تقرير نموذجي · منشأة افتراضية

INSPECTION, TESTING & ASSURANCE

ISO/IEC 27001

تقرير تقييم الفجوات

نظام إدارة أمن المعلومات ISO/IEC 27001:2022

شركة الواحة للخدمات اللوجستية (نموذج)

المقر الرئيسي ومستودعان إقليميان ومنصة طلبات العملاء الإلكترونية

تاريخ التقييم	16 نوفمبر 2026
المواصفة	نظام إدارة أمن المعلومات ISO/IEC 27001:2022
ضمن النطاق	47 متطلبًا, 46 منطبقًا
الملف	النقل والخدمات اللوجستية · 180 موظفًا
أعدّه	فريق الجودة وأمن المعلومات

المحتويات

1 الملخص التنفيذي

2 الجاهزية حسب المحور

3 خطة المعالجة

A طريقة الاحتساب وكيف تساعدكم ITA

سري. أُعدّ لشركة الواحة للخدمات اللوجستية (نموذج) من تقييمها الذاتي باستخدام أداة ITA المجانية لتقييم الفجوات، ولم تتحقق منه ITA (انظر القسم أ). يُشارك مع المعنيين فقط.

أين تقف شركة الواحة للخدمات اللوجستية (نموذج) مقابل ISO/IEC 27001

الجاهزية الإجمالية

58.2%

المستوى 2 · قيد التطوير

العمل جارٍ، مع فجوات جوهرية سيجدها المدقق.

مبتدئ | **قيد التطوير** | راسخ | جاهز للتدقيق

منطبق	موثق	فجوات مفتوحة	أولوية عالية
46	11	35	14

حالة كل متطلب



فجوات لها مسؤول	لها تاريخ مستهدف	غير مُجاب
25 من 35	20 من 35	0

ما يخبركم به هذا التقييم

- الجاهزية الإجمالية 58.2% مقابل ISO/IEC 27001 عبر 46 متطلبًا منطبقًا، منها 11 مطبق وموثق.
- أكثر ما يحتاج إلى العمل «تقييم الأداء» (29%)، وأقوى المحاور «الدعم» (75%).
- هناك 2 من بنود نظام الإدارة أقل من النصف. ولا يمكن استثناء البنود، فكل منها مرشح لعدم مطابقة جوهرية في تدقيق الشهادة.
- هناك 11 متطلبًا مطبقًا دون أدلة، وجمع سجلاته وحده يرفع النتيجة إلى 64.1% (+6.0 نقطة).
- هناك 14 فجوة ذات أولوية عالية (لم تبدأ أو مخطط لها فقط)، منها 4 في «تقييم الأداء».
- هناك 10 فجوة مفتوحة بلا مسؤول حتى الآن، والعمل بلا مسؤول نادرًا ما يُنجز.

ابدؤوا بهذا

	الأولوية	الإجراء	المسؤول
1	عالية	**الرصد والقياس** 9.1 · الاتفاق على قائمة مختصرة من المؤشرات وتكرارها ومالكها، ومراجعتها شهريًا.	مدير الموارد البشرية
2	عالية	**التدقيق الداخلي** 9.2 · تدريب مدققين داخليين أو ثلاثة، وتخطيط برنامج تدقيق يغطي جميع المتطلبات، وتنفيذ أول التدقيقات.	مدير تقنية المعلومات
3	عالية	**مراجعة الإدارة** 9.3 · تحديد موعد أول مراجعة للإدارة باستخدام جدول أعمال يغطي جميع المدخلات المطلوبة.	مسؤول أمن المعلومات

التحليل والأولويات

في جملة واحدة

عند 58.2%، العمل جارٍ، لكن «تقييم الأداء» والفجوات ذات الأولوية العالية تحتاج إلى معالجة قبل وصول المدقق.

للإدارة العليا ومجلس الإدارة

يُظهر تقييمنا الذاتي مقابل ISO/IEC 27001 نتيجة إجمالية قدرها 58.2%، ما يضعنا في المستوى 2 من 4 (قيد التطوير). لدينا 35 فجوة مفتوحة، منها 14 ذات أولوية عالية. أضعف محاورنا «تقييم الأداء» (29%)، وأقواها «الدعم» (75%). هناك 11 متطلبًا مطبقًا لكن لا يمكن إثباته بعد، وجمع سجلاته وحده يرفع النتيجة إلى 64.1%. نطلب من الإدارة اعتماد خطة المعالجة، وتحديد مسؤول وموعد لكل فجوة مفتوحة، ومراجعة التقدم شهريًا.

