العرض الفني والمالي (مشروع تعزيز الأمن السيبراني، والامتثال، واستمرارية الأعمال باستخدام حلول Microsoft 365)

الإصدار 1.0

التاريخ: 17-فبراير-2026 ميلادي

الموافق 29-شعبان-1446 هجري

إعداد: شركة الرؤيا الموثوقة للأمن السيبراني

معلومات التواصل

للاستفسار حول هذا المستند والمعلومات الواردة، بإمكانكم التواصل مع الأشخاص الوارد ذكرهم في الجدول أدناه:

الاسم	**هاشم العزيزي**
رقم الهاتف	**+966-53-122-1580**
البريد إلكتروني	**Hashem.azizi@trustedvision.biz**
العنوان	**حي قرطبة، شارع سعيد بن زيد،** **مبنى مجموعة إنجاز، رقم 6482، الدور الأول،** **صندوق البريد: 13247،** **الرياض، المملكة العربية السعودية.**

المحتويات

1.	ملخص تنفيذي لمتطلبات العميل	5
2.	مقدمة	6
3.	منهجية إدارة وتنفيذ المشروع	7
4.	نقل المعرفة	22
5.	تقرير سير عمل المشروع الأسبوعي	23
6.	تقويم الشركة	24
7.	خطط الموارد والجودة والتواصل	25
8.	المخاطر عالية المستوى	26
9.	الجدول الزمني التقريبي لتنفيذ المشروع	27
10.	الضمان الابتدائي	28
11.	معلومات عن الشركة	29
12.	العرض المالي	**Error! Bookmark not defined.**
13.	الشهادات	30
14.	المشاريع السابقة التي تم تنفيذها	33

15. طاقم العمل 44

13 ملخص تنفيذي لمتطلبات العميل

يسر شركة الرؤيا الموثوقة تقديم الخدمات الفنية والاستشارية لإدارة الأمن السيبراني في مشروع تطوير وتعزيز منظومة الأمن السيبراني والامتثال واستمرارية الأعمال لدى الهيئة من خلال تطبيق حلول Microsoft 365 E5وMicrosoft Azure وفق أفضل الممارسات العالمية ومعايير ISO/IEC 27001:2022

يعتمد نموذج التنفيذ المقترح على منهجية تنفيذ تدريجية قائمة على تحليل الوضع الحالي، وتقييم الفجوات، وتصميم الحلول وفق متطلبات الهيئة، ثم تنفيذ الحلول بشكل مرحلي مع الاختبار والتحقق المستمر لضمان تحقيق أعلى مستويات الجودة والامتثال.

يرتكز العرض على أربعة محاور رئيسية:

- **تعزيز الأمن السيبراني المتقدم** عبر Microsoft Defender و Microsoft Intuneلحماية الأجهزة والهويات والتطبيقات.
- **حوكمة البيانات والامتثال التنظيمي** باستخدام Microsoft Purview لتصنيف البيانات ومنع تسربها وإدارة دورة حياتها.
- **استمرارية الأعمال والتعافي من الكوارث** من خلال Microsoft 365 Backup و Azure Backupو.Azure Site Recovery
- **نقل المعرفة وبناء القدرات التشغيلية** لضمان الاستقلالية التشغيلية للهيئة واستدامة الحلول.

نلتزم بتطبيق نموذج حوكمة قوي، وإدمان المخاطر بشكل استباقي، وضمان جودة التنفيذ، ونقل المعرفة الكامل، بما يحقق للهيئة:

- رفع مستوى النضج الأمني المؤسسي.
- تحقيق الامتثال التنظيمي.
- تقليل المخاطر التشغيلية.
- تحسين الكفاءة التشغيلية.
- تعزيز جاهزية التعافي واستمرارية الأعمال.

14 مقدمة

إن خبرتنا في تنفيذ مشاريع مماثلة تجعلنا قادرين على تنفيذ هذا المشروع والالتزام بكافة المتطلبات الخاصة بالجهة كما أننا سنعمل على تطبيق المعايير والأطر العالمية والمحلية في هذا المجال.

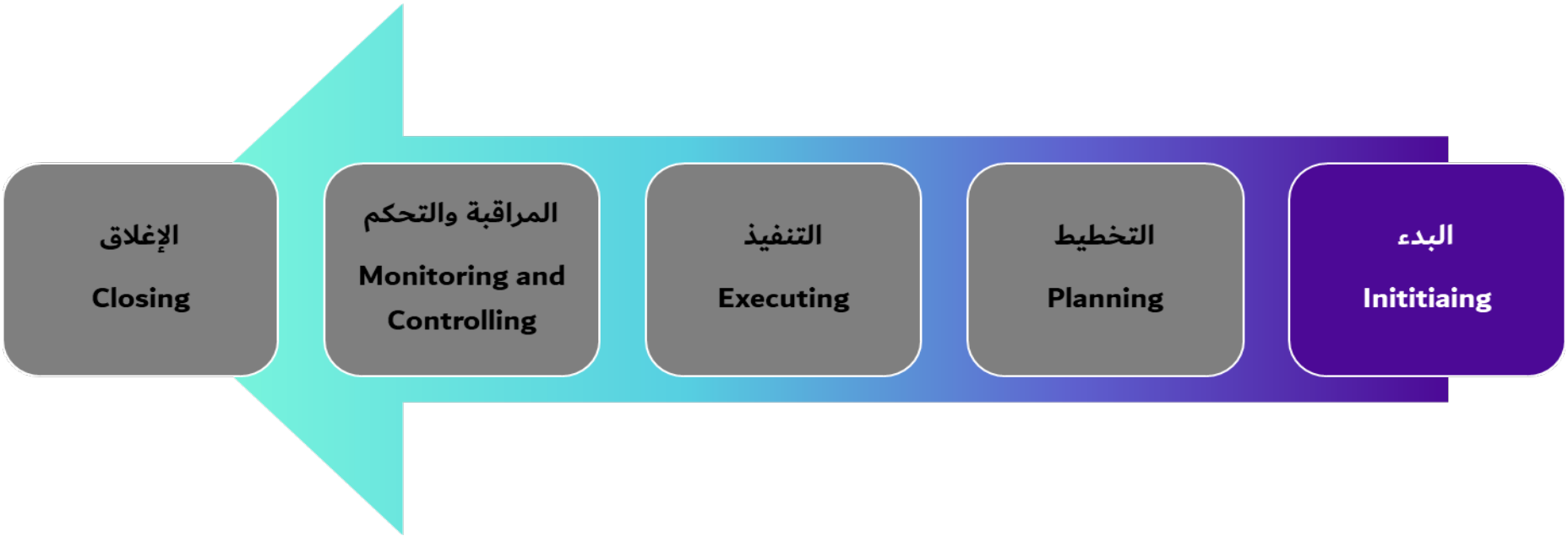
ونأمل أن تحقق خدماتنا الاستشارية كل متطلبات الجهة ونتطلع إلى شراكة حقيقية مع الجهة لتحقيق المنفعة المتبادلة.

نتبع في شركة الرؤيا الموثوقة منهجية إدارة المشاريع العالمية الخاصة بمؤسسة إدارة المشاريع العالمية (PMI) من حيث البدء (Initiating) والتخطيط (Planning) والتنفيذ (Executing) والمراقبة والتحكم (Monitoring and Controlling) والإغلاق (Closing).

