إطار عمل إدارة أمن المعلومات

سبتمبر/2019

إصدارات الوثيقة:

الإصدار	الإعداد	التاريخ	التغييرات
1.0	رشا العبدلي	30.07.2017	النسخة الأولى

الفهرس

الوثائق ذات الصلة

- سياسة إدارة أمن المعلومات, 2019
- سياسة حوكمة تقنية المعلومات, 2018
- إطار عمل إدارة مخاطر تقنية المعلومات, 2017
- إطار المعايير التقنية للحكومة الإلكترونية (OeGaf), 2018
- الضوابط الضوابط الأساسية لأمن المعلومات, 2017
- إطار عمل استمرارية -خدمات تقنية المعلومات , 2018
- إطار عمل بنية أمن الشبكات الحكومية, 2015
- إطار عمل بنية أمن المعلومات في التطبيقات الحكومية والخدمات الإلكترونية, 2016
- إطار عمل بنية أمن الأجهزة الطرفية, 2017

القوانين والتشريعات ذات الصلة

- قانون المعاملات الإلكترونية, 2008
- تعميم إنشاء مكاتب أمن المعلومات في وحدات الجهاز الإداري للدولة، أ ع م و / 3367/102
- المرسوم السلطاني 2011/118 لتصنيفات أمن البيانات

2. المقدمة

يضم إطار عمل إدارة أمن المعلومات أفضل الممارسات والخبرات السابقة في هذا المجال من أجل مساعدة الجهات الحكومية في تنفيذ برنامج أمن المعلومات بنجاح وتمكين تلك المؤسسات لتحقيق أهدافها الرئيسية.

إن الغاية الأساسية من تأطير عمل برنامج أمن المعلومات داخل وحدات الجهاز الإداري للدولة هو تقديم أداة فعّالة لتحقيق القيمة الفعلية لها وتكون قابلة للقياس والاستمرارية والتحسين المستمر.

3. الهدف من الوثيقة

تم وضع هذا الإطار للمساعدة في إدارة برنامج أمن المعلومات في وحدات الجهاز الإداري للدولة والتأكد من أن جميع العمليات والأشخاص والأنظمة محمية بشكل كاف أثناء القيام بالأعمال المختلفة التي تحقق أهداف قطاع الأعمال.

4. القطاعات المستهدفة

يستهدف إطار عمل إدارة أمن المعلومات مسؤولي أمن المعلومات في الجهات الحكومية المسؤولين عن إدارة أمن المعلومات في هذه الجهات. كما يمكن استخدام إطار العمل من قبل المختصين في المستويات الإدارية من أجل بناء فهم واسع للعناصر الرئيسية التي يتطلبها تبني أفضل الممارسات في أمن المعلومات.

5. نطاق العمل

يغطي إطار العمل جميع النواحي المتعلقة بإنشاء وإدارة برنامج أمن المعلومات في المؤسسات كما يتضمن تحديد العناصر الأساسية الواجب مراعاتها لضمان فعالية واستمرارية هذا البرنامج. وبما أن أمن المعلومات في المؤسسات هو عملية مستمرة، فلقد اشتمل إطار العمل على جميع المكونات اللازمة للحماية على مختلف المستويات :كالأفراد والعمليات والبنى والتقنيات، حيث تتكامل هذه المكونات لتكون محور أعمال الإدارة الأمنية اليومية.

6.مبادئ أمن المعلومات

هناك ثلاث مبادئ في أمن المعلومات هي سرية المعلومات وسلامة المعلومات وتوفر المعلومات، وتستخدم هذه المبادئ كأهداف رئيسية ينبغي تحقيقها في أي برنامج لأمن المعلومات. وتعرّف هذه المبادئ كما يلي:

- **سرية المعلومات**

ضمان الدخول المصرح فقط إلى المعلومات وتقييد الكشف عن المعلومات، بما في ذلك ضمان حماية الخصوصية الشخصية والمعلومات الخاصة.

- **سلامة المعلومات**

حماية المعلومات من التلف أو التعديل الغير صحيح وضمان صحة المعلومات وصحة مصدرها.

- **توفر المعلومات**

ضمان الوصول الموثوق للمعلومات في الوقت المناسب لإستخدامها.

7.كيفية تنظيم أمن المعلومات

7.1 أصحاب المصلحة الرئيسيين

إن الهدف الرئيسي من أمن المعلومات هو ضمان استمرارية الأعمال الرئيسية للمؤسسات، أو بعبارة أخرى، تمكين المؤسسات من تحقيق اهدافها دون انقطاع وضمان توفر التدابير الأمنية الصحيحة لحماية أصول المعلومات ذات الأهمية لها. يتوجب ذلك إشراك كافة أصحاب المصلحة لضمان وضع برنامج أمني فعال وهم كالتالي :
نذكر هنا أمثلة لأصحاب المصلحة الذين يلعبون دوراً هاماً في وضع برنامج أمن المعلومات والذين يشتركون في كامل مراحل العملية:

- مسؤول أمن المعلومات
- الإدارة العليا
- تقنية المعلومات
- الموارد البشرية
- الشؤون القانونية
- الشؤون المالية والإدارية
- المشتريات والعقود

يمكن لجهات أخرى من داخل المؤسسة أن تعتبر أيضاً من أصحاب المصلحة، فعلى سبيل المثال في بعض المؤسسات يلعب قطاع التخطيط الاستراتيجي دورا محوريا عند مراجعة الإستراتيجية الأمنية التي لابد أن تكون متوائمة مع أهداف وتوجهات المؤسسة .

