# معايير التقييم

| النجاح | التفوق | الامتياز |
|---|---|---|
| نتائج التعلم أ فهم تهديدات الأمن السيبراني وثغرات النظام وأساليب الحماية الأمنية | | |
| **A.P1**<br>شرح تهديدات الأمن السيبراني المختلفة التي يمكن أن تؤثر في أنظمة تكنولوجيا المعلومات في المؤسسات.<br>**تمرين تقييمي 11.1**<br>**A.P2**<br>شرح ثغرات النظام التي يمكن أن تؤثر في أنظمة تكنولوجيا المعلومات في المؤسسات.<br>**تمرين تقييمي 11.1**<br>**A.P3**<br>شرح الكيفية التي يمكن بها للمؤسسات استخدام تدابير أمان البرامج والأجهزة لمواجهة التهديدات الأمنية.<br>**تمرين تقييمي 11.1** | **A.M1**<br>تقييم الأثر الذي يمكن أن تسببه تهديدات الأمن السيبراني في أنظمة تكنولوجيا المعلومات في المؤسسات مع مراعاة المتطلبات القانونية.<br>**تمرين تقييمي 11.1** | **AB.D1**<br>تقييم فعالية التدابير المستخدمة لحماية المؤسسات من تهديدات الأمن السيبراني مع مراعاة المتطلبات القانونية.<br>**تمرين تقييمي 11.1**<br>**تمرين تقييمي 11.2** |

**أولًا: الفكرة الكبرى**

نتائج التعلّم (أ) :**فهم تهديدات الأمن السيبراني وثغرات النظام وأساليب الحماية.**
المستويات:

- **النجاح**A.P3 + A.P2 + A.P1 :
- **التفوّق**A.M1 :
- **الامتياز**AB.D1 :

**— A.P1وصف التهديدات (مستوى النجاح)**

**شو مطلوب؟** تعرّف وتشرح التهديدات اللي بتواجه مؤسسات/أنظمة تقنية المعلومات، وبأمثلة واقعية.

**كيف تجاوب؟ (قالب قصير يتكرّر لكل تهديد):**

1. اسم التهديد) :تصيّد، برمجيات خبيثة، فدية، هجمات كلمة مرور، DoS، اختراق داخلي، هندسة اجتماعية، ثغرات تحديثات... إلخ(
2. كيف بصير؟ (قناة الهجوم/المدخل)
3. شو بستهدف؟) السرّية/السلامة/التوفّر(CIA –
4. أثر سريع على المؤسسة (مثال صغير من بيئة مدرسة/شركة/مستشفى).

**مثال سريع (واحد من كتير):**

- التهديد: التصيّد الاحتيالي
- كيف بصير: إيميل مزوّر يطلب "تحديث كلمة السر"

- يستهدف :**السرّية** )سرقة الحساب(
- أثر: دخول لحساب الموظف، تسريب ملفات طلاب/عملاء.

كرّر نفس القالب على 6–8 تهديدات متنوعة، هيك تضمن A.P1 بكاملها.

**— A.P2تفسير الأثر على أمن النظام (لسّا نجاح)**

**شو مطلوب؟** تربط **كل تهديد** بأثره التقني والعملي على النظام/العمل.

**كيف تجاوب؟**

- لكل تهديد من:A.P1
  - شو بصير للنظام؟ (تعطّل خدمة، فساد بيانات، تسريب، تباطؤ الشبكة...)
  - شو الأثر على العمل؟ (توقّف الدوام، خسائر، سمعة، مخالفات قانونية)
  - مؤشرات اختراق Inbox) فيه رسائل مرتدة، زيادة ترافيك، تنبيهات مضاد الفيروسات.(...

**— A.P3كيف بنواجه التهديدات (ضوابط وحماية) (لسّا نجاح)**

**شو مطلوب؟** تذكر **إجراءات الحماية** اللي المؤسسات بتستخدمها.

**رتّب الضوابط بثلاث طبقات (إكتب أمثلة محددة):**

- **تقنية** :جدار ناري، مضاد فيروسات، تصفية بريد، MFA، تشفير، نسخ احتياطي، تحديثات...
- **إجرائية/إدارية** :سياسات كلمات مرور، إدارة صلاحيات، خطط استجابة للحوادث، تدريب موظفين.
- **فيزيائية** :أقفال، كاميرات، التحكم بالدخول لغرف السيرفر.

لكل تهديد اكتب "الضبط الأنسب" + سطر ليش هو الأنسب.

---

**— A.M1تقييم المخاطر مع مراعاة المتطلبات القانونية (التفوّق)**

**شو مطلوب؟** تعمل **تقييم مخاطر** حقيقي: احتمال × أثر، وتلمّح للالتزام القانوني (مثل خصوصية البيانات وقانون الجرائم الإلكترونية في بلدك).

**كيف تجاوب؟ (خُطّة مختصرة):**

1. **جدول مخاطر** )اعمل 5–7 صفوف من أقوى التهديدات لديك:(
   - التهديد | الأصل/الأصول المتأثرة | احتمال (منخفض/متوسط/عالٍ) | أثر | **درجة الخطر** (مثلاً 1–5 × 1–5) | ضوابط موجودة | فجوات.
2. **تحليل** :ليش هاد عالي؟ شو الدليل/المؤشرات؟

3. **قانون/سياسات** :إذا عندك بيانات شخصية/طلابية/مرضى ← ضرورة حماية الخصوصية، حفظ السجلات، موافقات، إلخ.
4. **أولويات** :رتّب المخاطر من الأعلى للأقل مع سبب.