15 منهجية إدارة وتنفيذ المشروع

نتبع في شركة الرؤيا الموثوقة منهجية إدارة المشاريع العالمية الخاصة بمؤسسة إدارة المشاريع العالمية (PMI) من حيث البدء (Initiating) والتخطيط (Planning) والتنفيذ (Executing) والمراقبة والتحكم (Monitoring and Controlling) والإغلاق (Closing)

3.1 مرحلة البدء

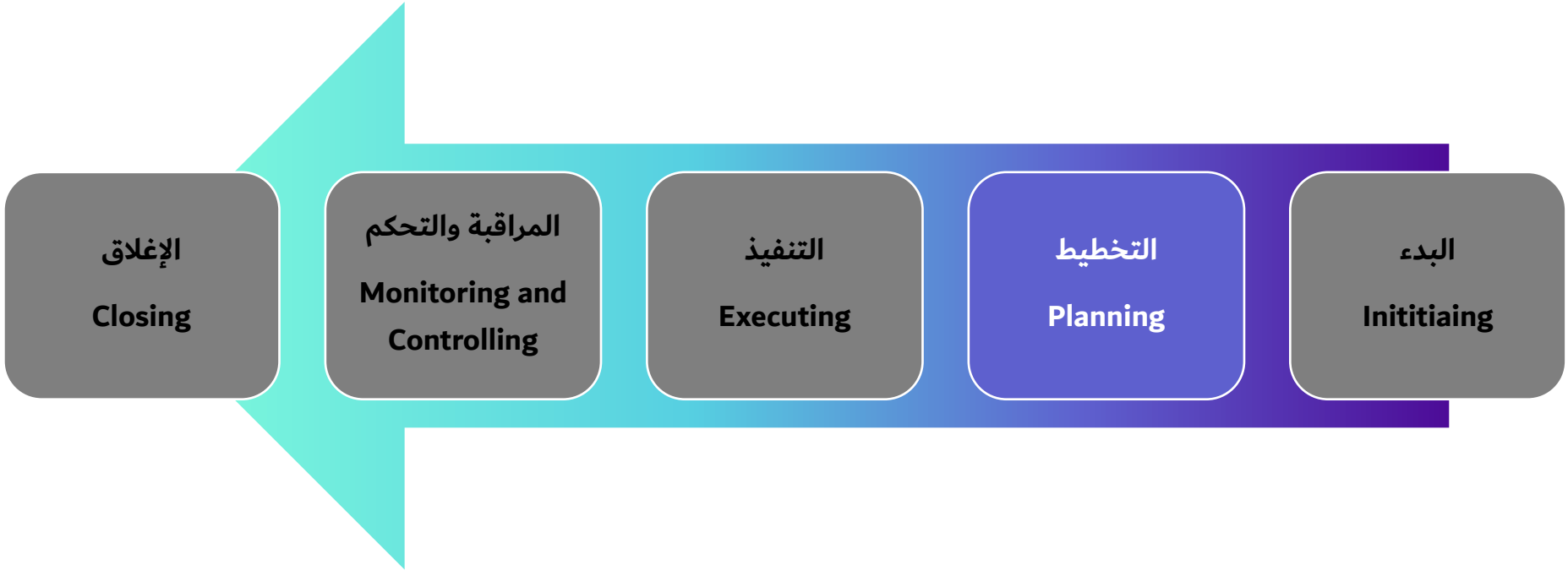


في هذه المرحلة يتم تعريف المشروع وتحديد قائد المشروع صلاحياته وأهم أصحاب المصلحة وأهم المخاطر المتوقعة وأهم المخرجات وتدوين ذلك في ميثاق المشروع.

يحتوي الجدول أدناه على الأنشطة التي سيتم القيام بها في هذه المرحلة:

الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الهيئة	الأنشطة المُنجزة والمواد المُسلّمة للجهة
1	تجهيز فريق المشروع	تخصيص مدير مشروع من الجهة للعمل مع الاستشاريين	فريق مجهّز للبدء في المشروع
2	تحديد أصحاب المصلحة	-	-
3	تطوير ميثاق المشروع(Project Charter)	مراجعة واعتماد ميثاق المشروع	ميثاق المشروع

3.2 مرحلة التخطيط



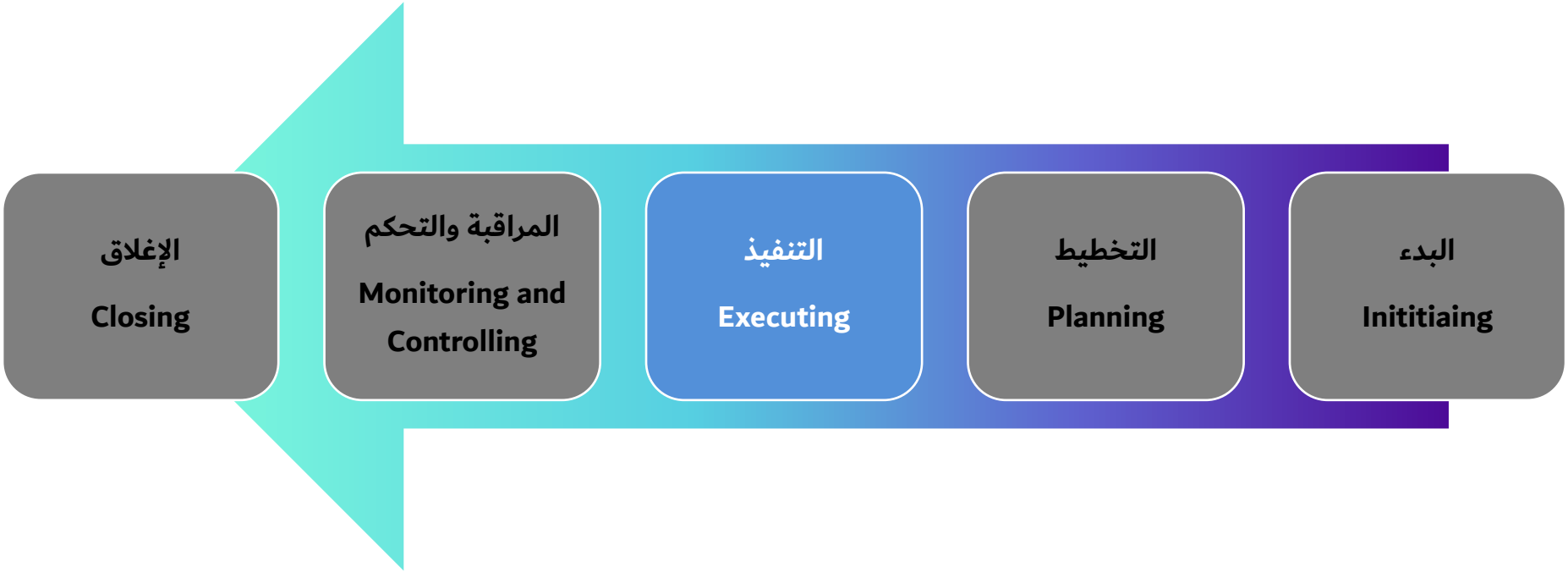
في هذه المرحلة، يتم حصر النطاق وتحديد طرق العمل للوصول إلى الأهداف كما يتم تحديد الجدول الزمني وميزانية المشروع وأهم مخرجات هذه المرحلة خطة تنفيذ المشروع التي تحتوي على كل المعلومات السابقة.

يحتوي الجدول أدناه على الأنشطة التي سيتم القيام بها في هذه المرحلة:

الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الهيئة	الأنشطة المُنجزة والمواد المُسلّمة للجهة
1	1. جمع الأدلة والمعلومات ذات العلاقة بمتطلبات الأمن السيبراني والتي تشمل وثائق حوكمة الأمن السيبراني الحالية: • السياسات • الإجراءات • استراتيجية الأمن السيبراني والتحول الرقمي وإدارة البيانات وتقنية المعلومات • أطر العمل • المعايير التقنية • سجل الأصول المعلوماتية والتقنية • مصفوفة حوكمة البيانات 2. ويتم إجراء دراسة لجميع المعلومات ونتائج المقابلات ليتم فهم طبيعة العمل	تقديم الوثائق المطلوبة	محاضر اجتماعات
2	عمل مقابلات مع الإدارات والأطراف ذات العلاقة وعلى سبيل المثال لا الحصر: • الإدارة العامة للأمن السيبراني	• تنسيق مواعيد المقابلات • تقديم الوثائق المطلوب	محاضر اجتماعات

الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الهيئة	الأنشطة المُنجزة والمواد المُسلّمة للجهة
	• الإدارة العامة لتقنية المعلومات • الإدارة العامة للتحول الرقمي • إدارة المرافق • إدارة الشؤون الإدارية • الإدارة العامة للتواصل المؤسسي		
3	تطوير خطة تنفيذ المشروع	• مراجعة واعتماد خطة تنفيذ المشروع • تخصيص الموارد والميزانيات لإتمام المشروع	خطة تنفيذ المشروع

3.3 مرحلة التنفيذ



في هذه المرحلة يتم تنفيذ المشروع حسب الخطة الموضوعة للحصول على المخرجات المتوقعة.