أين تقفون

يضع التقييم الذاتي شركة الواحة للخدمات اللوجستية (نموذج) في المستوى 2 من 4 (قيد التطوير)، بنتيجة إجمالية 58.2% عبر 46 متطلبًا منطبقًا. منها 11 مطبق وموثق، و35 ما زال مفتوحًا. بعض بنود نظام الإدارة أقل من النصف: «تقييم الأداء» (29%)، «التخطيط» (46%).

ماذا يعني ذلك

هناك 14 متطلبًا لم يبدأ أو ما زال في مرحلة التخطيط، وهي أول ما يصل إليه المدقق، وكل منها في بنود نظام الإدارة مرشح لأن يكون عدم مطابقة جوهرية. و10 مطبق جزئيًا: النهج موجود لكنه لا يُطبق بعد على النطاق كاملًا. و11 يُطبق دون سجلات، والمدقق يأخذ عينات من السجلات لا من النوايا، فستُسجل ملاحظات عليها حتى تتوفر الأدلة. وإلى أن تُسد هذه الفجوات، يُستبعد أن يوصي تدقيق الشهادة بمنحها.

بماذا تبدؤون

ابدؤوا بالفجوات ذات الأولوية العالية في أضعف المحاور، لأنها تحمل أكبر مخاطر التدقيق. وبالتوازي، اجمعوا أدلة ما يُطبق فعلًا، فهو أقل المكاسب تكلفة ويرفع النتيجة إلى 64.1%. ثم يرفعها استكمال ما طُبق جزئيًا إلى 75.0%. وحددوا لكل فجوة مسؤولًا وتاريخًا مستهدفًا؛ فحاليًا 25 من 35 لها مسؤول، و20 لها تاريخ.

الأولويات

	الأولوية	لماذا يهم	الخطوة الأولى	خلال
1	**الرصد والقياس** 9.1	دون قياس لا يمكنكم معرفة ما إذا كان النظام يعمل ولا أين تحسّنون.	الاتفاق على قائمة مختصرة من المؤشرات وتكرارها ومالكها، ومراجعتها شهريًا.	30 يومًا
2	**التدقيق الداخلي** 9.2	تتوقع جهة المنح دورة تدقيق داخلي كاملة واحدة على الأقل قبل تدقيق الشهادة.	تدريب مدققين داخليين أو ثلاثة، وتخطيط برنامج تدقيق يغطي جميع المتطلبات، وتنفيذ أول التدقيقات.	30 يومًا
3	**مراجعة الإدارة** 9.3	مراجعة الإدارة دليل إلزامي على إشراف الإدارة على النظام، ولا يمكن تجاوزها.	تحديد موعد أول مراجعة للإدارة باستخدام جدول أعمال يغطي جميع المدخلات المطلوبة.	60 يومًا
4	**المخاطر والفرص** 6.1	التخطيط المبني على المخاطر جوهر كل مواصفة حديثة لأنظمة الإدارة، ويُفحص بعناية في التدقيق.	إعداد سجل للمخاطر والفرص لكل عملية رئيسية، بمالك وإجراء وتاريخ مراجعة.	60 يومًا
5	**تقييم مخاطر أمن المعلومات** 6.1.2	تقييم المخاطر هو العمود الفقري لنظام إدارة أمن المعلومات، وكل قرار بشأن الضوابط يعتمد عليه.	الاتفاق على منهجية للمخاطر بمعايير ومالكين، ثم تقييم مخاطر أصول المعلومات الرئيسية.	90 يومًا

خارطة طريق 30 / 60 / 90 يومًا

أول 30 يومًا

- الاتفاق على قائمة مختصرة من المؤشرات وتكرارها ومالكها، ومراجعتها شهريًا.
- تدريب مدققين داخليين أو ثلاثة، وتخطيط برنامج تدقيق يغطي جميع المتطلبات، وتنفيذ أول التدقيقات.
- جمع الأدلة الموثقة للمتطلبات الـ11 المطبقة فعلًا.

