نموذج الاستفسارات

مشروع تدقيق أنظمة تقنية المعلومات وضوابط الأمن السيبراني

م	الاسئلة والاستفسارات	إجابة الهيئة السعودية للمقيمين المعتمدين
1	يرجى تزويدنا بالهيكل التنظيمي الخاص بإدارة الأمن السيبراني وتقنية المعلومات ؟	1-ادارة الامن السيبراني منفصلة / 2-التحول الرقمي والتقنية تشمل ادارة الحلول الرقمية ، البنية التحتية والعمليات ، التحول الرقمي ، مكتب البيانات
2	كم عدد الموظفين بكل من إدارة الأمن السيبراني وتقنية المعلومات؟	ادارة الامن السيبراني مدير مكلف + موظف + متوقع موظف اضافي الفترة القادمة التحول الرقمي والتقنية 8 من غير المتعاقدين
3	هل سيتم عمل تقييم امتثال منفصل للتنظيمات التشريعية المطبقة؟ أو سيقوم المراجع بعمل مراجعات على الممارسات الإدارية المطبقة داخل الإدارات فقط؟	نعم للكل
4	ما هي المعايير المحددة التي سيتم التحقق من الامتثال لها؟ (مثلاً: ضوابط الهيئة الوطنية الأساسية للأمن السيبراني(ECC) ، ضوابط الهيئة الوطنية للحوسبة السحابية (CCC)، ضوابط الهيئة الوطنية للأمن السيبراني للعمل عن بعد (TCC))	ECC + TCC + CCC
5	هل هناك أنظمة أو خدمات تُصنف كـ "أنظمة حساسة (Critical Assets)" لدى الهيئة؟	لا
6	كم عدد الأنظمة أو التطبيقات التي تندرج ضمن نطاق المراجعة؟	7
7	هل تعتمد الهيئة على بنية تحتية محلية (On-premise) فقط، أم بيئات سحابية (Cloud/Hybrid)؟	hybird

م	الاسئلة والاستفسارات	إجابة الهيئة السعودية للمقيمين المعتمدين
8	كم عدد الأنظمة وأجهزة الشبكات التي سيتم مراجعتها؟ • Firewalls • Routers • Switches • Servers • Databases Security Devices	• Firewalls – 4 • Routers – 2 • Switches – 15 • Servers – 120 • Databases - 6 approx numbers
9	ما هو العدد الإجمالي لقواعد البيانات ومستودعات البيانات التي سيتم مراجعتها ضمن نطاق المراجعة؟	6
10	في نطاق تدقيق الأنظمة والتطبيقات، هل يشمل ذلك مراجعة إعدادات تقنية تفصيلية (Configuration Review)للخوادم وقواعد البيانات والشبكات؟	لا

11	ما هي أبرز المهام والمسؤوليات الخاصة بإدارة مكتب البيانات؟	* مواكبة أحدث المعايير والسياسات الصادرة عن مكتب إدارة البيانات الوطنية [NDMO] وضمان التنفيذ فى الهيئة من خلال التوعية والتوجيه * الإشراف على دليل بيانات الهيئة بما يتماشى مع معايير وسياسات مكتب إدارة البيانات الوطنية * مراجعة طلبات تبادل البيانات بين إدارات الصئة والجهات الخارجية والتنسية، مع مكتب إدارة السانات الوطنية وفقا لذلك تطوير الاتفاقيات ذات الصلة * إعداد استراتيجية لإدارة وتنظيم البيانات وحوكمتها وحماية البيانات الشخصية لرفع قدرات إدارة البيانات فى الهيئة بما يتماشى مع إرشادات مكتب إدارة البيانات الوطنية * الإشراف على جمع متطلبات واحتياجات العمل وبيانات ذكاء الأعمال وطلبات لوحة المعلومات من أصحاب المصلحة المعنيين * تصميم قاعدة البيانات وفقا لاحتاجات تقنية المعلومات وأفضل الممارسات وتحديد أصحاب المصلحة المعنين المسؤولين عن البيانات وضبط الوصول إلى قواعد البيانات وفقا للسياسات * ضمان التوافق مع السياسات والمعايير الموضوعة من خلال المراجعات الدورية للبيانات وتقديم التقارير ذات الصلة إلى مكتب إدارة البيانات الوطنية * معالجة المتطلبات الداخلية والتحديات المتعلقة بإدارة البيانات وحماية البيانات الشخصية لضمان الامتثال لمعايير وسياسات مكتب إدارة البيانات الوطنية
12	هل مركز العمليات الأمنية SOC داخل الهيئة أو يتم إدارته عن طريق طرف خارجي؟	طرف خارجي