7.2 الهيكل التنظيمي

لابد من وجود هيكل تنظيمي محدد وواضح حيث يسهم ذلك في تحقيق وتمكين الإدارة الجيدة لبرنامج أمن المعلومات. هناك ثلاث عناصر رئيسية يجب توفرها في الهيكل التنظيمي:

1- **مكتب أمن المعلومات،** ويتبع بشكل مباشر لأعلى سلطة في المؤسسة، ويتمتع بالاستقلالية وعدم التبعية لأي وحدة إدارية أو تقنية. ولابد من الإشارة إلى الخطأ الذي تقع به المؤسسات بوضع مكتب أمن المعلومات تابعاً لقسم تقنية المعلومات، أو اعتبار قسم أمن تقنية المعلومات (المسؤول عن تطبيق الضوابط الأمنية تقنياً) مسؤولاً عن تنفيذ برنامج أمن المعلومات.

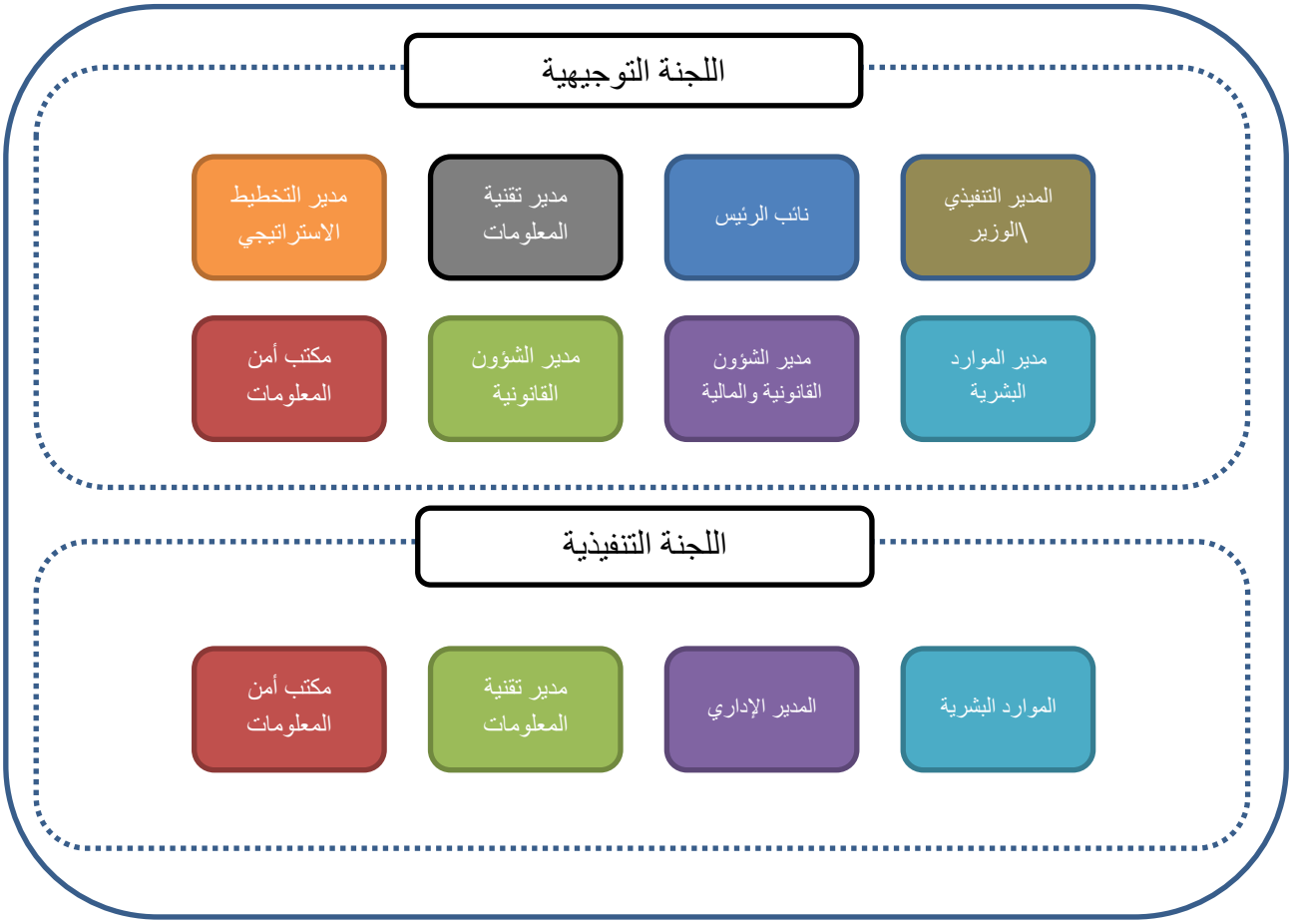
هناك اختلاف في المهام والمسؤوليات بين أمن المعلومات و أمن تقنية المعلومات لدرجة تستدعي الفصل بين القسمين، حيث يوضح الجدول التالي الفروقات بينهما:

