيف الأصول.

2. التهديدات ونقاط الضعف

- حصر التهديدات المحتملة (مثل الهجمات السيبرانية أو الأعطال).
- تحديد نقاط الضعف في الأصول (مثل ضعف التحديثات أو سوء الإعدادات).

3. تحليل المخاطر

- نوعي :تقييم الاحتمالية والأثر اعتمادًا على خبرة الفرق.
- كمي :تقدير الخسائر المحتملة رقميا (مالية أو تشغيلية).

4. تقييم المخاطر وتحديد الأولويات

- استخدام مصفوفة المخاطر لتحديد مستوى الخطورة واحتمالية وقوعها (impact vs .likelihood).
- تصنيف المخاطر إلى: منخفضة – متوسطة – عالية – حرجة.

5.معالجة المخاطر

- التخفيف :تقليل الاحتمالية أو الأثر.
- التحويل :نقل الخطر لطرف آخر أو التأمين.
- القبول :إذا كان الخطر ضمن المستوى المقبول.
- التجنب :إيقاف النشاط المسبب للخطر.

6. الموافقة والإشراف

- اعتماد نتائج التقييم وخطة المعالجة من الإدارة العليا.
- تحديد فرق التنفيذ والمتابعة.

7.المراقبة والمراجعة المستمرة

- مراجعة دورية للمخاطر وتحديث التقييم عند حدوث تغييرات.

8. التوثيق والتقارير

- حفظ جميع النتائج في سجل المخاطر.
- إعداد تقارير دورية ورفعها للإدارة العليا

8.ضوابط التحكم والحماية

تعد ضوابط التحكم والحماية في الأصول جزءا أساسيا من إدارة المخاطر لضمان حمايتها وتقليل الاحتمالية أو الأثر الناتج عن المخاطر وتنقسم إلى ثلاثة أنواع رئيسية:

8.1الضوابط التقنية:

- تشفير البيانات أثناء التخزين والنقل لضمان السرية وسلامة المعلومات.
- التحكم في الوصول وصلاحيات المستخدمين، بما في ذلك استخدام المصادقة متعددة العوامل.
- إجراء النسخ الاحتياطي الدوري للبيانات والأنظمة لضمان استمرارية العمل.
- العزل الشبكي للأنظمة والخدمات الحساسة لتقليل التأثير في حال حدوث أي خرق أمني.

8.2 الضوابط الإجرائية:

- إجراء التدقيق الدوري على الأنشطة والتغييرات في الأنظمة للتأكد من الالتزام بالسياسات والإجراءات.
- مراجعة الضوابط والإجراءات بشكل دوري للتأكد من فعاليتها ومواكبتها للتغيرات في بيئة العمل والمخاطر.

8.3ضوابط الموردين والمتعاقدين:

- تضمين متطلبات وضوابط أمنية واضحة في العقود والاتفاقيات مع الموردين والمتعاقدين.
- تقييم الموردين والمتعاقدين بشكل دوري للتحقق من التزامهم بالضوابط الأمنية.
- متابعة ومراقبة الأنشطة التي يقوم بها الموردون لضمان عدم تأثيرها على أمان البيانات والأنظمة.

9.التكامل مع استمرارية الأعمال:

يهدف التكامل بين إدارة المخاطر واستمرارية الأعمال وخطط التعافي من الكوارث إلى ضمان جاهزية الوحدة لمواجهة الأحداث الطارئة والتقليل من تأثيرها على العمليات الحيوية. ويشمل ذلك ما يلي

- تضمين نتائج تقييم المخاطر في خطط BCP/DRP لتحديد الأصول الحرجة والعمليات الحيوية وحمايتها.
- مواءمة الإجراءات بين خطط إدارة المخاطر وخطط الاستمرارية، مثل النسخ الاحتياطية، التكرار الجغرافي (المواقع الرديفة أو البديلة) ونقاط الاستعادة.