من اليوم 31 إلى 60

- تحديد موعد أول مراجعة للإدارة باستخدام جدول أعمال يغطي جميع المدخلات المطلوبة.
- إعداد سجل للمخاطر والفرص لكل عملية رئيسية، بمالك وإجراء وتاريخ مراجعة.
- تحديد مسؤول وتاريخ مستهدف واقعي لكل فجوة ذات أولوية عالية.
- تدريب المدققين الداخليين وتخطيط برنامج التدقيق الداخلي.

من اليوم 61 إلى 90

- الاتفاق على منهجية للمخاطر بمعايير ومالكين، ثم تقييم مخاطر أصول المعلومات الرئيسية.
- تنفيذ أول دورة تدقيق داخلي كاملة وإغلاق ملاحظاتها.
- عقد مراجعة للإدارة لتأكيد الجاهزية والموارد.
- إعادة هذا التقييم الذاتي، ثم الاتفاق على مواعيد التدقيق مع جهة منح الشهادات.

النضج عبر المواصفة

يبين كل شريط توزيع متطلبات المحور حسب الحالة، والنتيجة متوسط المتطلبات المنطبقة، وتعدّ المربعات الفجوات المفتوحة حسب الأولوية (عالية، متوسطة، منخفضة).

المحور	توزيع الحالات	النتيجة	الفجوات ع · م · ن
سياق المنشأة	2 · 1 · 1 · 1	70%	1 · 1 · 1
القيادة	2 · 1 · 1 · 1	70%	1 · 1 · 1
التخطيط	1 · 1 · 2 · 2 · 1	46%	1 · 2 · 3
الدعم	3 · 2 · 1 · 1	75%	2 · 1 · 1
التشغيل	1 · 1 · 1	50%	1 · 1 · 1
تقييم الأداء	1 · 1 · 2 · 2	29%	1 · 1 · 4
التحسين	1 · 1	63%	1 · 1 · 0
ضوابط الملحق (أ)	1 · 3 · 3 · 2 · 2 · 1	61%	3 · 2 · 3

لم يبدأ · مخطط له · مطبق جزئيًا · مطبق دون دليل · مطبق وموثق · لا ينطبق

من أين تأتي النقاط التالية

النتيجة بعد كل نوع من العمل، بدءًا بالأقل تكلفة. الذهبي هو ما تضيفه كل خطوة.

اليوم	58.2%	
توثيق ما يُطبق فعلًا 11 متطلبًا	64.1%	+6.0
استكمال ما طُبق جزئيًا 10 متطلبًا	75.0%	+10.9
تطبيق ما خُطط له 10 متطلبًا	91.3%	+16.3
البدء بما لم يبدأ 4 متطلبًا	100.0%	+8.7

كيف تساعدكم ITA

سدّوا الفجوات أسرع بدعم من خبراء يطبقون هذه الأنظمة ويدققونها يوميًا.

الاستشارات وتحليل الفجوات

دعم التطبيق حتى الشهادة

تفاصيل الخدمة

دورة التطبيق

ثلاثة أيام تطبيقية للفريق الذي يبني النظام

تفاصيل الدورة

دورة المدقق الداخلي

خططوا لتدقيقكم الداخلي ونفذوه

تفاصيل الدورة

تحدثوا مع خبير

مكالمة مجانية لمراجعة هذا التقرير معكم

تواصلوا معنا

كل فجوة مفتوحة، مصنفة حسب ما يجب أن يحدث بعد ذلك

ابدؤوا من الأعلى. المتطلبات التي لم تبدأ أو المخطط لها فقط هي أول ما يصل إليه المدقق، والمجموعة الأخيرة مطبقة وتحتاج إلى سجلاتها فقط.

عالية لم يبدأ · 4

ابدؤوا بأساس موثق: اتفقوا على النهج ودوّنوه ثم طبّقوه.