معيار المقارنة	أمن المعلومات	أمن تقنية المعلومات
يتبع بشكل مباشر	رئيس الوحدة الحكومية (الرئيس التنفيذي أو مكتب الوزير)	مدير تقنية المعلومات
حجم الفريق	صغير (1-3)	متوسط\كبير (3+)
المهارات المطلوبة	مهارات قيادية/ مهارات إدارة الأعمال/ مهارات تقنية	مهارات تقنية
المهام الرئيسية	التنسيق والإشراف على المهام التنفيذية لبرنامج إدارة أمن المعلومات، والتأكد من قيام المعنيين بتطبيق السياسات الأمنية العامة، والقيام بتقييم المخاطر والتدقيق الدوري للتأكد من تطبيق الضوابط الأمنية وتقديم تقارير سير عمل برنامج إدارة أمن المعلومات إلى اللجنة التوجيهية المشرفة على البرنامج.	تنفيذ الضوابط الأمنية والتوصيات حسب توجيهات اللجنة التوجيهية المشرفة على البرنامج.

2- **اللجنة التوجيهية لبرنامج إدارة أمن المعلومات،** وتتكون من الإدارة العليا في المؤسسة ممثلة بأصحاب المصلحة الرئيسيين من الأقسام التي تم ذكرها في القسم السابق.

3- **اللجنة التنفيذية** ، ممثلة بالإدارة الوسطى من أصحاب المصلحة في المؤسسة، حيث تكون مهمة هذه اللجنة تطبيق الضوابط الأمنية من قبل فرقهم حسب ما يتطلبه برنامج أمن المعلومات.

فيما يلي مثال عام للهيكل التنظيمي لأمن المعلومات:



المخطط 1: الهيكل التنظيمي الخاص بمنظومة أمن المعلومات*

*إن هذا الهيكل قابل للتعديل حيث يمكن إضافة أصحاب المصلحة المرتبطة أعمالهم بأمن المعلومات، سواء في اللجنة التوجيهية أو اللجنة التنفيذية ويكون مسؤول أمن المعلومات هوه الحلقة الأساسية للتنسيق والمتابعة مع هذه اللجان حسب مقتضيات إدارة البرنامج

7.3 المهام والمسؤوليات

يجب تحديد المهام والمسؤوليات بشكل واضح في الهيكل التنظيمي من أجل ضمان الإدارة والتنفيذ الفعّال لبرنامج أمن المعلومات، ويتضمن الجدول التالي المسؤوليات الرئيسية لكل دور وظيفي مذكور سابقا:

الدور الوظيفي	المسؤوليات
الإدارة التنفيذية العليا	• وضع العمليات اللازمة للتكامل بين أمن المعلومات وأهداف المؤسسة. • التأكد من وجود إدارة جيدة للمخاطر ضمن كافة الأنشطة المرتبطة بأمن المعلومات • متابعة الإلتزام بالقوانين. • التأكد من وجود دراسات لجدوى المبادرات الأمنية وتحديد قيمة المعلومات التي تتم حمايتها. • طلب تقارير دورية لمتابعة سير عمل البرنامج و إعداد أدوات قياس مناسبة لآليات المتابعة. • التأكد من وجود آليات لقياس الفعالية واكتساب المعرفة.
اللجنة التوجيهية	• المراجعة والمساعدة في تنفيذ استراتيجية أمن المعلومات وتحقيق التكامل، وحث مدراء قطاع الأعمال والمسؤولين عن العمليات المختلفة على تفعيل هذا التكامل. • تحديد المخاطر المستجدة وتعزيز الممارسات الأمنية في قطاع الأعمال وتحديد فجوات الإلتزام بالمعايير.

	• المراجعة والتأكد من كفاية المبادرات الأمنية في خدمة قطاع الأعمال وقيمة الخدمات المقدمة. • مراجعة المبادرات الأمنية وتقديم المشورة عن مدى تطابقها مع الأهداف الرئيسية للمؤسسة.
مكتب أمن المعلومات	• تطوير إستراتيجية أمن المعلومات للوحدة ومتابعة البرنامج الخاص بها والمبادرات الأمنية والتنسيق مع مدراء القطاعات/المديريات المعنيين والمسؤولين عن العمليات المختلفة لتحقيق التكامل المطلوب. • أداء تقييم خاص بالمخاطر الأمنية ووضع خطط للتعامل معها وفرض الإلتزام بالسياسات والقوانين. • متابعة استغلال الموارد الأمنية وفعاليتها وأثرها في بناء الثقة المطلوبة لخلق ثقافة ووعي داخل الوحدة. • تطوير وتنفيذ مؤشرات المتابعة والتحليل ورفع التقارير • الإشراف والمتابعة لأنشطة أمن المعلومات • تطوير طرق حفظ المعرفة ونشرها وتطوير مؤشرات الفعالية والكفاءة
اللجنة التنفيذية	• التأكد من تطبيق الضوابط الأمنية حسب متطلبات برنامج أمن المعلومات. • التأكد من فعالية ضوابط أمن المعلومات • المتابعة المستمرة والمحافظة على مستويات الأداء. • التأكد من وجود آلية للتدقيق على العمليات. • الإخطار بأي مخاطر تتعلق بأمن المعلومات. • توفير التدريب والموارد اللازمة من أجل ضمان حسن التنفيذ. • توفير المعلومات اللازمة عن سير العمل وتنفيذ ضوابط أمن المعلومات.