- تحديد المسؤوليات المشتركة لفرق إدارة المخاطر، الاستمرارية، وتقنية المعلومات لضمان استجابة منسقة.
- إجراء اختبارات محاكاة دورية (سنوياً أو نصف سنوي) لأحداث مثل الانقطاع المفاجئ أو الهجمات السيبرانية، وتحديث الخطط بناءا على النتائج لمعالجة أية نقاط ضعف.

نموذج لمصفوفة المخاطر مقابل إجراءاتBCP/DRP

نوع المخطر	تأثيره على الأعمال	مستوى الخطورة	الإجراءات الوقائية(BCP)	إجراءات التعافي (DRP)	المسؤول / الفريق
اختراق البريد الالكتروني	توقف التواصل الداخلي	حرِج	-نسخ احتياطية يومية للبريد - مراقبة البريد واكتشاف الأنشطة المشبوهة - تدريب المستخدمين	-استعادة النظام من النسخ الاحتياطية - تغيير كلمات المرور - تفعيل خطة بديلة للتواصل	تقنية المعلومات
انقطاع الكهرباء	توقف الخوادم والتطبيقات	عالي	-وحدات UPS لكل الخوادم - مولد كهرباء احتياطي - مراقبة مستمرة للتيار الكهربائي	-تشغيل المولد الاحتياطي - نقل العمليات الحرجة إلى مركز بيانات بديل	تقنية المعلومات
فقدان بيانات حساسة	خرق السرية وتأثر العمليات	عالي	-تشفير البيانات - نسخ احتياطية دورية واحتفاظ بنسخ خارجية - سياسة إدارة الوصول	-استعادة النسخ الاحتياطية - إشعار الإدارة العليا	تقنية المعلومات

				-مراجعة الاسباب وتحديث الإجراءات	
هجوم DDoS	توقف الخدمة أو بطء الأداء	عالي	-جدران حماية متقدمة - مراقبة حركة الشبكة - إعداد خطط للحماية من هجماتDDoS	-تفعيل خطط الطوارئ - استخدام خدمات الحماية الخارجية أو النسخ الاحتياطية	الأمن السيبراني
فشل الأنظمة الحرجة	توقف العمليات الأساسية	حرج	-صيانة دورية للأنظمة - تحديث البرمجيات والتطبيقات - اختبار مستمر للأنظمة	-تفعيل الأنظمة البديلة - استعادة البيانات والإعدادات	تقنية المعلومات
انقطاع الشبكة (Network Outage)	توقف الاتصالات والأنظمة المعتمدة على الشبكة	عالي	-استخدام شبكة بديلة - إعادة جدولة الأنشطة الحيوية	-استعادة الأنظمة من النسخ الاحتياطية - إعادة تشغيل الخوادم	البنية التحتية / تقنية المعلومات
تعطل التطبيقات الحيوية (App Failure)	تعطل العمليات المرتبطة بالتطبيق	متوسط	-اختبار التطبيقات بشكل دوري -إعادة توجيه العمليات لتطبيقات بديلة	- إعادة تثبيت التطبيقات -استعادة البيانات من النسخ الاحتياطية -اختبار الوظائف بعد الاستعادة	تقنية المعلومات

			- خطط تشغيل يدوية مؤقتة		
كوارث طبيعية (Natural Disasters)	توقف شامل للعمليات والبنية التحتية	حرج	-نقل العمليات لمواقع بديلة -التأكد من جاهزية الموظفين	-استعادة البنية التحتية - نقل البيانات والمعدات -تشغيل الموقع الاحتياطي	إدارة الطوارئ / تقنية المعلومات

10.المتابعة والتحسين المستمر

10.1مراجعة وتحديث سجل المخاطر

- اجراء مراجعات دورية (مثال كل ثلاثة أشهر) لضمان تقييم وتصنيف المخاطر الجديدة أو المعدلة بشكل صحيح.
- تحديث سجل المخاطر لإضافة أي خطر جديد أو تعديل تقييم المخاطر القائمة نتيجة التغيرات في البنية الأساسية، العمليات، أو البيئة التقنية.
- توثيق كل تعديل أو إضافة مع ذكر المسؤول عن التحديث وتاريخ التغيير.