**مثال مختصر من الجدول:**

- رانسوموير | ملفات الشركة | احتمال: م | أثر: ع | الدرجة: 25/12 | موجود: نسخ أسبوعي | فجوة: ما في عزل نسخ/لا MFA للبريد.

---

**— AB.D1تقييم فاعلية التدابير مع توصيات مُحكَمة (الامتياز)**

**شو مطلوب؟** تحكيم مهني: هل التدابير الحالية **فعّالة فعلًا؟** وبعدين توصي بتحسينات **مبرّرة** ومراعية للقانون والتكلفة.

**كيف تجاوب؟**

1. **قياس الفاعلية** لكل ضبط مهم:
   - التغطية (قديش مغطّي التهديدات؟)
   - سرعة الكشف (MTTD) وسرعة المعالجة(MTTR)
   - نتائج اختبارات (فحص اختراق/محاكاة تصيّد).
2. **ثغرات** :أين الفشل؟ (مثال: جدار ناري ممتاز، بس ما في تدريب موظفين ← التصيّد لسه بيمرّ).
3. **توصيات مرتّبة حسب العائد** ← Quick wins)مشاريع:(
   - قصير: تفعيلMFA ، فلترة بريد متقدّمة، سياسة كلمات سر + تدريب عاجل.
   - متوسط: نسخ احتياطي مع **عزل** +اختبارات استعادة، إدارة تصحيحات تلقائية.
   - طويل SIEM/SOC :مصغّر أو تعهيد مراقبة، تصنيف بيانات وسياسة احتفاظ.
4. **ربط قانوني/سياساتي** :كيف كل توصية تقلّل احتمال مخالفة أو غرامة.
5. **خلاصة قوية"** :بالحالة الحالية الخطر المتبقّي ← High بعد تنفيذ 1–3 بصير."...Medium

---

**كيف "تحلّ" تمرين 11.1 و 11.2 عمليًا**

**تمرين تقييمي 11.1) عادةً يغطّي A.P3 + A.P2 + A.P1 وربما(A.M1**

**اكتب تقريرًا قصيرًا من 2–4 صفحات** بالترتيب التالي:

1. **مقدّمة** :تعريف الأمن السيبراني + نطاق المؤسسة الافتراضية (مدرسة/شركة صغيرة).
2. **قائمة تهديدات** 8–6 :**(A.P1)** تهديدات بصيغة القالب المذكور.

3. **أثر التهديدات :(A.P2)** فقرة/جدول يربط كل تهديد بتأثير تقني وتشغيلي.
4. **ضوابط الحماية :(A.P3)** مصفوفة "تهديد ← الضبط المناسب + سبب الاختيار."
5. **لمسة تقييم مخاطر خفيفة A.M1) إن طلب :(**جدول احتمال/أثر بسيط وخاتمة أولويات.

**تمرين تقييمي 11.2) عادةً يرفعك للامتياز(AB.D1**

**اكتب ملحقًا احترافيًا (1–2 صفحة):**

- **تقييم فاعلية** الضوابط الحالية بأرقام أو تقديرات (تغطية%، زمن كشف/استجابة تقديري).
- **ثلاث توصيات ذهبية** مبررة (الأثر على الخطر، الكلفة، الزمن، الالتزام).
- **خلاصة** :كيف التوصيات بتخفّض الخطر المتبقّي ولماذا هي أولى.

---

**نموذج فقرات جاهزة (انسخ وكيّف على مؤسستك)**

**مقدّمة قصيرة:**
"تهدف هالتقرير لتحديد أبرز تهديدات الأمن السيبراني التي قد تواجه قسم تقنية المعلومات في [اسم المؤسسة]، وشرح أثرها على السرّية والسلامة والتوفّر، مع اقتراح ضوابط مناسبة وتقويم فاعليتها بما يراعي المتطلبات القانونية المحلية".

**تهديد + أثر + ضبط (نموذج واحد):**

- التهديد: هجوم كلمات المرور.(Brute Force)
- الأثر: تعطيل حسابات حرجة، احتمال اختراق بريد إداري، تسريب بيانات.
- الضوابط: تفعيلMFA ، سياسة كلمات سر قوية + قفل تلقائي بعد محاولات فاشلة، مراقبة سجلات الدخول.
- لماذا هذي الضوابط؟ MFA يكسر سلسلة الهجوم حتى لو انكشفت الكلمة؛ القفل يقلّل فرص التخمين؛ المراقبة تكشف الأنماط بسرعة.

**تقييم فاعلية مختصر:(AB.D1)**
"على الرغم من وجود سياسة كلمات سر، عدم تفعيل MFA يترك خطرًا متبقّيًا عاليًا. بتفعيل MFA خلال أسبوعين وتطبيق قفل الحساب بعد 5 محاولات، نتوقّع خفض حوادث الدخول غير المصرّح به بنسبة ملحوظة، وتقليل زمن الاستجابة إلى أقل من ساعتين".

---

**أخطاء شائعة (إبعد عنها):**

- سرد عام بدون **سيناريو مؤسسي** واضح.
- ذكر ضوابط بدون "ليش هذا مناسب."
- نسيان ربط التهديد بـ **CIA**والأثر العملي.

- خلط بين "وصف" و"تقييم.(A.P vs A.M/AB) "

**تشيك ليست سريعة قبل التسليم**

- 6–8تهديدات موصوفة بوضوح(A.P1)
- أثر تقني + تشغيلي لكل تهديد(A.P2)
- ضوابط مناسبة مع تبرير مختصر(A.P3)
- جدول مخاطر احتمال×أثر + أولويات(A.M1)
- قياس فاعلية + توصيات مرتّبة ومبرّرة(AB.D1)