وزارة الاتصالات وتقنية المعلومات

السياسات العامة لأمن المعلومات

في الجهات الحكومية

إعداد:
م/ صـــادق الصوفي

18

سياسة تقييم وتدقيق المخاطر الأمنية

سياسة تقييم وتدقيق المخاطر الأمنية

1 بنود السياسة

2 محتويات إعداد السياسة

2.1 المقدمة

2.2 النطاق

2.3 الأهداف

2.4 المخاطر والتهديدات للبيانات

2.5 الأدوار والمسئوليات

سياسة تقييم وتدقيق المخاطر الأمنية

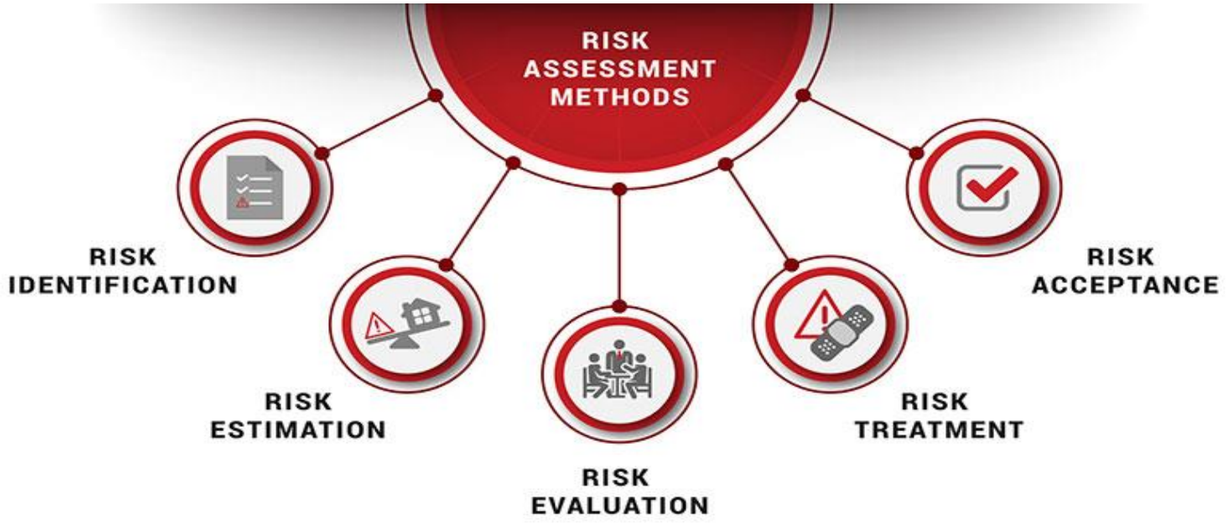
بنود السياسة

- يجب أن يتم تقييم المخاطر الأمنية لنظم المعلومات والتطبيقات لمرة واحدة على الأقل كل عامين، على أن يتم انجاز تقييم المخاطر الأمنية قبل التحسينات والتغييرات الرئيسية المرتبطة بتلك النظم والتطبيقات.
- يجب أن يكون استعمال البرمجيات المستخدمة لتحليل تقييم المخاطر الأمنية مقيدة ومضبوطة .
- يجب أن يتم تقييم نظم المعلومات دورياً من قبل مدققين من طرف مستقل وموثوق به ومعتمد من قبل وزارة الاتصالات وتقنية المعلومات، وذلك لتحديد الحد الأدنى من الضوابط اللازمة لتقليل المخاطر الأمنية إلى مستوى مقبول .
- يجب أن يتم مراجعة وتقييم مدى الامتثال لسياسات أمن المعلومات كافة .
- يجب أن يتم تقييد وضبط استعمال البرمجيات المستخدمة لتحليل التدقيق الأمني .
- يجب ان يتم تأمين وتقييد نتائج عمليات التقييم والتدقيق وحصرها على المعنيين فقط.