7.4 موائمة برنامج أمن المعلومات مع أهداف المؤسسة الرئيسية

بعد وضع الهيكل التنظيمي لتمكين برنامج أمن المعلومات في المؤسسة، يقوم مدير أو مسؤول أمن المعلومات بإعداد استراتيجية برنامج أمن المعلومات وسياسة أمن المعلومات موائمة مع تلك الاستراتيجية.

يجب أن يتوافق البرنامج الأمني مع أهداف المؤسسة ويعالج المخاطر الرئيسية المتعلقة بها، حيث يجب أن تحقق الأهداف الأمنية مستويات الحماية المطلوبة لتوفير بيئة آمنة ومحمية تساعد في تحقيق أهداف المؤسسة، كما يجب أن ينعكس ذلك في الخطط الأمنية واختيار ضوابط الحماية التي تتناسب معها.

يجب في البداية معرفة وفهم أهداف المؤسسة من أجل وضع الاستراتيجية الأمنية الملائمة والمقنعة للإدارة العليا التي بدورها تقدم الدعم اللازم لبرنامج أمن المعلومات، كما يجب تحديد المؤشرات اللازمة لمراقبة التقدم في تحقيق أهداف الاستراتيجية الأمنية.

المخطط 2: يظهر الشكل الهرمي عناصر بناء استراتيجية وبرنامج أمن المعلومات.

8.المفاهيم الخاطئة

هناك العديد من المفاهيم الخاطئة حول مكتب أمن المعلومات ودوره في المؤسسة، وأبرز هذه المفاهيم:

1- أن يتضمن دور مدير / مسؤول أمن المعلومات تنفيذ الضوابط الأمنية التقنية.
2- أن يكون لدى مكتب أمن المعلومات صلاحية اعتماد أو رفض المبادرات الأمنية الجديدة.
3- أن يقوم مكتب أمن المعلومات بإعاقة وإيقاف تنفيذ أعمال المؤسسة في حال عدم اتباع المتطلبات الأمنية.

إن هذه المفاهيم غير صحيحة عملياً حيث لا يجب أن يشارك مدير أو مسؤول أمن المعلومات في تنفيذ الضوابط الأمنية التقنية حيث يسبب ذلك تضارباً في المصالح. ويوضح القسم التالي الفروقات مابين الأدوار المتعلقة بالتنفيذ تلك المتعلقة بمتابعة التنفيذ والتدقيق عليه لاحقا.

تكون اللجنة التوجيهية هي المخوَل الوحيد لإعتماد أو رفض المشاريع والمبادرات والسياسات الأمنية، بينما يكون دور مكتب أمن المعلومات هو تقييم المخاطر المرتبطة بالجوانب الأمنية وتقديم التوصيات بناء على ذلك التقييم ووضع السياسات المطلوبة أو العروض التي يتم مراجعتها والموافقة عليها من قبل اللجنة التوجيهية.
كما لا يقوم مكتب أمن المعلومات بإعاقة قطاع الأعمال أثناء القيام بأعمالهم بل إن جهودهم تنصب في تحقيق أهداف قطاع الأعمال من خلال العمل مع مسؤولي العمليات لوضع الضوابط الأمنية الفعالة.

تعاون مكتب أمن المعلومات مع الفرق المختلفة يخلق ثقافة ايجابية تضمن نجاح أمن المعلومات .

9.مقارنة بين مكتب أمن المعلومات وفريق أمن تقنية المعلومات

يظهر الجدول التالي مقارنة بين مكتب أمن المعلومات وفريق أمن تقنية المعلومات من حيث المهام الوظيفية.

معيار المقارنة	أمن المعلومات	أمن تقنية المعلومات
يتبع بشكل مباشر	أعلى سلطة في الوحدة (كالرئيس التنفيذي أو مكتب الوزير)	مدير تقنية المعلومات
حجم الفريق	صغير (1-3)	متوسط\كبير (+3)
المهارات المطلوبة	مهارات قيادية\مهارات إدارة الأعمال\ خلفية جيدة في المهارات التقنية	مهارات تقنية
المهام الرئيسية	• التنسيق والإشراف على الضوابط والإجراءات الخاصة ببرنامج أمن المعلومات. • اعداد السياسات الأمنية العامة وتنفيذ برنامج توعوي للتعريف عنها والتأكد من تطبيقها بعد ذلك. • تقييم المخاطر المتعلقة بجوانب أمن المعلومات • التدقيق الدوري للتأكد من تطبيق الضوابط الأمنية • تقديم تقارير تقدم برنامج إدارة أمن المعلومات إلى اللجان الأمنية.	• تنفيذ الضوابط الأمنية التقنية والتوصيات حسب توجيهات اللجنة التوجيهية. • تقديم تقارير تنفيذ الضوابط الأمنية إلى مكتب أمن المعلومات وتقديم وثائق التدقيق المتعلقة بهذه الضوابط.