م	الاسئلة والاستفسارات	إجابة الهيئة السعودية للمقيمين المعتمدين
13	ما نوعية السجلات والبيانات المطلوب فحصها، وهل سيتم الفحص على كامل البيانات أم على عينة؟	عينة
14	هل يتضمن النطاق مراجعة نظام ERP إن وجد؟ إذ نعم، الرجاء التأكيد إذا ما سيتم تغطية عمليات الأعمال المؤتمتة داخل النظام أو سيتم التطرق إلى الضوابط الفنية والأمنية فقط؟	نعم للكل
15	عدد الmodules داخل نظام ERP؟ (المالية، الموارد البشرية، مشتريات وغيره..)	يشمل نظام ال ERP (المشتريات والعقود، المالية، الموارد البشرية)
16	يرجى تزويدنا بتصميم الشبكة عالي المستوى ويشمل جميع مكونات الأمان.	لا
17	هل يقتصر نطاق مراجعة مكتب إدارة البيانات (Data management Office) على مجالات إدارة البيانات (حوكمة البيانات، جودة البيانات، تصنيف البيانات، سلامة البيانات) المذكورة في طلب تقديم العروض (RFP) فقط؟	فقط المذكور
18	هل يوجد تشكيل رسمي لمكتب إدارة البيانات(DMO) ؟ وفي حال عدم وجوده، أي جهة تتولى حالياً مسؤوليات الحوكمة؟	نعم
19	يرجى تأكيد ما إذا كانت الهيئة تستخدم أي أدوات لإدارة البيانات وحماية البيانات الشخصية، وذلك تحديداً في المجالات التالية: •تصنيف البيانات •جودة البيانات •تكامل البيانات	نعم ، نظام حاليا في مرحلة الاختبار
20	هل سيتم تقييم الحوكمة على جميع أصول البيانات أم على عناصر البيانات الحرجة / مجموعات البيانات عالية المخاطر فقط؟ وفي حال كان النطاق محدوداً، كيف يتم تحديدها؟	عالية المخاطر

م	الاسئلة والاستفسارات	إجابة الهيئة السعودية للمقيمين المعتمدين
21	ما هي الأنظمة واللوائح المحلية والدولية المطبقة على ممارسات إدارة البيانات في الهيئة	لوائح وسياسات سدايا
22	هل يمكن تحديد عدد المواقع أو الفروع المشمولة ضمن نطاق المراجعة؟	مقر الهيئة
23	هل سبق للهيئة إجراء تقييمات لإدارة البيانات وحماية البيانات الشخصية؟	لا
24	هل قامت الهيئة بإجراء تقييم نضج مؤشر البيانات الوطني؟ وفي حال الإجابة بنعم، يرجى تزويدنا بالدرجة.(05 – 01)	نعم لكن لم يتم رصد الدرجة حتى الان
25	فيما يتعلق بجودة البيانات، هل يقتصر النطاق على الحوكمة فقط (الإطار، الأدوار، اعتماد القواعد، دورة حياة معالجة المشكلات)، أم يشمل أيضاً الاختبارات التقنية (تحليل البيانات، نتائج تنفيذ القواعد، الاستثناءات، إغلاق إجراءات المعالجة)؟	نعم للكل
26	بالنسبة لتصنيف البيانات، هل سيتم التحقق من سياسة وإجراءات التصنيف فقط، أم سيتم أيضاً التحقق من تطبيق ملصقات التصنيف على مجموعات البيانات والتقارير والمستودعات؟	نعم للكل
27	فيما يتعلق بسلامة البيانات، هل سيقتصر التقييم على ضوابط الحوكمة (التعريفات، الملكية، المراقبة) أم سيشمل أيضاً ضوابط الأنظمة (القيود، المطابقات، المجموعات الاختبارية، سجلات التدقيق)؟	نعم للكل
28	ما هي البيئات المشمولة ضمن النطاق (بيئة الإنتاج فقط، أم أيضاً التعافي من الكوارثDR ، وبيئة الاختبارUAT ، وبيئة التطوير)؟	نعم للكل
29	بالنسبة لضوابط الوصول إلى قواعد البيانات، هل سيتم اختبار الحوكمة فقط (السياسات، الأدوار، الموافقات) أم أيضاً الإعدادات(الحسابات ذات الصلاحيات العالية، ربط الأدوار، المصادقة متعددة العواملMFA ، حسابات الخدمة، الحسابات المشتركة)؟	نعم للكل

م	الاسئلة والاستفسارات	إجابة الهيئة السعودية للمقيمين المعتمدين
30	هل ينبغي إدراج ضوابط النسخ الاحتياطي، والاستعادة، والتكرار، والتوافر العالي لقواعد البيانات ضمن النطاق، أم أنها تندرج تحت عمليات تقنية المعلومات؟	نعم
31	هل سيكون تقييم ضوابط أمن الواجهات (المصادقة، التشفير أثناء النقل، إدارة بيانات الاعتماد والمفاتيح السرية، الشهادات) ومعالجة الأخطاء (إعادة المحاولة، قوائم الانتظار للرسائل غير المعالجة، المطابقات) جزءاً من النطاق؟	نعم
32	بالنسبة لضوابط سلامة البيانات، هل يشمل النطاق ما يلي: •قيود قواعد البيانات •سلامة العلاقات المرجعية •المشغلات(Triggers) •الإجراءات المخزنة •إجراءات المطابقة •ضوابط المعالجة الدفعية	نعم
33	هل توجد أطراف ثالثة مشاركة في عمليات التكامل (موردون، منصات حكومية)، وهل ينبغي مراجعة أدلة التأكيد الخاصة بالأطراف الثالثة؟	نعم يوجد اطراف ثالثة