يحتوي الجدول أدناه على الأنشطة التي سيتم القيام بها في هذه المرحلة:

الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الهيئة	الأنشطة المُنجزة والمواد المُسلّمة للجهة
	إعداد وتطبيق السياسات والإجراءات الأمنية المطلوبة وفق المواصفة الدولية ISO/IEC 27001:2022.		.1
	تنفيذMicrosoft Defender • تفعيل الحماية للأجهزة والخوادم من التهديدات السيبرانية. • إعداد سياساتASR. الأساسية • إعداد الاستجابة التلقائية للحوادث. • تفعيلthreat detection.		• Microsoft Defender for Endpoint مفعّل وجاهز للتشغيل • سياسات حماية معتمدة للأجهزة الطرفية. • تقارير اختبار وقبول. • أدلة استخدام وتشغيل وتدريب
	تنفيذMicrosoft Intune • إعداد آلية تسجيل الأجهزة. • إعداد وتطبيق سياسات الامتثال. • إدارة التطبيقات. • .منع الوصول إلى أنظمة الهيئة من الأجهزة غير المتوافقة. • .تكامل Microsoft Intune معMicrosoft Defender for Endpoint.		• Microsoft Intuneمفعّل وجاهز للتشغيل • سياسات إدارة وأمن أجهزة معتمدة. • تقارير اختبار وقبول. • وثائق تشغيل وتدريب

الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الهيئة	الأنشطة المُنجزة والمواد المُسلّمة للجهة
	• Conditional Access. • مواءمة السياسات الأمنية بين الحلول • إعداد التقارير الفنية. • الاختبار والقبول		
	تنفيذMicrosoft Purview • Sensitivity labels. • Data classification. • DLP policies. (Mail, MS Teams, One Drive, SharePoint, USB, Printing, Backup) • Data lifecycle management. • eDiscovery & Audit. • مواءمة إعدادات Microsoft Purview مع سياسات أمن المعلومات وحوكمة البيانات المعتمدة لدى الهيئة • التكامل مع حلول الأمن الأخرى مثل Microsoft Defender و Entra IDعند الحاجة.		• تصنيف البيانات الحساسة وتطبيق Sensitivity Labelsعلى مستوى المؤسسة. • تطبيق سياسات منع تسرب البيانات (DLP) • تفعيل eDiscoveryوسجلات التدقيق (Audit Logs) • أدوار وصلاحيات إدارية واضحة.(RBAC)

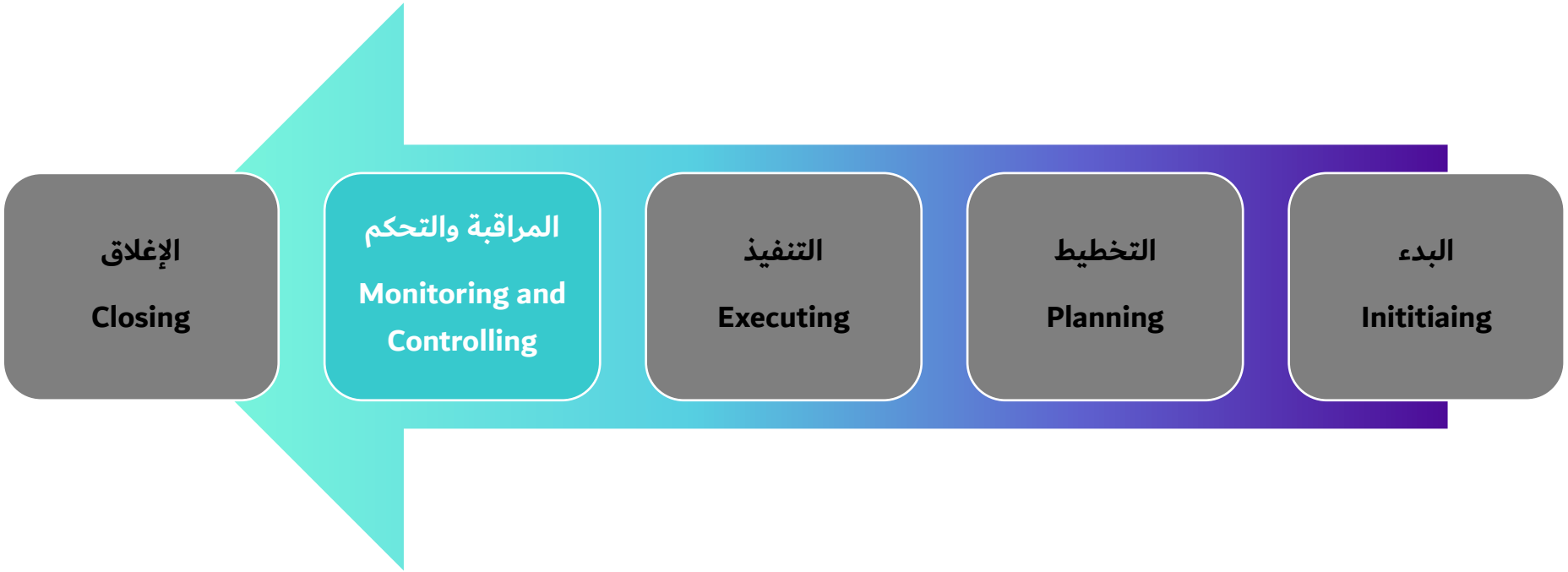
الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الهيئة	الأنشطة المُنجزة والمواد المُسلّمة للجهة
	• إعداد أدوار، وصلاحيات إدارية، واضحة، ومعتمدة		

	تنفيذ النسخ الاحتياطي والتعافي Microsoft 365 Backup و Azure Backup.
	• Azure Site Recovery.
	• تقديم خطة تفصيلية تشمل:
	  • تحليل الوضع الحالي.
	  • خطة زمنية للتنفيذ.
	  • سياسات RTO/RPO واضحة
	• تشفير البيانات أثناء النقل والتخزين
	• اختبار الاستعادة.
			• حلول نسخ احتياطي وتشغيل جاهزة.
			• تقارير اختبار واستعادة.
			• خطة استمرارية الأعمال لإدارة التقنية تشمل Backup Policy & Disaster Recovery Guide
			• تفعيل خدمة Microsoft 365 Backup لحماية:
			  • البريد الإلكتروني(Exchange Online)
			  • الملفات.(OneDrive, SharePoint)
			  • محادثات.Teams
			• تفعيل خدمة Azure Backup لحماية:
			  • الخوادم التقليدية والافتراضية (VMs) الموجودة بالهيئة وكذلك المستضافة على بيئة. aws
			  • قواعد البيانات.