10.مكونات برنامج أمن المعلومات

أ. تقييم المخاطر

يسهم دور مكتب أمن المعلومات بشكل رئيسي في إدارة المخاطر المرتبطة بسير العمليات وإدارة أنظمة المعلومات المختلفة من أجل تحقيق أهداف المؤسسة الاستراتيجية.

عادة يتم النظر إلى أمن المعلومات من زاوية محدودة من قبل الإدارة العليا واعتبارها مسألة تقنية جانبية أو مستقلة عن مخاطر المؤسسة ونمط الإدارة التقليدي ومراحل العمليات المختلفة، وينتج عن هذه الرؤية الضيّقة إهمال التأثير الكبير للمخاطر الأمنية على استمرار عمل المؤسسات وقدرتها على تنفيذ أعمالها الأساسية.

لذلك يعتبر تقييم المخاطر واحدة من المكونات الأساسية لبرنامج أمن المعلومات، حيث تستخدم نتائج التقييم في تحديد أوجه الخلل التي تتطلب ضوابط أمنية من أجل حماية المعلومات شديدة الأهمية في المؤسسة واتخاذ قرارات التغيير والمبادرات ذات التأثير على الجانب الأمني للمؤسسة.

كما أن نتائج التقييم يمكن أن تتضمن مستويات مختلفة من المخاطر حيث يمكن للجنة التوجيهية التركيز على هذه المخاطر واعتماد الاستراتيجية المقترحة من مكتب أمن المعلومات للتغلب على الفجوات المكتشفة وضمان تنفيذ الضوابط المناسبة من قبل الجهات المعنية في المؤسسة.

يجب القيام بتقييم شامل للمخاطر بشكل سنوي يشمل كافة المعلومات التي تمتلكها المؤسسة.
يوفر "إطار عمل إدارة مخاطر تقنية المعلومات لحكومة سلطنة عُمان" إرشادات مفصلة حول تقييم المخاطر.

ب.تنفيذ الضوابط الأمنية

إن عملية ضبط البيئة تتضمن جوانب تقنية وغير تقنية (إدارية وتنظيمية) يتم تنفيذها لضمان وجود الضوابط التي تقوم باكتشاف ومنع المخاطر الأمنية وحماية بيئة المؤسسة.

الضوابط التقنية قد تتضمن وضع جدار للحماية ضمن الشبكة وإعداده بشكل مناسب ليقوم بمراقبة البيانات المتبادلة مع المؤسسة، كما قد تتضمن برامج الحماية للكشف عن الفيروسات والبرمجيات الخبيثة ومنعها من إحداث أي أضرار للأنظمة ومنعها من الانتشار إلى شبكات أو أجهزة أخرى.

وتتضمن الضوابط الإدارية (الغير تقنية) السياسات الأمنية الداخلية ووضع العمليات والإجراءات التي تساعد في بناء فهم واضح عن كيفية التعامل مع المعلومات الخاصة بالمؤسسة وتوضيح الأدوار والمسؤولين عن العمليات المرتبطة بالمراحل المختلفة.

هناك العديد من الأمثلة عن هذه الضوابط المذكورة في معيار الآيزو 27002 والتي يمكن الإستعانة بها كمرجع من قبل مسؤولي الأنظمة الأمنية عند إدارة برنامج أمن المعلومات في مؤسساتهم.

ت. التوعية والتدريب

هناك مقولة عامة يتم ذكرها عادة في المحافل والمؤتمرات والدورات التدريبية وهي أن "الأفراد هم الحلقة الأمنية الأضعف في المؤسسة", فالعديد من الاختراقات والهجمات تعتمد على وجود أشخاص ليسوا على دراية أو وعي شامل عن التهديدات الأمنية التي يمكن أن تؤدي لحدوث اختراقات أمنية تؤثر على الأشخاص أنفسهم أو على المؤسسة وبالتالي تسبب خسائر كبيرة.

تركز بعض المؤسسات على الحلول الأمنية التقنية المتقدمة بينما يتم تهميش تطوير الجانب البشري من حيث المعرفة والخبرة في معالجة الحالات المشتبه بها. حيث يجب أن تتضمن الخطط الأمنية التدريب الأساسي الجيد وخطط التوعية لجميع المستويات الوظيفية في المؤسسة من أجل بناء ثقافة ناضجة حول أفضل الممارسات الأمنية. ولابد أن يشمل التدريب والبرنامج التوعوي للمؤسسة الشرائح التالية:

- الفرق الإدارية
- الفرق التقنية والمعنية بتنفيذ الضوابط
- المستخدمين

كما لا ينصح بالإكتفاء بالقيام بجلسات التوعية الأمنية وجمع الموظفين في مكان واحد للتحدث عن الجوانب الأمنية وعن كيفية تطور الحوادث الأمنية فقط، بل لابد من تثقيف الأشخاص بطرق مبتكرة ومشوقة تضمن تغيير القناعات الداخلية عند الموظفين والتي من شأنها أن تولد

الالتزام والتفاعل بشكل كامل مع السياسات والإجراءات الأمنية. وتستخدم لذلك الوسائل والأدوات الإبداعية من أجل التنفيذ الفعّال للبرنامج الأمني ورفع مستوى الوعي تجاه حماية المؤسسة.