المرجع	المتطلب	المحور	المسؤول · الموعد	الخطوة التالية
6.1.2	تقييم مخاطر أمن المعلومات هل توجد منهجية محددة لتقييم المخاطر بمعايير ومالكين للمخاطر ونتائج قابلة للتكرار؟	التخطيط	مدير الموارد البشرية 2 مايو 2027	الاتفاق على منهجية للمخاطر بمعايير ومالكين، ثم تقييم مخاطر أصول المعلومات الرئيسية.
9.1	الرصد والقياس هل تُحلل النتائج وتُقيّم للحكم على الأداء وفاعلية النظام؟	تقييم الأداء	مدير العمليات 26 يناير 2027	الاتفاق على قائمة مختصرة من المؤشرات وتكرارها ومالكها، ومراجعتها شهريًا.
9.2	التدقيق الداخلي هل تُرفع نتائج التدقيق إلى الإدارة وتُتابع الملاحظات حتى إغلاقها؟	تقييم الأداء	مدير تقنية المعلومات 13 فبراير 2027	تدريب مدققين داخليين أو ثلاثة، وتخطيط برنامج تدقيق يغطي جميع المتطلبات، وتنفيذ أول التدقيقات.
A	جاهزية تقنية المعلومات لاستمرارية الأعمال (A.5.30) هل متطلبات استمرارية تقنية المعلومات محددة ومطبقة ومختبرة؟	ضوابط الملحق (أ)	مدير تقنية المعلومات 14 يناير 2027	تحديد أهداف التعافي للأنظمة الحرجة واختبار عملية استعادة.

عالية مخطط له · 10

انتقلوا من الخطة إلى التطبيق. حددوا مسؤولًا وموعدًا ثم طبّقوا الترتيب.

المرجع	المتطلب	المحور	المسؤول · الموعد	الخطوة التالية
4.4	النظام وعملياته هل العمليات اللازمة وتسلسلها وتفاعلاتها ومالكوها ومعاييرها ومؤشراتها محددة؟	سياق المنشأة	مسؤول الامتثال 19 فبراير 2027	رسم خريطة عمليات في صفحة واحدة، وتحديد مالك ومدخلات ومخرجات ومؤشر أو مؤشرين لكل عملية.
5.2	السياسة هل السياسة مُبلغة ومفهومة ومتاحة للأطراف المعنية ذات الصلة؟	القيادة	يُحدد لاحقًا 27 مارس 2027	مراجعة السياسة مع الإدارة العليا واعتمادها، وتوعية كل فريق بما تعنيه لعمله.
6.1	المخاطر والفرص هل تُقيّم فاعلية الإجراءات المتخذة تجاه المخاطر والفرص؟	التخطيط	يُحدد لاحقًا	إعداد سجل للمخاطر والفرص لكل عملية رئيسية، بمالك وإجراء وتاريخ مراجعة.
6.2	الأهداف والتخطيط لتحقيقها هل تحدد خطط كل هدف ماذا والموارد ومن ومتى وكيف تُقيّم النتائج، وتُتابع؟	التخطيط	مدير تقنية المعلومات	وضع ثلاثة إلى خمسة أهداف قابلة للقياس للعام، لكل منها مالك وموارد وموعد وطريقة متابعة.
7.5	المعلومات الموثقة هل المعلومات الموثقة مضبوطة من حيث التعريف والمراجعة والاعتماد والإصدار والوصول والحماية؟	الدعم	مدير الموارد البشرية 2 أبريل 2027	إعداد قائمة رئيسية بالوثائق بمالكيها وإصداراتها، والاتفاق على مكان حفظ السجلات ومدته.
8.1	تخطيط العمليات وضبطها هل العمليات والمنتجات والخدمات المقدمة خارجيًا والمؤثرة في النظام محددة ومضبوطة؟	التشغيل	مدير تقنية المعلومات	اختيار أكثر ثلاث عمليات أهمية وتحديد معاييرها وضوابطها والسجلات التي تثبتها.

المرجع	المتطلب	المحور	المسؤول · الموعد	الخطوة التالية
9.1	**الرصد والقياس** هل حُدد ما يُرصد ويُقاس والطرق والتكرار ومن يحلل النتائج؟	تقييم الأداء	مدير الموارد البشرية	الاتفاق على قائمة مختصرة من المؤشرات وتكرارها ومالكها، ومراجعتها شهريًا.
9.3	**مراجعة الإدارة** هل تراجع الإدارة العليا النظام على فترات مخططة مغطية جميع المدخلات المطلوبة؟	تقييم الأداء	مسؤول أمن المعلومات	تحديد موعد أول مراجعة للإدارة باستخدام جدول أعمال يغطي جميع المدخلات المطلوبة.
A	**أمن الموردين والخدمات السحابية (A.5.19، A.5.23)** هل يُتفق على متطلبات الأمن مع الموردين ومقدمي الخدمات السحابية ويُراقب أداؤهم؟	ضوابط الملحق (أ)	يُحدد لاحقًا 26 أبريل 2027	حصر الموردين والخدمات السحابية الحرجة والاتفاق على متطلبات الأمن مع كل منهم.
A	**مكافحة البرمجيات الضارة وإدارة الثغرات (A.8.7، A.8.8)** هل الحماية من البرمجيات الضارة ومعالجة الثغرات التقنية في الوقت المناسب مطبقة؟	ضوابط الملحق (أ)	يُحدد لاحقًا 19 فبراير 2027	تحديد مهل التحديث حسب الخطورة ومتابعة الالتزام شهريًا.