	التكامل بين الحلول		

الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الهيئة	الأنشطة المُنجزة والمواد المُسلّمة للجهة
	• Defender + Intune • Purview + Microsoft 365 • Azure security integration		

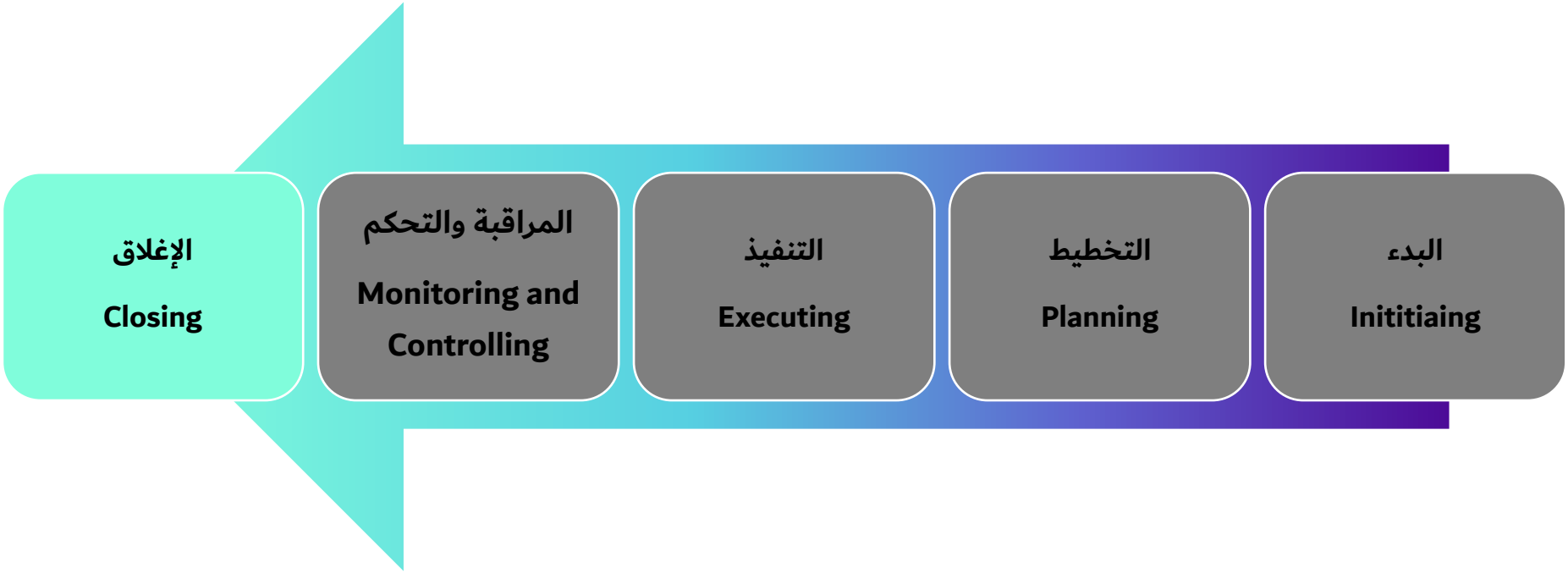
3.4 مرحلة المراقبة والتحكم



في هذه المرحلة تتم مراقبة أعمال المشروع وتتم مراقبة الأداء والتغييرات ويتم تعديل خطة المشروع حسب التغييرات الموافق عليها إن وجدت أهم مخرجات هذه المرحلة تقارير أداء الأعمال والتغييرات وتحديث خطة المشروع. كما يحتوي الجدول أدناه على الأنشطة التي سيتم القيام بها في هذه المرحلة:

الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الهيئة	الأنشطة المُنجزة والمواد المُسلّمة للجهة
	تقارير الأداء • Weekly Status Reports. • KPI Monitoring. • Security compliance reports.		تقارير الأداء

3.5 مرحلة الإغلاق



في هذه المرحلة يتم التحقق من جميع مخرجات المشروع والتأكد من تحقيق أهداف المشروع وتوثيق الدروس المستفادة من المشروع والحصول على الموافقة النهائية لمخرجات المشروع وإعلان إغلاق المشروع بشكل رسمي. كما يحتوي الجدول أدناه على الأنشطة التي سيتم القيام بها في هذه المرحلة:

الرقم	الأنشطة التي يجب أن تقوم بها شركة الرؤيا الموثوقة	الأنشطة التي يجب أن تقوم بها الهيئة	الأنشطة المُنجزة والمواد المُسلّمة للجهة
1	1. التأكد من استكمال المخرجات 2. كتابة الدروس المستفادة 3. توقيع وثيقة إغلاق المشروع 4. نقل المعرفة النهائي	1. الموافقة على المخرجات 2. المشاركة في كتابة الدروس المستفادة 3. التوقيع على وثيقة إغلاق المشروع	1. توثيق الدروس المستفادة 2. وثيقة إغلاق المشروع

16 نقل المعرفة

يتضمن نقل المعرفة، نقل المعارف من الاستشاري الى منسوبي الجهة والتدريب بهدف القيام بالأعمال التي كان يقوم بها الاستشاريون وتمكين موظفي الهيئة من القدرة على القيام بكافة أعمال الاستشاريون بثقة وتمكن.

سيتم نقل المعرفة لمنسوبي الجهة عن طريق الجدول التالي:

ماذا (المحتوى)	متى	من (الإدارة المستهدفة)	كيف (قنوات التواصل)
نقل المعرفة لفريق الأمن السيبراني جميع الوثائق والخطط المتعلقة بالمشروع • مشاركة وتوزيع الوثائق والسياسات • تبادل المعلومات حول التهديدات والهجمات والتقنيات الجديدة • بث المعلومات عبر منصات تبادل المعلومات • تطبيق أفضل الممارسات.	بشكل يومي خلال جميع مراجل المشروع	• محاضرات ودورات وورش عمل تدريبية • تقارير تهديدات	• الاجتماعات المرئية • الاجتماعات الحضورية