ث. التدقيق والالتزام

بعد إنشاء مكتب أمن المعلومات في المؤسسة للقيام بتنفيذ برنامج أمن المعلومات ووضع السياسات المطلوبة وتصميم جميع الضوابط الأمنية، يأتي دور العنصر الرابع المهم، وهو التأكد من تطبيق الضوابط الأمنية وفعاليتها والالتزام بالسياسات للمحافظة على البيئة الآمنة.
من المهم القيام بالتدقيق الدوري على تطبيق الضوابط الأمنية، حيث تشمل خطط التدقيق عدة أطر زمنية مختلفة: الشهرية والربع سنوية والنصف سنوية وذلك حسب حجم المؤسسة ومجال أعمال التدقيق. تتنوع أدوات التدقيق التي يمكن استخدامها في التحقق من تطبيق الضوابط، مثل سجلات الأنظمة والآليات التقنية التي تحدد الثغرات ضمن بيئة العمل.

يجب تسجيل ملاحظات التدقيق وتحليلها وإعداد التقارير ورفعها للجنة التوجيهية بعد إعلام الفرق المسؤولة عن اتخاذ الإجراءات التصحيحية. ويحتوي التقرير الجيد على النماذج الشائعة والمشاكل الداخلية التي يمكن حلها في مراحل مبكرة لمنع الهجمات المحتملة.

ولابد من الإشارة إلى أن الالتزام بالسياسات الأمنية هو مسألة مهمة يجب التحقق منها من أجل التأكد من التزام جميع الموظفين بالقواعد والأعمال المتوقعة منهم لحماية المؤسسة والمعلومات القيّمة فيها.

11. العمليات الأساسية الداعمة

يعمل مسؤول أمن المعلومات بشكل مباشر مع الفرق الداخلية للتأكد من وجود العمليات الأساسية الداعمة لأمن المعلومات. ومع وجود الدعم من قبل اللجنة التوجهية ومدراء الفرق المعنية، يتم وضع العمليات التالية إذا لم تكن موجودة مسبقاً أو مراجعتها إذا لم تكن ممارسة بصورة منظمة ومنتظمة من أجل التأكد من تحقيقها لاحتياجات برنامج أمن المعلومات:

- **إدارة الأصول:** هذه العملية تعطي تصوراً واضحاً عن جميع أصول المعلومات التي تملكها المؤسسة وتساعد هذه العملية في تحديد الأصول ذات القيمة الأعلى والتي تحتاج لمستويات حماية محددة.

- **إدارة المخاطر:** كما ذكر سابقاً، تعتبر المخاطر واحدة من العوامل الهامة في إدارة أمن المعلومات داخل المؤسسة، ويساعد التحكم الشامل بالمخاطر على اتخاذ القرارات السليمة لجميع نواحي البرنامج، من تحليل تأثير التهديدات على أعمال المؤسسة واتخاذ قرارات الاستثمار للمشاريع الجديدة أو عند الحصول على تقنيات جديدة.

- **إدارة الوصول وإدارة هوية المستخدمين:** إن وجود تحكم فعّال بالوصول إلى أصول المؤسسة ومواردها يساعد على تجنب كم كبير من المخاطر، والمساعدة في أنشطة التدقيق، كما يساعد في الكشف عن الدخول غير المصرح به وإيقافه، فمثل هذه الحالات قد تؤدي إلى اختراقات في أمن المؤسسة.

- **معالجة الحوادث الأمنية:** يجب أن يتضمن برنامج أمن المعلومات خطة محددة تشتمل على الإجراءات اللازمة لمعالجة الحوادث. ويجب أن يكون الموظفين على اطلاع بالجهات والفرق الواجب مخاطبتها في حال وقوع حادث أمني، ويجب أيضاً تدريب فرق الاستجابة للحوادث الأمنية على معالجة الحوادث وفق أحدث الطرق. ولابد ايضا

من تحديد الإطار الزمني لمعالجة الحوادث الأمنية على اختلاف شدتها، وتحديد مسار التصعيد بشكل واضح وجعله متاحا لجميع أفراد المؤسسة بعد الحصول على اعتماد اللجنة التوجيهية.

- **استمرارية الأعمال والحماية من الكوارث:** يعتبر توفر الخدمات بشكل مستمر من العناصر الرئيسية في برنامج أمن المعلومات، فوجود الخطط والأساليب الجيدة لتحقيق استمرارية الأعمال دون توقف عند وجود أي كارثة أو انقطاع يساعد في تأمين بيئة العمل من حيث القدرة على التحكم وإدارة تدفق المعلومات والمعاملات الالكترونية.

- **التطوير المستمر:** يمكن تعلم العديد من الدروس المستفادة في المراحل المختلفة عند تنفيذ برنامج أمن المعلومات كما يمكن تحسين نواحي متعددة في البرنامج. إن هذه المرحلة التي يتم إهمالها أحيانا تضيف قيمة كبيرة إلى رفع نضج بيئة العمل وبناء ثقافة داعمة تساعد في رفع مستويات أمن المعلومات.