سياسة تقييم وتدقيق المخاطر الأمنية

المقدمة

تعتبر سياسة التقييم جزء رئيسي من مراحل التطوير العام في الجهة وذلك لمعرفة المستوى الأمني لديها والى أي مستوى وصلت الموارد المعلوماتية لديها من معيارية الحماية والأمان العالمية، حيث وجب التنويه عند إجراء تقييم لمخاطر تقنية المعلومات في الجهة الحكومية ان يكون متوافقاً مع إطار إدارة المخاطر لها، بحيث يتم تعريف مخاطر تقنية المعلومات وفقاً لمتطلبات الأعمال في الجهة عبر تأسيس سياق لتقييم مخاطر تقنية المعلومات Risk Assessment كم هو موضح في الشكل التالي:



الهدف

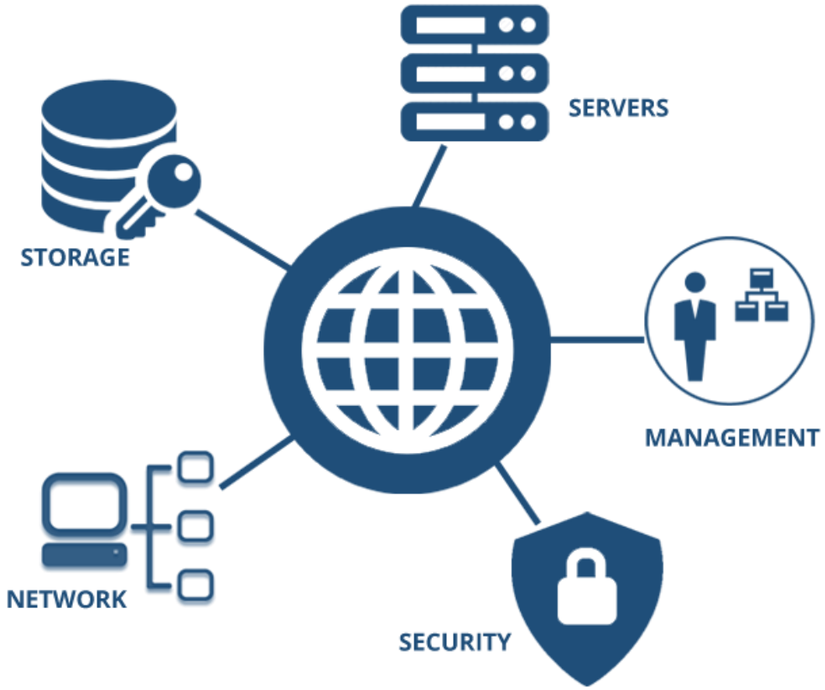
تهدف سياسة التقييم إلى الآتي:

- معرفة إلى أي مدى سياسات الأمان مطبقة على الأنظمة المعلوماتية ومواردها وأجهزتها.

المساهمة في تطوير الإجراءات الأمنية المستقبلية والشاملة التي تفي بمتطلبات الامن لدى الجهة.