10.2 تحسين الضوابط

- مراجعة الحوادث السابقة لتحديد نقاط الضعف.
- تعديل الضوابط التقنية والإجرائية، إضافة أدوات حماية جديدة، وتحسين إجراءات النسخ الاحتياطي.
- تقييم فعالية الضوابط بعد التحديث وتوثيق النتائج لضمان تقليل الاحتمالية والأثر كما هو مخطط

11.التقارير والتوثيق:

11.1إعداد سجل مخاطر مركزي

- جمع كافة المخاطر المكتشفة، نتائج التقييم، وخطط المعالجة في نظام أو جدول مركزي قابل للبحث والتحليل.
- التأكد من تحديث السجل بانتظام بعد كل مراجعة أو عند إضافة خطر جديد.
- تمكين الفرق المختصة من الوصول إلى السجل لاتخاذ قرارات مدروسة وفي الوقت المناسب.

11.2تقديم تقارير دورية

- للإدارة العليا :تقارير ملخصة تشمل مستوى المخاطر، الإجراءات المتخذة، وأي مخاطر حرجة تحتاج اهتمام القيادة.
- للجهات الرقابية :توفير البيانات المطلوبة وفق اللوائح الوطنية، مثل التزام الوحدة بمعايير الأمن السيبراني وإدارة المخاطر.
- الجدول الزمني للتقارير :شهرية، ربع سنوية، وسنوية حسب حجم الوحدة وحساسية الأصول.

11.3توثيق إجراءات المعالجة والاستجابة

- تسجيل جميع الخطوات والإجراءات الفنية والإجرائية لمعالجة كل خطر، مع توثيق الأدلة والمستندات المرتبطة بها.
- التأكد من أن كل خطوة قابلة للمراجعة والتتبع لضمان الشفافية والالتزام بالسياسات.
- يمكن إعداد نماذج إجراءات جاهزة لكل نوع من المخاطر لتسهيل عملية التوثيق وتوحيدها بين الفرق.

12.إدارة الوثيقة

1. تعود ملكية هذه الدليل إلى وزارة النقل والاتصالات وتقنية المعلومات وسيخضع للمراجعة كلما اقتضت الحاجة ذلك.

13.مراجع ذات صلة

- ISO/IEC 27001:2022
- ISO/IEC 27005:2018
- ISO 22301:2019
- ISO 31000:2018
- NIST SP 800-30 Rev.1 (2012)
- NIST SP 800-37 Rev.2 (2018)
- COBIT 2019 Framework
- إطار حوكمة وادارة البيانات الوطنية 2025م – وزارة النقل والاتصالات