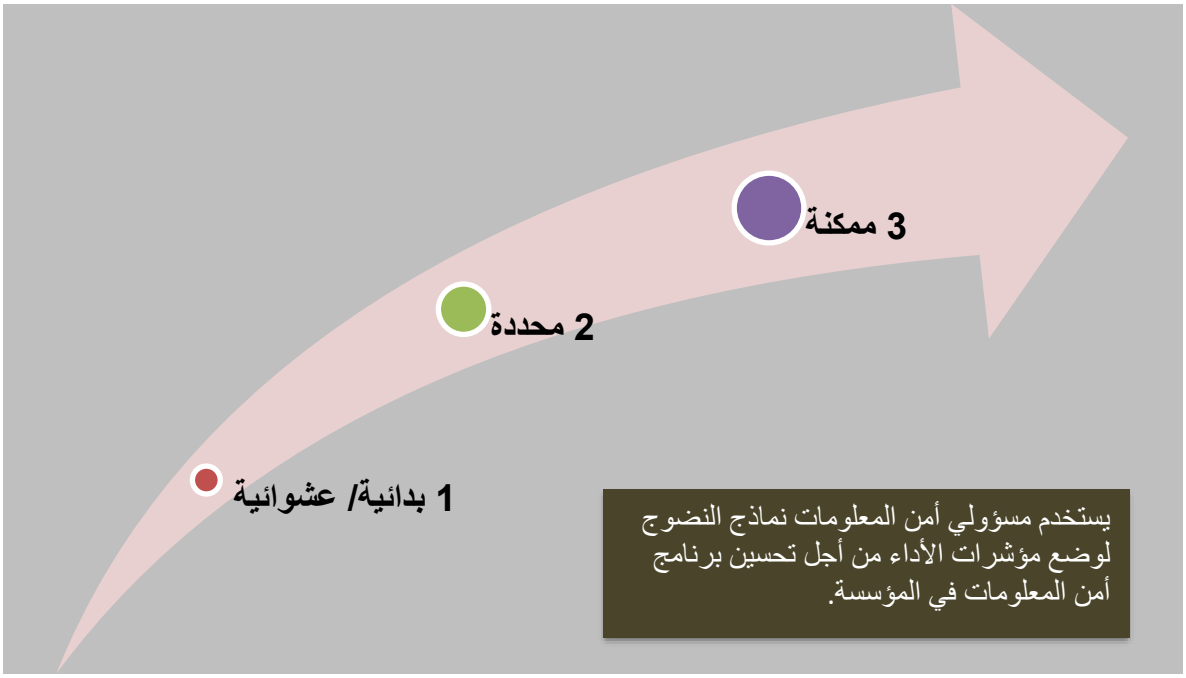
من أجل نجاح عملية التحسين المستمر لابد من وجود آلية واضحة يتم من خلالها بناء قاعدة بيانات لتسجيل الملاحظات المتجددة التي من شأنها أن تسهم في تحسين برنامج أمن المعلومات بالمؤسسة.

12. قياس مستوى نضج برنامج أمن المعلومات

إن تنفيذ برنامج أمن المعلومات في أي مؤسسة يجب أن يدعم تحقيق الأهداف الاستراتيجية لهذه المؤسسة، ولتحقيق ذلك يجب على مسؤول أمن المعلومات والإدارة وأصحاب المصلحة التركيز على تحسين مستوى نضج البرنامج الأمني. وينبغي عليهم دراسة الوضع الحالي ومعرفة الأعمال التي تتم بشكل صحيح والأعمال الواجب تنفيذها للانتقال إلى مستوى أعلى. تنفذ معظم الممارسات الأمنية بشكل مستقل في المؤسسة ويزداد نضوجها يوماً بعد يوم من خلال العمل المكرس ووضع الخطط الصحيحة وتحديد الأهداف والمراحل المطلوب إنجازها، ويساعد أيضا تقييم المخاطر في تحديد الفجوات بين الوضع الحالي ومستوى الذي تطمح المؤسسة للوصول إليه. ويجب أن يرتكز بناء آليات ناضجة على مؤشرات محددة من أجل تسريع الأداء وجودة البرنامج الأمني، ويستخدم لذلك نموذج تحديد مستويات النضج.

يحتوي تحديد نموذج مستويات المتعارف عليه دوليا في العادة على خمسة مستويات تتدرج من مستوى عدم وجود للممارسات المطلوبه (المستوى الأول)و وصولا إلى المستوى الأمثل (المستوى الخامس)، ويظهر المخطط التالي نسخة معدلة من هذا النموذج يركز بشكل أكبر على اتباع الممارسات المتعقة بإدارة أمن المعلومات في وحدات الجهاز الإداري للدولة ورفعها إلى أعلى مستويات النضوج، ويظهر المخطط ثلاث مستويات للبدء بتنفيذ برنامج أمن المعلومات.

للمزيد من المعلومات والتوضيح عن المستويات الأخرى للنضج يمكن الرجوع إلى ممارسات إطار عمل كوبيت (COBIT) في مجال أمن المعلومات.



نموذج نضوج برنامج أمن المعلومات

يتضمن الجدول التالي وصفاً لمتطلبات مستويات النضوج والتي يجب تحقيقها للانتقال إلى المستويات الأعلى.