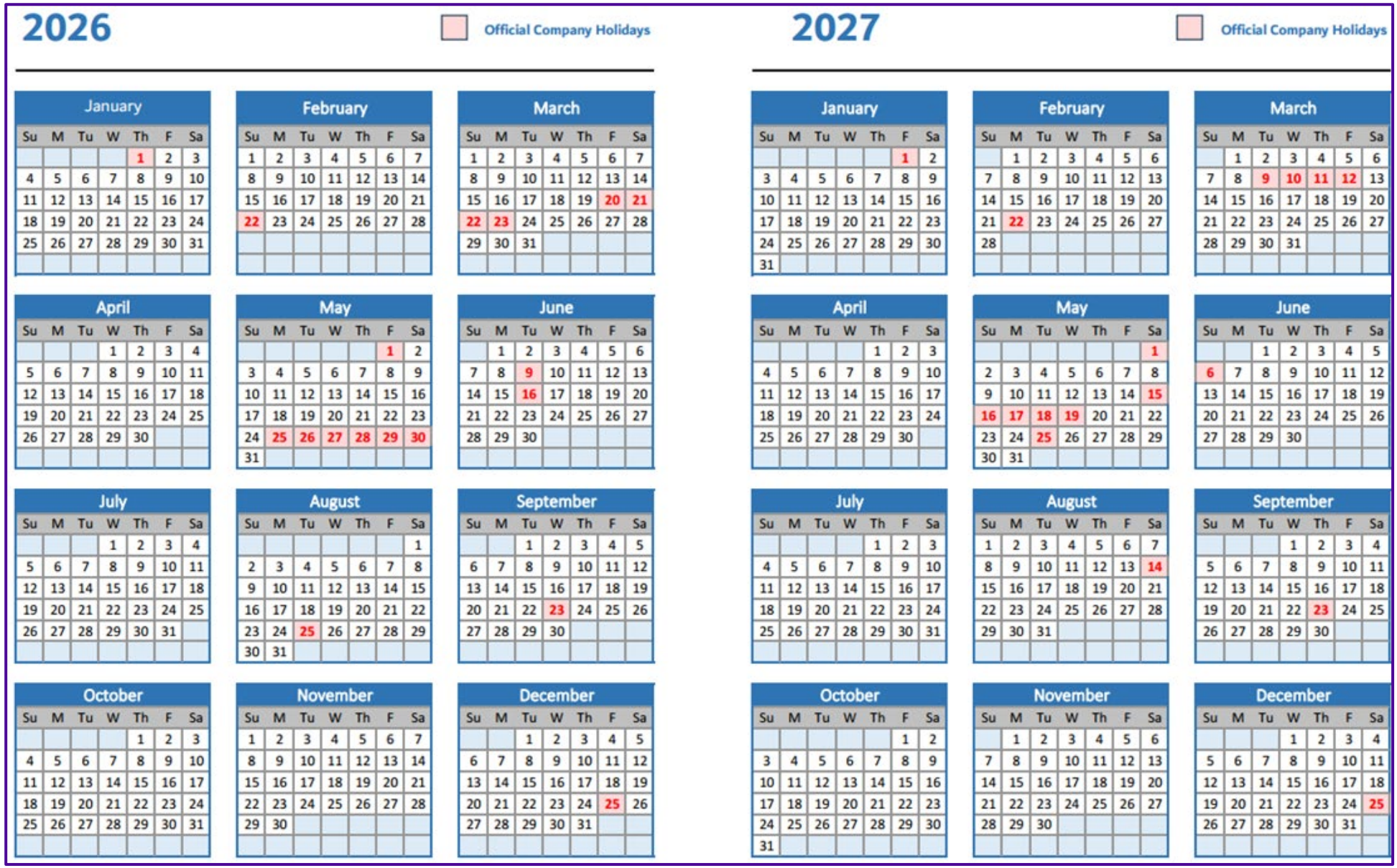
17 تقرير سير عمل المشروع الأسبوعي

يوضح الجدول أدناه تقدم المشروع بشكل أسبوعي لضمان تحقيق الأهداف وفقًا للجدول الزمني المخطط. يتم تقسيم التقرير إلى أربعة محاور رئيسية:

1. منجزات الأسبوع الحالي: تشمل جميع الأنشطة والمهام المكتملة خلال الأسبوع.
2. منجزات الأسبوع القادم: تحديد المهام والأنشطة المخطط تنفيذها لضمان الاستمرارية.
3. التحديات: استعراض العقبات التي قد تؤثر على سير العمل، مع تحديد الجوانب التي تحتاج إلى حلول.
4. التوصيات: تقديم اقتراحات لتحسين الأداء، وتقليل التحديات المحتملة، وضمان كفاءة العمليات.

اسم المشروع مدير المشروع (من طرفكم)		مدير المشروع (الرؤيا الموثوقة)	
منجزات الأسبوع الحالي	1		
منجزات الأسبوع القادم	1		
التحديات	1		
التوصيات	1		

18 تقويم الشركة



19 خطط الموارد والجودة والتواصل

يقوم مدير المشروع في مرحلة التخطيط بعمل مجموعة من الخطط من أجل تنفيذ المشروع على أفضل وجه ومنها خطة للموارد وخطة للجودة وخطة للتواصل كما يلي:

- في خطة الموارد يتم حصر الموارد المتوفرة وتحديد المتطلبات والأولويات وتوزيع الموارد حسب الأولويات.
- في خطة الجودة يتم تحديد معايير الجودة من أجل تطبيقها في المشروع مثل طرق سير العمل والوقت اللازم لمراجعة الوثائق وآليات مراجعة الوثائق واعتمادها.
- في خطة التواصل يتم تحديد أفضل طرق للتواصل حسب احتياجات أصحاب المصلحة ويتم تدوين الخطة ولعمل بها

تعد الخطط المذكورة جزء مهم في إدارة المشاريع، والهدف منها تحديد كيفية تجهيز الموارد وإدارة الجودة وكيفية التواصل خلال حياة المشروع. حيث تشمل كل أدوار أصحاب المصلحة.

20 المخاطر عالية المستوى

تم تحديد أهم المخاطر عالية المستوى في المشروع كما في الجدول أدناه

رقم الخطر	سيناريو الخطر	المستوى الإجمالي	ضوابط التعامل مع الخطر
1	عدم تعاون منسوبي الجهة وبالتالي حصول تأخير في التسليمجات	عالي	1- تخصيص مدير للمشروع من الجهة وتفريغه للعمل مع الاستشاريين 2- إعطاء رسالة وأمر من صاحب الصلاحية لجميع الإدارات بضرورة التعاون مع الاستشاريين لضمان إتمام المشروع خلال الوقت المحدد
2	عدم رضى الجهة عن الوثائق المسلّمة	متوسط	تطوير خطة جودة وتفعيلها بين الشركة وبين الجهة
3	استقالة أحد الاستشاريين خلال عمل المشروع	منخفض	1- توفير استشاريين آخرين للاحتياط من قبل الشركة

21 الجدول الزمني التقريبي لتنفيذ المشروع

مدة المشروع هي 12 شهرا مع الملاحظة أن الجدول الزمني التالي تقريبي وغير مفصل لتسهيل العرض على الشاشة وإظهار التداخل بين الأنشطة.

م	المرحلة	الشهر											
		1	2	3	4	5	6	7	8	9	10	11	12
1	المرحلة 1												
2	المرحلة 2												
3	المرحلة 3												
4	المرحلة 4												
5	المرحلة 5												

22 الضمان الابتدائي

بما أن شركة الرؤيا الموثوقة تعتبر منشأة صغيرة وحسب الأحكام العامة للضمانات تعفى الشركة من تقديم الضمان الابتدائي.

افتراضات

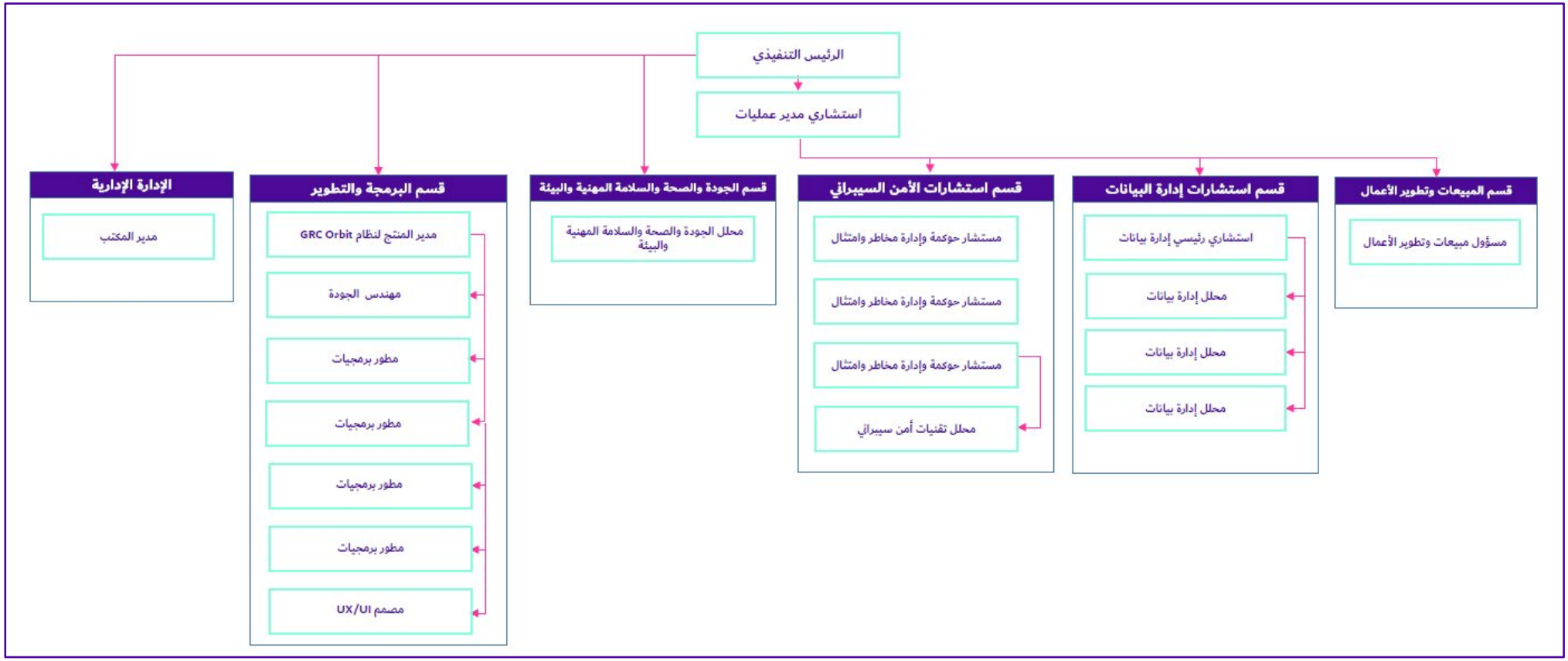
- أي خدمة أخرى لم يتم ذكرها بوضوح في الأقسام السابقة سيتم اعتبارها خارج نطاق العمل.
- تنفيذ أو تطبيق أي ضابط من الضوابط الأساسية للأمن السيبراني.
- التعاون من أقسام وإدارات الجهة إلزامي لنجاح المشروع.
- فترة مراجعة الوثائق وإبداء الملاحظات هي ثلاثة (3) أيام عمل.
- مدة تنفيذ المشروع هي سنة عمل فقط.
- يتضمن العرض المراجعة مرة واحدة فقط للوثائق المسلمة.
- سيتم إضافة بوت ذكاء اصطناعي لتسجيل المحادثات وتلخيصها، بهدف مساعدة الاستشاريين في تحسين محاضر الاجتماعات وتطويرها.
- يحق للشركة إيقاف المشروع بشكل مؤقت في حال عدم تسديد الدفعة خلال أسبوعين من تاريخ إصدار الفاتورة وإرسالها للجهة