متوسطة

مطبق جزئيًا · 10

وسّعوا النهج القائم ليشمل النطاق كاملًا وطبّقوه باتساق، ثم وثّقوه.

المرجع	المتطلب	المحور	المسؤول · الموعد	الخطوة التالية
4.2	**الأطراف المعنية** هل حُددت الأطراف المعنية ومتطلباتها ذات الصلة، وما يصبح منها التزامات واجبة؟	سياق المنشأة	يُحدد لاحقًا 1 فبراير 2027	إعداد جدول بسيط بالأطراف المعنية واحتياجاتها، وتحديد ما إذا كانت كل حاجة التزامًا واجبًا عليكم.
5.1	**القيادة والالتزام** هل متطلبات النظام مدمجة في عمليات العمل بدلًا من تشغيلها بصورة موازية؟	القيادة	مسؤول أمن المعلومات 9 مارس 2027	إدراج النظام في جدول اجتماع الإدارة الشهري، مع تسجيل النتائج والقرارات والموارد.
6.1	**المخاطر والفرص** هل حُددت المخاطر والفرص، مع تخطيط الإجراءات ودمجها في العمليات؟	التخطيط	مدير تقنية المعلومات 14 أبريل 2027	إعداد سجل للمخاطر والفرص لكل عملية رئيسية، بمالك وإجراء وتاريخ مراجعة.
6.2	**الأهداف والتخطيط لتحقيقها** هل وُضعت أهداف قابلة للقياس للوظائف والمستويات المعنية ومتسقة مع السياسة؟	التخطيط	يُحدد لاحقًا 20 يناير 2027	وضع ثلاثة إلى خمسة أهداف قابلة للقياس للعام، لكل منها مالك وموارد وموعد وطريقة متابعة.
7.2	**الكفاءة** هل تُتخذ إجراءات التدريب وغيره لسد فجوات الكفاءة، وتُقيَّم فاعليتها؟	الدعم	مسؤول الامتثال	إعداد مصفوفة كفاءات للأدوار الرئيسية، وسد أكبر الفجوات بتدريب موجّه.
8.1	**تخطيط العمليات وضبطها** هل العمليات التشغيلية مخططة ومضبوطة وفق معايير محددة، مع سجلات تثبت تنفيذها كما خُطط؟	التشغيل	مسؤول الامتثال 20 أبريل 2027	اختيار أكثر ثلاث عمليات أهمية وتحديد معاييرها وضوابطها والسجلات التي تثبتها.
9.2	**التدقيق الداخلي** هل يوجد برنامج تدقيق داخلي يغطي جميع المتطلبات وينفذه مدققون أكفاء ومحايدون؟	تقييم الأداء	يُحدد لاحقًا	تدريب مدققين داخليين أو ثلاثة، وتخطيط برنامج تدقيق يغطي جميع المتطلبات، وتنفيذ أول التدقيقات.
10.1	**التحسين المستمر** هل التحسين المستمر ظاهر في اتجاهات المؤشرات وإجراءات التحسين المنجزة والدروس المستفادة؟	التحسين	مدير العمليات	الاحتفاظ بسجل للتحسين، وعرض ما تم تحسينه وما تغير من نتائج في كل مراجعة للإدارة.

المرجع	المتطلب	المحور	المسؤول · الموعد	الخطوة التالية
A	**التحكم في الوصول والصلاحيات المميزة (A.5.15، A.8.2)** هل تُمنح صلاحيات الوصول على أساس الحاجة، وتُراجع دوريًا، وتُقيَّد الصلاحيات المميزة؟	ضوابط الملحق (أ)	مدير الموارد البشرية	إجراء مراجعة للصلاحيات في الأنظمة الرئيسية وإلغاء غير الضروري منها والصلاحيات المميزة.
A	**التوعية والتدريب (A.6.3)** هل يتلقى العاملون توعية أمنية منتظمة تشمل التصيد الاحتيالي وواجبات الإبلاغ؟	ضوابط الملحق (أ)	مدير الموارد البشرية 1 فبراير 2027	إطلاق برنامج توعية قصير ومحاكاة للتصيد الاحتيالي.