المستوى	الحالة	الوصف
0	**غير موجودة**	• أمن المعلومات لا ينظر إليه كاحتياج أساسي في المؤسسة • مسؤوليات أمن المعلومات غير محددة • التدابير الداعمة لإدارة أمن المعلومات غير منفذة • عملية رفع التقارير والاستجابة للاختراقات الأمنية غير موجودة • لا يوجد تحديد لأي عمليات إدارية أمنية.

1	**بدائية/ عشوائية**	• هنالك إدراك للحاجة لأمن المعلومات في المؤسسة بصوره متفرقه ومحدوده • ينظر لأمن المعلومات كمسؤولية محدودة بتقنية المعلومات ولا علاقة للوظائف والمجالات الأخرى بالمؤسسة بها. • يتم إسناد مسؤوليات أمن المعلومات لمكتب أمن المعلومات، مع وجود صلاحيات محدودة لإدارة المكتب • يتم تطوير السياسات الأمنية لكن المهارات والأدوات غير كافية. • يتم معالجة الأمور المتعلقة بأمن المعلومات بعد حدوث الحالة الأمنية فقط دون وجود خطط للتعامل مع حدوث أي اختراقات بشكل مسبق. • تقارير أمن المعلومات غير مكتملة أو مضللة . • يوجد تدريب أمني لكنه يتم بشك غير منتظم أو عشوائي.
2	**محددة**	• يوجد إدراك لأمن المعلومات في المؤسسة كما يتم تعزيزه من قبل الإدارة • إجراءات أمن المعلومات محددة بما يتوافق مع سياسة أمن المعلومات. • مسؤوليات أمن المعلومات محددة وواضحة لكنها ليست مطبقة دائماً • وجود خطة أمنية وحلول أمنية مرتبطة بتحليل المخاطر. • التقارير الأمنية لا تركز على النواحي الهامة المتعلقة بالوظائف الرئيسية للمؤسسة. • الاختبارات الأمنية يتم تنفيذها بشكل عشوائي (مثل اختبار الاختراق). • يوجد تدريب أمني للفرق التقنية و الفرق الأخرى في المؤسسة لكنه ينظم ويدار بشكل غير رسمي.

3	**ممكّنة**	• مسؤوليات أمن المعلومات محددة بوضوح وممكّنة ومطبقة بشكل متكامل. • تحليل مخاطر أمن المعلومات وتأثيراتها يتم بشكل دائم وفاعل. • إجراءات وسياسات أمن المعلومات مكتملة مع وجود أسس أمنية محددة. • استخدام وسائل التوعية الأمنية بشكل فاعل وإلزامي. • يتم تحديد هوية المستخدمين والمصادقة والتفويض من خلال معايير وإجراءات محددة. • تسعى المؤسسة لرفع كفاءة الموظفين المسؤولين عن التدقيق وإدارة أمن المعلومات من خلال دورات معتمدة والحصول على شهادات مهنية خاصة بهذا الجانب. • يتم تنفيذ الاختبارات الأمنية وفق معايير محددة وآليات واضحة تؤدي إلى تحسين المستويات الأمنية. • يتم تنسيق الإجراءات المتعلقة بجانب أمن المعلومات في المؤسسة وفق منظومة متكاملة مع كافة الفرق المعنية بالمؤسسة. • يتم ربط التقارير الأمنية بما يتناسب مع تحقيق أهداف المؤسسة. • يتم تنفيذ التدريب الأمني لجميع المستويات الوظيفية من إدارة وفرق تقنية ومستخدمين. • يتم وضع وتنفيذ خطط التدريب الأمنية بما يتوافق مع احتياجات المؤسسة والمخاطر الأمنية المتعلقة بها والتي تم تحديدها من خلال نشاط تقييم وتحليل المخاطر. • يتم قياس مؤشرات أهداف أمن المعلومات بالمؤسسة وجمعها وعرضها على اللجنة التوجيهية. • تستخدم الإدارة مؤشرات الأهداف لتعديل خطة برنامج أمن المعلومات ضمن عمليات واجراءات التحسين المستمر للبرنامج.

13. خطة العمل لتنفيذ برنامج أمن المعلومات في المؤسسات

يلخص هذا القسم الخطوات الأساسية اللازمة لإعداد برنامج أمن المعلومات بعد تعيين المسؤولين في مكتب أمن المعلومات في المؤسسة:

1- تشكيل اللجنة التوجيهية لبرنامج أمن المعلومات أو تطوير اللجان التوجيهية الحالية من خلال اسناد الأدوار والمسؤليات المتعلقة بالإشراف على برنامج أمن المعلومات الخاص بالمؤسسة.
2- تطوير سياسة أمن المعلومات الخاصة بالمؤسسة والمتوافقة مع تمكين تحقيق أهداف المؤسسة الرئيسية.
3- وضع الهيكل التنظيمي لبرنامج أمن المعلومات الخاص بالمؤسسة.
4- أداء تقييم شامل للمخاطر المتلعقة بجوانب أمن المعلومات وتحضير خطط متكاملة وخطط زمنية مسندة للفرق المعنية لمعالجتها.
5- تطوير السياسات التقنية الخاصة بعمليات أمن المعلومات ووضع الآليات الأساسية لمراقبة وتنفيذ الإجراءات والضوابط مع الفرق المختلفة.
6- القيام بالجلسات التوعوية لتثقيف جميع الموظفين في المؤسسة.