خارج نطاق العمل

- أي خدمة أخرى لم يتم ذكرها بوضوح في الأقسام السابقة سيتم اعتبارها خارج نطاق العمل.
- تنفيذ أو تطبيق أي ضابط من الضوابط الأساسية للأمن السيبراني.

23 معلومات عن الشركة

شركة الرؤيا الموثوقة هي شركة استشارية تعمل في مجال الأمن السيبراني وإدارة البيانات وتقدم خدمات كاملة في مجال إدارة الحوكمة والمخاطر والامتثال، بالإضافة إلى حلول وتدريبات، لمساعدة الجهات على تلبية متطلبات أعمالهم. ما يميزنا هو القيم الجوهرية التي نتبناها.



24 الشهادات

يحمل فريقنا مجموعة متنوعة من الشهادات، بما في ذلك ما يلي:

CISSP® CISM CGEIT CRISC CISA COBIT 2019 Foundation An ISACA® Certificate

PECB ISO/IEC 27001 SENIOR LEAD IMPLEMENTER

PECB ISO/IEC 27001 SENIOR LEAD AUDITOR

PECB ISO/IEC 27032 LEAD CYBERSECURITY MANAGER

PECB ISO/IEC 38500 LEAD IT CORPORATE GOVERNANCE MANAGER

PECB ISO 31000 LEAD RISK MANAGER

PECB ISO/IEC 27005 SENIOR LEAD RISK MANAGER

PECB DATA PROTECTION OFFICER

PECB ISO 22301 FOUNDATION

PECB ISO/IEC 20000 FOUNDATION

PECB ISO 45001 LEAD AUDITOR

PECB ISO 14001 LEAD AUDITOR

PECB ISO 9001 LEAD IMPLEMENTER


PECB
ISO 9001
LEAD AUDITOR


ITIL
FOUNDATION


CompTIA
CCAP
Cloud Admin
PROFESSIONAL


CompTIA
CSCP
Secure Cloud
PROFESSIONAL


CompTIA
Data+


CompTIA
Cloud+


CompTIA
CySA+


CompTIA
Network+


CompTIA
A+


CompTIA
Security+


CNSS


FORTINET
NSE
1
ASSOCIATE


FORTINET
NSE
2
ASSOCIATE


FORTINET
NSE
3
ASSOCIATE


FORTINET
NSE
4
PROFESSIONAL


C|EH
Certified Ethical Hacker


paloalto
NETWORKS
PCCSA


paloalto
NETWORKS
PCNSA


paloalto
NETWORKS
PCNSE


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
CISA
CYBER+INFRASTRUCTURE


ASSOCIATE
CERTIFIED

25 المشاريع السابقة التي تم تنفيذها

تم تنفيذ العديد من المشاريع من خلال التعامل مع جهات متنوعة في دول مختلفة وبيئات متعددة ونسعى دائمًا إلى تنفيذ أفضل الممارسات والمعايير من أجل تحقيق أفضل النتائج المطلوبة

رقم المشروع	اسم المشروع	اسم العميل أو الجهات المستفيدة	الشعار	وصف المشروع

1	تنفيذ إطار عمل الأمن السيبراني SAMA CSF	شركة اتحاد الخليج والأهلية للتأمين		• تطوير سياسات وإجراءات ومعايير الأمن السيبراني الصادرة من البنك المركزي السعودي • إجراء تقييم المخاطر Cybersecurity Risk Assessmentعلى الأنظمة والأصول المعلوماتية والعمليات • تطوير مؤشرات الأداء الرئيسية ومؤشرات المخاطر الرئيسية للعمليات(KPIs) ، KRIs) • أداء مراقبة العمليات

2	تنفيذ نظام إدارة استمرارية الأعمال SAMA BCM	شركة اسيج للتأمين		• إنشاء نظام إدارة استمرارية الأعمال • تطوير السياسات والإجراءات والمعايير ذات الصلة • تحديد وتنفيذ تحليل تأثير الأعمال • إجراء تقييم لمخاطر استمرارية الأعمال • تحديد هدف وقت الاستعادة (RTO)وهدف نقطة الاستعادة (RPO) • وضع استراتيجية استمرارية الأعمال • تطوير خطط استمرارية الأعمال • تحديد مقاييس الأداء ومؤشرات الأداء الرئيسية
3	تنفيذ برنامج استمرارية الأعمال والتعافي من الكوارث	شركة التصنيع وخدمات الطاقة (طاقة)		• إنشاء نظام إدارة استمرارية الأعمال • تطوير السياسات والإجراءات والمعايير ذات الصلة

				• تحديد وتنفيذ تحليل تأثير الأعمال • إجراء تقييم لمخاطر استمرارية الأعمال • تحديد هدف وقت الاستعادة (RTO)وهدف نقطة الاستعادة (RPO) • وضع استراتيجية استمرارية الأعمال • تطوير خطط استمرارية الأعمال • تحديد مقاييس الأداء ومؤشرات الأداء الرئيسية
4	تنفيذ معيار ISO 27001 وضوابط الأمن السيبراني الأساسية (ECC,CCC,DCC,OSMACC,TCC)	شركة التصنيع وخدمات الطاقة (طاقة)		• إنشاء نظام إدارة الأمن السيبراني • تطوير استراتيجية الأمن السيبراني والنموذج التشغيلي • تطوير السياسات والإجراءات والمعايير ذات الصلة • ضمان الامتثال لأطر الهيئة ECC, CCC, DCC, OSMACC, TCC • ضمان الامتثال لمعيار ISO 27001

				• إجراء التدقيق الداخلي على أطر الهيئة ومعيار الآيزو 27001 • الحصول على شهادة الأيزو 27001
5	التدقيق والإشراف على تنفيذ الضوابط الأساسية للأمن السيبراني NCA-ECC	جهة حكومية سيادية		• التحسين على وثائق الحوكمة (استراتيجية الأمن السيبراني، الأدوار والمسؤوليات بالأمن السيبراني، سياسات الأمن السيبراني) • التدقيق على الضوابط الأساسية للأمن السيبراني NCA-ECC
6	تدقيق أنظمة تقنية المعلومات	شركة ليبارا اتصالات	LEBARA ليبارا موبايل	تدقيق السياسات والإجراءات المتعلقة بتقنية المعلومات (الضوابط التقنية العامة + الضوابط التقنية على التطبيقات)
7	تدريب معيار أمن المعلومات ISO 27001	شركة التصنيع وخدمات الطاقة (طاقة)	TAQA	• تقديم التدريب في معيار أمن المعلومات ISO 27001