منخفضة مطبق دون دليل · 11

اجمعوا الأدلة التي يمكن للمدقق أخذ عينات منها. الضابط يعمل، والناقص هو سجله.

المرجع	المتطلب	المحور	المسؤول · الموعد	الخطوة التالية
4.1	**فهم المنشأة وسياقها** هل حددتم ما إذا كان تغير المناخ قضية ذات صلة بالمنشأة؟	سياق المنشأة	مسؤول أمن المعلومات	عقد ورشة لمدة ساعة مع المديرين لحصر القضايا الداخلية والخارجية (SWOT أو PESTLE)، ثم تسجيلها مع تاريخ مراجعة.
5.2	**السياسة** هل توجد سياسة معتمدة مناسبة للمنشأة تتضمن الالتزام باستيفاء المتطلبات والتحسين؟	القيادة	مدير الموارد البشرية	مراجعة السياسة مع الإدارة العليا واعتمادها، وتوعية كل فريق بما تعنيه لعمله.
6.1.3	**معالجة المخاطر وبيان قابلية التطبيق** هل توجد خطة معالجة مخاطر معتمدة من مالكي المخاطر وبيان قابلية تطبيق يبرر كل ضابط من الملحق (أ)؟	التخطيط	مدير العمليات	إعداد خطة معالجة المخاطر وبيان قابلية التطبيق مع تبرير كل ضابط من الملحق (أ).
7.2	**الكفاءة** هل متطلبات الكفاءة محددة لكل دور مؤثر في الأداء، مع أدلة على الكفاءة؟	الدعم	مدير العمليات 25 فبراير 2027	إعداد مصفوفة كفاءات للأدوار الرئيسية، وسد أكبر الفجوات بتدريب موجّه.
7.4	**الاتصال** هل الاتصالات الداخلية والخارجية مخططة: ماذا ومتى ومع من وكيف ومن يتولاها؟	الدعم	مسؤول أمن المعلومات	إعداد خطة اتصال في صفحة واحدة: ماذا ومتى ومع من وكيف ومن المسؤول.
8.2	**تنفيذ تقييمات المخاطر** هل تُكرر تقييمات المخاطر على فترات مخططة وعند حدوث تغييرات جوهرية؟	التشغيل	يُحدد لاحقًا 8 مايو 2027	تحديد تكرار المراجعة ومحفزات إعادة تقييم المخاطر.
9.3	**مراجعة الإدارة** هل تسجل مخرجات المراجعة القرارات بشأن التحسين والتغيير والموارد، مع متابعة الإجراءات؟	تقييم الأداء	يُحدد لاحقًا 3 مارس 2027	تحديد موعد أول مراجعة للإدارة باستخدام جدول أعمال يغطي جميع المدخلات المطلوبة.
10.2	**عدم المطابقة والإجراء التصحيحي** هل تُصحح حالات عدم المطابقة، وتُحلل أسبابها الجذرية، وتُتخذ الإجراءات التصحيحية ويُتحقق من فاعليتها؟	التحسين	مسؤول الامتثال 21 مارس 2027	استخدام نموذج موحد للإجراء التصحيحي يتضمن تحليل السبب الجذري (لماذا الخمسة أو عظم السمكة) والتحقق من الفاعلية.
A	**حصر المعلومات وتصنيفها (A.5.9، A.5.12)** هل يوجد حصر للمعلومات والأصول بمالكيها، والمعلومات مصنفة ومعلَّمة؟	ضوابط الملحق (أ)	مسؤول أمن المعلومات 8 أبريل 2027	إعداد حصر للأصول بمالكيها ونظام تصنيف بسيط.
A	**المتطلبات القانونية والتعاقدية (A.5.31)** هل المتطلبات الأمنية القانونية والتنظيمية والتعاقدية، بما فيها الضوابط الوطنية للأمن السيبراني، محددة؟	ضوابط الملحق (أ)	يُحدد لاحقًا	حصر المتطلبات الأمنية القانونية والتنظيمية والتعاقدية، بما فيها الضوابط الوطنية مثل ECC.