ملحق: المصلحات والتعاريف

الوزارة	وزارة النقل والاتصالات وتقنية المعلومات
المخاطر	أحداث أو ظروف غير متوقعة ناتجة عن تهديدات أو ثغرات في الأنظمة أو العمليات أو الموارد التقنية، وقد تؤثر سلبًا على سرية أو سلامة أو توفر المعلومات أو على استمرارية الأعمال وتحقيق الأهداف التشغيلية والتنظيمية
إدارة المخاطر	عملية منهجية لتحديد المخاطر وتحليلها وتقييمها ومعالجتها ومراقبتها ومراجعتها، بهدف تقليل تأثيرها السلبي المحتمل على الأفراد أو الأصول أو الأنظمة أو العمليات، وتعزيز القدرة على تحقيق الأهداف المؤسسية بفعالية وكفاءة
الانظمة الحرجة	الأنظمة التقنية أو المعلوماتية التي يؤدي تعطلها أو اختراقها أو فقدانها أو إساءة استخدامها إلى تأثيرات جسيمة على استمرارية الأعمال، أو سلامة الأفراد، أو الأمن الوطني، أو تقديم الخدمات الحيوية، أو الامتثال التنظيمي.
الانظمة الحساسة	الأنظمة التقنية أو المعلوماتية التي تحتوي أو تعالج أو تنقل بيانات أو معلومات تتطلب حماية خاصة بسبب حساسيتها أو طبيعتها الخاصة، مثل البيانات الشخصية، أو المالية، أو الصحية، أو أي معلومات قد يؤدي كشفها أو تغييرها أو الوصول غير المصرح به إليها إلى أضرار قانونية أو تنظيمية أو تشغيلية.
الانظمة الاعتيادية	أنظمة تقنية أو معلوماتية لا تحتوي على معلومات حساسة أو سرية، ولا يعتمد عليها في تقديم خدمات حيوية أو مهام تشغيلية حرجة. ويؤدي تعرضها للخطر إلى تأثير محدود يمكن التحكم فيه دون تأثير كبير على استمرارية الأعمال أو الأمن أو الامتثال التنظيمي.
التحليل النوعي	عملية تقييم للمخاطر تعتمد على الأساليب غير الرقمية (غير الكمية)، وتركز على الوصف والتصنيف والتقدير النسبي لاحتمالية حدوث

	المخاطر وتأثيرها باستخدام مقاييس وصفية أو مرجعية (مثل: منخفض، متوسط، مرتفع)، بهدف تحديد أولويات الاستجابة للمخاطر
التحليل الكمي	احدى الأدوات الأساسية في إدارة مخاطر تقنية المعلومات، ويهدف إلى تقديم تقديرات عددية دقيقة للاحتمالية والأثر المالي للمخاطر. وتستخدم فيه الأساليب الرياضية والإحصائية لدعم عملية اتخاذ القرار بشأن أولويات المعالجة وتخصيص الموارد.
سجل المخاطر	وثيقة رسمية تحتفظ بها الوحدة تسجل فيها جميع المخاطر المكتشفة وتحليلها وخطط معالجتها
المخاطر الحرجة	المخاطر التي قد تؤدي إلى توقف الخدمات الوطنية أو تهدد الأمن السيبراني الوطني
ضوابط تقنية	تتمثل في الإجراءات والأدوات التقنية التي تطبق مباشرة على الأنظمة والأصول لحمايتها
التشفير	حماية البيانات المخزنة والمنقولة باستخدام تقنيات تشفير قوية لضمان السرية وسلامة البيانات.
التحكم في الوصول	تحديد وضبط من يمكنه الوصول إلى البيانات والأنظمة، بما في ذلك إدارة الصلاحيات والمصادقة متعددة العوامل
النسخ الاحتياطي	إجراء نسخ احتياطية دورية للبيانات والأنظمة لضمان استمرارية العمل في حالة حدوث أعطال أو فقدان للبيانات
العزل الشبكي	تقسيم الشبكات وفصل الأنظمة الحساسة لتقليل تأثير الهجمات أو الأعطال على باقي الأصول.
ضوابط إجرائية	تشمل السياسات والإجراءات المتبعة لضمان الالتزام بالمعايير الأمنية والإشراف على الأنشطة.
التدقيق	مراجعة الأنشطة والتغييرات على الأنظمة لتحديد أي انحرافات أو خروقات محتملة.

المراجعات الدورية	تقييم دوري للضوابط والإجراءات لضمان فعاليتها ومواكبتها للتغيرات في بيئة العمل والمخاطر
الاصول التقنية	كافة الموارد الرقمية والمكونات التقنية التي تستخدمها الوحدة لدعم أعمالها، وتشمل الأجهزة، البرمجيات، البيانات، الشبكات، والخدمات الرقمية.