8	استراتيجية إدارة وحوكمة البيانات	مكتبة الملك عبد العزيز العامة		• إجراء تحليل الفجوات المتعلق بإطار عمل الضوابط الوطنية لإدارة وحوكمة البيانات • دراسة الوضع الراهن • تطوير استراتيجية إدارة البيانات • تطوير خطة البيانات المفتوحة • نشر ست مجموعات من البيانات المفتوحة على المنصة السعودية للبيانات الوطنية
9	تنفيذ معيار أمن المعلومات ISO 27001	Genelle	genelle	• إنشاء نظام إدارة أمن المعلومات • تطوير السياسات والإجراءات والمعايير ذات الصلة • ضمان الامتثال لمعيار ISO 27001 • إجراء أنشطة التصحيح وحل الاستنتاجات • الحصول على شهادة الأيزو 27001
10	تنفيذ ضوابط أرامكو للأمن السيبراني	Maham	Maham مهام	• تنفيذ معيار أرامكو للأمن السيبراني SACS-002

	Saudi Aramco Cybersecurity Implementation			• تطوير السياسات والإجراءات والمعايير ذات الصلة
11	تصنيف البيانات Data Classification	Perfect Presentation	شركة العرض المتقن Perfect Presentation	• حصر وتصنيف جميع البيانات • تطوير السياسات والإجراءات والمعايير المتعلقة بتصنيف وحماية البيانات
12	تنفيذ معيار أمن المعلومات ISO 27001 وضوابط الأمن السيبراني الأساسية (ECC,CCC,DCC,OSMACC,TCC)	البرنامج الوطنية للتنمية المجتمعية (تنمية)	تنمية البرنامج الوطني للتنمية المجتمعية في المناطق	• إنشاء نظام إدارة الأمن السيبراني • تطوير استراتيجية الأمن السيبراني والنموذج التشغيلي • تطوير السياسات والإجراءات والمعايير ذات الصلة • ضمان الامتثال لأطر الهيئة ECC, TCC CCC, DCC, OSMACC, • ضمان الامتثال لمعيار ISO 27001 • إجراء التدقيق الداخلي على أطر الهيئة ومعيار الآيزو 27001 • الحصول على شهادة الأيزو 27001

13	إدارة مخاطر الأمن السيبراني	جهة حكومية سيادية		• تطوير منهجية إدارة مخاطر الأمن السيبراني وموائمتها مع المنهجية العامة لإدارة المخاطر • إجراء تقييم مخاطر الأمن السيبراني على الأصول المعلوماتية + الأطراف الثالثة + التغييرات الجوهرية + المشاريع التقنية + العمليات
14	NCA-ECC and CCC-P	Nashirnet		• إنشاء نظام إدارة الأمن السيبراني • تطوير السياسات والإجراءات والمعايير الخاصة بضوابط الحوسبة السحابية وبالضوابط الأساسية ECC + CCC لمزودي الخدمة • إجراء تقييمات لمخاطر الأمن السيبراني على المشاريع والمنتجات • إجراء التدقيق الداخلي • تطوير وقياس مؤشرات قياس الأداء

15	تصنيف ونمذجة البيانات	مكتبة الملك عبد العزيز العامة		• تطوير سجل البيانات • تصنيف البيانات • تطوير خطة نمذجة البيانات والقيام بالنمذجة لأنظمة المكتبة
16	تنفيذ نظام ولائحة حماية البيانات الشخصية PDPL	Aljaber Finance		• حصر البيانات الشخصية وأنشطة المعالجة • تطوير السياسات والمعايير والإجراءات ذات الصلة بخصوصية البيانات • تطوير عمليات إدارة الموافقات • إجراء التدقيق على عمليات أنشطة معالجة البيانات • تنفيذ ورشات توعوية في حماية البيانات الشخصية
17	تنفيذ نظام ولائحة حماية البيانات الشخصية PDPL	Hala Payment		• حصر البيانات الشخصية وأنشطة المعالجة • تطوير السياسات والمعايير والإجراءات ذات الصلة بخصوصية البيانات • تطوير عمليات إدارة الموافقات

				• إجراء التدقيق على عمليات أنشطة معالجة البيانات • تنفيذ ورشات توعوية في حماية البيانات الشخصية
	تنفيذ نظام ولائحة حماية البيانات الشخصية PDPL	Mrna Finance		• حصر البيانات الشخصية وأنشطة المعالجة • تطوير السياسات والمعايير والإجراءات ذات الصلة بخصوصية البيانات • تطوير عمليات إدارة الموافقات • إجراء التدقيق على عمليات أنشطة معالجة البيانات • تنفيذ ورشات توعوية في حماية البيانات الشخصية
18	تنفيذ إطار عمل الأمن السيبراني SAMA CSF	FinZey		• تطوير سياسات وإجراءات ومعايير الأمن السيبراني الصادرة من البنك المركزي السعودي • إجراء تقييم المخاطر Cybersecurity Risk Assessmentعلى الأنظمة والأصول المعلوماتية والعمليات

				• تطوير مؤشرات الأداء الرئيسية ومؤشرات المخاطر الرئيسية للعمليات (KPIs) ، (KRIs • أداء مراقبة العمليات
19	تأسيس مكتب إدارة البيانات	EXPRO	EXPRO هيئة كفاءة الإنفاق والمشروعات الحكومية Expenditure & Projects Efficiency Authority	• إجراء تحليل الفجوات المتعلق بإطار عمل الضوابط الوطنية لإدارة وحوكمة البيانات • دراسة الوضع الراهن • تطوير استراتيجية إدارة البيانات • تطوير نموذج تشغيلي • حصر وتصنيف البيانات • تطوير السياسات والمعايير والإجراءات ذات الصلة بإدارة البيانات • زيادة مستوى لنضج المتعلقة بالبيانات

13 طاقم العمل

الرقم	الاسم	المنصب الوظيفي	المستوى الدراسي	سنوات الخبرة	الخبرات
1	هـ. ع	مستشار تنظيم الأعمال والحوكمة وإدارة المخاطر (GRC) للرئيس التنفيذي	بكالوريوس هندسة الحاسوب	11 سنوات	• إدارة وإجراء مراجعات تشغيلية وعملية ملتزمة بمتطلبات الأمن السيبراني لشركة النفط العربية السعودية (ساس 002)، ومعايير ISO 27001، وNCA-ECC وNIST SP 800-53. • إدارة وتطوير سياسات وإجراءات الحوكمة في مجال الأمن السيبراني مخصصة باللغة العربية والإنجليزية وفقًا لمعايير ISO 27001، وNIST، وNCA، ومعيار الأمن السيبراني لشركة النفط العربية السعودية. • إدارة مخاطر الأمن السيبراني وإجراء تقييمات المخاطر الأمن السيبراني وتقييمات مخاطر تقنية المعلومات وفقًا للمعايير الوطنية والدولية. • تنفيذ ومراجعة نظام إدارة أمان المعلومات في المؤسسة وفقًا لمعيار ISO 27001 والهيئة (NCA-KSA). • إدارة وتنفيذ نظام إدارة استمرارية الأعمال في المؤسسة وفقًا لمعيار ISO 22301..
2	ب. ع	مستشار حوكمة وإدارة المخاطر (GRC)	ماجستير في الأمن السيبراني	2 سنة	• إدارة وإجراء مراجعات تشغيلية وعملية وفقًا لمتطلبات الأمن السيبراني لشركة أرامكو السعودية ISO 27001 (SACS-002)، وNCA-ECC، وNIST SP 800-53.