المرجع	المتطلب	المحور	المسؤول · الموعد	الخطوة التالية
A	النسخ الاحتياطي والسجلات والمراقبة (A.8.13، A.8.15، A.8.16) هل تُختبر النسخ الاحتياطية للاستعادة، وتُجمع السجلات وتُحمى وتُراجع؟	ضوابط الملحق (أ)	مدير تقنية المعلومات	اختبار استعادة من نسخة احتياطية والتأكد من جمع السجلات للأنظمة الحرجة.

طريقة الاحتساب

أوزان الحالات

الحالة	الوزن	المعنى
لم يبدأ	0.00	لا توجد سياسة أو عملية أو نشاط بعد.
مخطط له	0.25	النهج متفق عليه ومجدول، لكن لم يُطبق شيء بعد.
مطبق جزئيًا	0.50	مطبق في جزء من النطاق أو بصورة غير متسقة.
مطبق دون دليل	0.75	يعمل كما ينبغي، لكن لا يمكنكم إثباته اليوم.
مطبق وموثق	1.00	يعمل كما ينبغي، مع سجلات يمكن للمدقق أخذ عينات منها.
لا ينطبق	—	استثناء مبرر، يُستبعد من النتيجة.

مستويات الجاهزية

1 · مبتدئ (+0%)
معظم المتطلبات غير مطبقة بعد. ابنوا الأساس قبل التفكير في التدقيق.

2 · قيد التطوير (+40%)
العمل جارٍ، مع فجوات جوهرية سيجدها المدقق.

3 · راسخ (+65%)
معظم الضوابط تعمل، والمتبقي سد فجوات محددة وتوثيق ما يُطبق.

4 · جاهز للتدقيق (+85%)
المتطلبات مطبقة وموثقة. جاهزون للتدقيق الداخلي والخارجي.

إذا قلّ أي بند من بنود نظام الإدارة عن 50% يبقى المستوى عند «قيد التطوير»، لأن البنود لا يمكن استثناؤها من نطاق الشهادة.

أساس هذا التقرير وحدود المسؤولية

هذا التقرير ناتج عن تقييم ذاتي. والنتائج والمستويات والملاحظات والتوصيات مستمدة فقط من المعلومات التي أدخلتها المنشأة، ولم تراجعها ITA أو تتحقق منها أو تختبرها أو تدققها، ولم تدقق أنظمة المنشأة.

تعتمد دقة النتائج كليًا على دقة الإجابات واكتمالها. ولا تقدم ITA أي ضمان أو شهادة أو رأي تدقيق، ولا تتحمل أي مسؤولية عن القرارات المتخذة أو غير المتخذة اعتمادًا على هذا التقرير.

يُولَّد التحليل آليًا من النتائج لأغراض التخطيط فقط، وهو ليس استشارة قانونية أو مهنية، ولا يغني عن تقييم مستقل أو تدقيق شهادة.

المتطلب المطبق الذي لا يمكن إثباته يحصل على 0.75 لا 1.00، فالمدقق يأخذ عينات من السجلات لا من النوايا، ولذلك فإن سد هذه المسافة أسرع طريق إلى نتيجة أعلى. وجميع الأسئلة بصياغة ITA الخاصة، وأرقام البنود للإشارة فقط، ولا يُنسخ أي نص من المواصفة. اعملوا دائمًا من نسختكم المرخصة.

ملف EXCEL

يتبع ملف Excel من الأداة نفسها الأقسام والألوان نفسها، وعند تغيير أي حالة فيه تتحدث كل النتائج والمستويات والملخصات.

تواصلوا مع ITA

الاستشارات وتحليل الفجوات
دعم التطبيق حتى الشهادة
تفاصيل الخدمة

دورة التطبيق
ثلاثة أيام تطبيقية للفريق الذي يبني النظام
تفاصيل الدورة

دورة المدقق الداخلي
خططوا لتدقيقكم الداخلي ونفذوه
تفاصيل الدورة

تحدثوا مع خبير
مكالمة مجانية لمراجعة هذا التقرير معكم
تواصلوا معنا

ITA – Inspection, Testing & Assurance Company · ita-cert.co.uk · info@ita-cert.co.uk