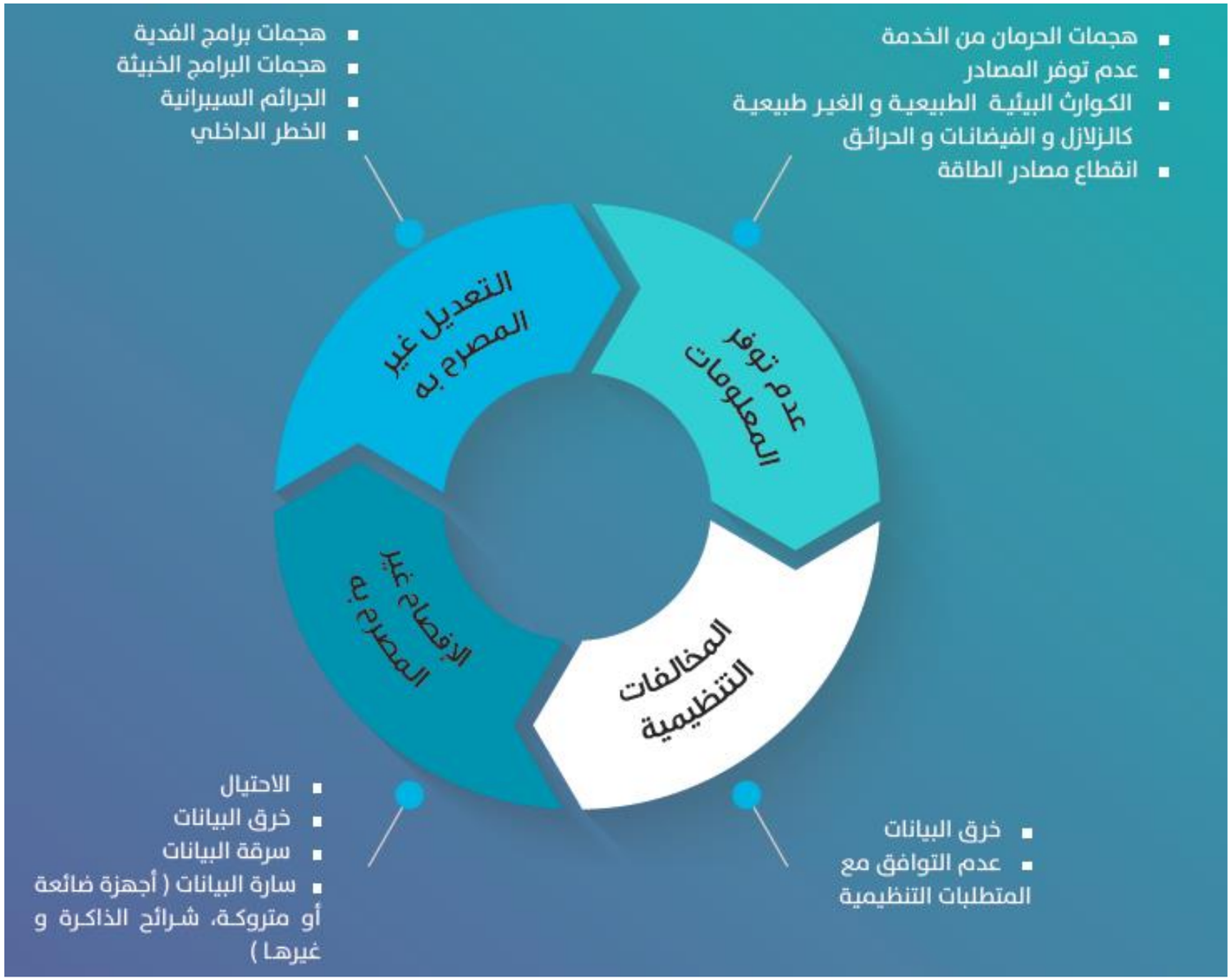
النطاق

تطبق هذه السياسة على جميع موارد الأنظمة المعلوماتية وجميع المعدات وكل ما يخص أجهزة الشبكة والخدمات المقدمة من قبل الجهة كما يجب ان تتضمن المختصين بالتطوير من الموظفين والاستشاريين بداخل الجهة.



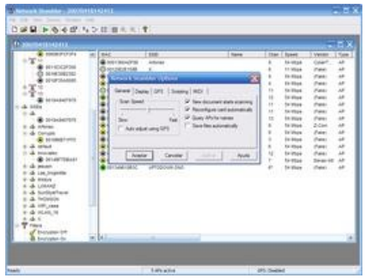
.

أمثلة عن أبرز المخاطر والتهديدات للبيانات



الأدوار والمسئوليات

مسئولية الجهة



يجب أن يكون استعمال البرمجيات المستخدمة لتقييم المخاطر الأمنية مقيدة وحسب المعايير الخاصة بذلك

يتم انجاز تقييم المخاطر الأمنية قبل التحسينات والتغييرات الرئيسية

يجب أن يتم تقييم المخاطر الأمنية لموارد المعلومات والأنظمة والتطبيقات بشكل دوري تقره الجهة سواء بشكل نصفي بالسنة او دوري سنويا

يجب أن يتم تقييم نظم المعلومات دوريا من قبل مدققين من طرف مستقل وموثوق به، وذلك لتحديد الحد الأدنى من الضوابط اللازمة لتقييم المخاطر الأمنية إلى مستوى مقبول.

يجب أن يتم مراجعة مدى الامتثال لسياسات أمن المعلومات بشكل دوري.

يجب أن يتم تقييد وضبط استعمال البرمجيات المستخدمة للتدقيق الأمني.

سياسة تقييم وتدقيق المخاطر الأمنية

انتهى