					• إدارة وتطوير سياسات وإجراءات الحوكمة الخاصة بالأمن السيبراني بشكل مخصص باللغتين العربية والإنجليزية وفقًا للمعايير ISO 27001، وNIST، وNCA، ومعايير الأمن السيبراني لشركة أرامكو. • إدارة مخاطر الأمن السيبراني وإجراء تقييمات للمخاطر السيبراني وتقييمات المخاطر التكنولوجية ضد المعايير الوطنية والدولية. • تنفيذ وتدقيق نظام إدارة أمان المعلومات في المؤسسة استنادًا إلى ISO 27001 وهيئة الأمن السيبراني الوطنية (NCA-KSA).
3	غ ح	مستشار حوكمة وإدارة المخاطر (GRC)	بكالوريوس في الأمن السيبراني	3 سنوات	• إدارة وإجراء مراجعات تشغيلية وعملية وفقًا لمتطلبات الأمن السيبراني لشركة أرامكو السعودية ISO 27001 (SACS-002)، وNCA-ECC، وNIST SP 800-53. • إدارة وتطوير سياسات وإجراءات الحوكمة الخاصة بالأمن السيبراني بشكل مخصص باللغتين العربية والإنجليزية وفقًا للمعايير ISO 27001، وNIST، وNCA، ومعايير الأمن السيبراني لشركة أرامكو. • إدارة مخاطر الأمن السيبراني وإجراء تقييمات للمخاطر السيبراني وتقييمات المخاطر التكنولوجية ضد المعايير الوطنية والدولية. • تنفيذ وتدقيق نظام إدارة الأمن السيبراني في الشركة استنادًا إلى ISO 27001 وهيئة الأمن السيبراني الوطنية (NCA-KSA).
4	أ ي	مستشار حوكمة وإدارة المخاطر (GRC)	ماجستير امن سيبراني	1 سنوات	• إدارة وإجراء مراجعات تشغيلية وعملية وفقًا لمتطلبات الأمن السيبراني لشركة أرامكو السعودية ISO 27001 (SACS-002)، وNCA-ECC، وNIST SP 800-53.

					• إدارة وتطوير سياسات وإجراءات الحوكمة الخاصة بالأمن السيبراني بشكل مخصص باللغتين العربية والإنجليزية وفقًا للمعايير ISO 27001، وNIST، وNCA، ومعايير الأمن السيبراني لشركة أرامكو.

13 فريق العمل

غيداء حسن حران

المسمى الوظيفي: استشاري حوكمة وإدارة مخاطر وامتثال

سنوات الخبرة: 5 سنوات

ملخص مهني

استشاري في حوكمة البيانات والأمن السيبراني، أتمتع بخبرة واسعة في دعم الجهات الحكومية والخاصة للامتثال لضوابط الهيئة الوطنية للأمن السيبراني (NCA) وإطار حوكمة البيانات الوطنية (NDMO) الصادر من الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA)، كما أسهم في رفع جاهزية الجهات لتحقيق متطلبات مؤشر نُضيء الوطني لقياس نضج حوكمة البيانات، من خلال تقييم الفجوات، وتقديم خطط التحسين، وبناء قدرات الكوادر. لدي خبرة في تصنيف البيانات وحمياتها ، حماية البيانات الشخصية وفق نظام حماية البيانات الشخصية (PDPL)، وإعداد خطط التوعية والتدريب، إضافة إلى دعم مشاريع التحول الرقمي بما يعزز الخصوصية والأمن في التعامل مع البيانات.

الشهادات الاحترافية

1. ISO/IEC 27001:2022 Lead Implementer 2024 – PECP
2. ISO/IEC 27005:2022 Risk Manager 2024 – PECP
3. Completed a specialized training course on ISO/IEC 27701 – Privacy Information Management System (PIMS).
4. Completed a specialized training course on ISO 31000 Risk Management Aug/ 2023 - Trusted Vision

المهارات

المهارات التقنية

- الامتثال لمتطلبات نظام ولوائح حماية البيانات الشخصية
- تصنيف البيانات
- تقييم مخاطر الأمن السيبراني ومخاطر الخصوصية
- تحليل البيانات
- تطوير السياسات والإجراءات

المهارات الشخصية

- العمل الجماعي والتعاون ضمن الفريق
- التطوير المهني المستمر
- الاستماع الفعّال
- التفكير التحليلي
- حل المشكلات
- إدارة الوقت

العملاء والمشاريع

- **تنفيذ وتطبيق نظام ولوائح حماية البيانات الشخصية**
- **الإشراف على تطبيق نظام ولائحة حماية البيانات الشخصية**
- **تنفيذ وتطبيق نظام إدارة امن المعلومات ISO 27001:2022**
- **المساعدة في تنفيذ مشروع تنفيذ إطار حوكمة تقنية المعلومات من مؤسسة النقد العربي السعودي**
- **مستشار الحوكمة والمخاطر والامتثال والخصوصية**
- **الإشراف على مشروع تنفيذ اللائحة العامة لحماية البيانات General Data Protection Regulation (GDPR)**
- **تكوين وإعداد أدوات Microsoft، بما يشمل تهيئة الأجهزة وتطبيق السياسات الأمنية والإدارية ضمن Microsoft Endpoint Manager (Intune)**

المؤهل العلمي

بكالوريوس هندسة حاسوب
جامعة الحسين بن طلال، الأردن– 2021
المعدل التراكمي: 80

Restricted

عبد الله العزيزي

- **المسمى الوظيفي:** محلل تقنيات أمن سيبراني
- **سنوات الخبرة: 2**

ملخص مهني

محلل تقنيات أمن سيبراني أتمتع بخبرة عملية في مجالات الشبكات، أمن المعلومات، وهندسة المؤسسات. عملت خلال مسيرتي في شركات تقنية مثل شركة Huawei كمهندس شبكات، وشركة TSME كمهندس بنية مؤسسية، حيث ساهمت في فهم البنية التحتية الشبكية وتصميم البنى المؤسسية للشركات. كما لدي القدرة على دعم الجهات الحكومية والخاصة للامتثال لضوابط الهيئة الوطنية للأمن السيبراني (NCA) وإطار حوكمة البيانات الوطنية (NDMO) الصادر من الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) و، حماية البيانات الشخصية وفق نظام حماية البيانات الشخصية (PDPL) من الناحية التقنية.

الشهادات الاحترافية

1. Cisco Packet Tracer for Beginners - Udemy
2. CCNA Course – Cisco
3. HCIA Datacom Course - Huawei
4. A+ Course – Pioneers Academy
5. COBIT 2019 training
6. CC – ISC2

المهارات

المهارات التقنية

- Programming Languages: Assembly 8086, C, C++, Python
- Network and Security Skills
- Hardware Skills
- Packet Tracer

المهارات الشخصية

- Time Commitment
- Detail Oriented
- Teamwork Layer
- Self Improvement
- Turkish Language

العملاء والمشاريع

- **إعداد سياسات الامتثال لمعيار ISO 27001 (Genelle)**
  إعداد وتطوير سياسات وإجراءات أمن المعلومات لشركة Genelle بهدف تحقيق الامتثال لمتطلبات معيار ISO/IEC 27001. شمل ذلك تحديد ضوابط الأمن المطلوبة، وتوثيق السياسات التشغيلية والإجرائية الداعمة، وضمان مواءمة البيئة التقنية مع متطلبات النظام، مما يدعم حماية البيانات وتحسين جاهزية الشركة للحصول على شهادة الاعتماد.
- **تدقيق وتنفيذ ضوابط حماية البيانات NCA-DCC (EXPRO)**
- **تدقيق ضوابط حماية البيانات NCA-DCC (وزارة الموارد البشرية HRSD)**
- **تدقيق على إطار CRF (Emdad Digital)**

المؤهل العلمي

- **بكالوريوس هندسة حاسوب**
  جامعة الأميرة سمية للتكنولوجيا، عمّان– 2023
  المعدل التراكمي: جيد

Restricted