INTOSAI
DEVELOPMENT INITIATIVE

INTOSAI
Working Group on IT Audit

مجموعة العمل القائمة على تدقيق تقنية المعلومات (WGITA) - دليل مبادرة الإنتوساي للتنمية (IDI) بخصوص تدقيق تقنية المعلومات لمؤسسات التدقيق العليا

(مراجعة 2022)

مجموعة العمل القائمة على تدقيق تقنية المعلومات (WGITA) - دليل مبادرة الإنتوساي للتنمية (IDI) بخصوص تدقيق تقنية المعلومات

لمؤسسات التدقيق العليا

(مراجعة 2022)

كتيب بيان جودة مجموعة عمل الإنتوساي المعنية بتدقيق تكنولوجيا المعلومات ومبادرة تنمية الإنتوساي (WGITA - IDI) بشأن تدقيق تكنولوجيا المعلومات للأجهزة العليا للرقابة (مراجعة 2022)، الإصدار 1 (19 ديسمبر 2022)

حدد رؤساء لجان تحقيق أهداف الإنتوساي والوثيقة المشتركة لمبادرة تنمية الإنتوساي حول "ضمان جودة المنافع العامة للإنتوساي التي تم تطويرها ونشرها بدون مراعاة الإجراءات الواجبة" ثلاثة مستويات لضمان الجودة، على النحو التالي:

ضمان جودة المنافع العامة للإنتوساي التي تم تطويرها ونشرها بدون مراعاة الإجراءات الواجبة - مستويات ضمان الجودة

المستوى الأول: المنتجات التي خضعت لعمليات ضمان الجودة المكافئة لإجراءات الإنتوساي الواجبة قانونًا، بما في ذلك تمديد فترة العرض العام المتمتع بالشفافية (90 يومًا)

المستوى الثاني: المنتجات التي خضعت لعمليات ضمان الجودة المحدودة بشكل أكبر والتي تشمل الأطراف ذات العلاقة من خارج الهيئة أو مجموعة العمل المسؤولة عن التطوير الأولي للمنتجات. وقد تتضمن عمليات ضمان الجودة، على سبيل المثال، التجربة والاختبار والدعوة لتلقي التعليقات من الأطراف ذات العلاقة الرئيسية، رغم أنها لا تتجاوز مدة 90 يومًا كاملة من العرض العام

المستوى الثالث: المنتجات التي خضعت لتدابير صارمة بشأن مراقبة الجودة داخل الهيئة أو مجموعة العمل المسؤولة عن تطويرها

قد تكون المستويات المختلفة لضمان الجودة مناسبة لمختلف المنافع العامة العالمية التي تم تطويرها وفقًا للمستوى الثاني من ضمان الجودة

بروتوكول ضمان الجودة: الإصدار 2.0

يحدد بروتوكول مبادرة تنمية الإنتوساي المُتَّبع لضمان جودة المنافع العامة العالمية تدابير ضمان الجودة بناءً على المستويات الثلاثة سعيًا لتحقيق ضمان الجودة المذكورة أعلاه. أما بالنسبة لمستوى ضمان الجودة الثاني، فتتضمن هذه التدابير: تصديق مجلس إدارة مبادرة تنمية الإنتوساي على إنشاء المنافع العامة العالمية؛ وتشكيل فريق لتطوير منتج ذي قدرة تنافسية؛ وتنفيذ مراجعة بواسطة خبراء من غير أعضاء فريق التطوير، وإجراء تعديلات تستند إلى المراجعة، وتدقيق الوثائق لغويًا وتحريرها وترجمتها بواسطة أشخاص أكفّاء؛ وإجراء عرض عام على الأطراف ذات العلاقة المعنيين؛ واستصدار الموافقات اللازمة للإصدار 1 من المنافع العامة العالمية.

تحديث هذه المنافع العامة العالمية

للإبقاء على كون هذه المنافع العامة العالمية وثيقة الصلة بالغرض منها، سوف تضطلع مبادرة تنمية الانتوساي ومجموعة عمل الإنتوساي المعنية بتدقيق تكنولوجيا المعلومات بإجراء مراجعة عابرة لهذا الكتيب مرة كل عامين، وقد تقرر مبادرة تنمية الإنتوساي ومجموعة عمل الإنتوساي المعنية بتدقيق تكنولوجيا المعلومات العمل على إصدار نسخة مُعدلة من الكتيب في حالة وجود تغييرات جوهرية يتعين إجراؤها. وتتخذ هذه القرارات على أساس إجراء المراجعة مرة كل عامين، وسوف تلتزم المراجعات الرئيسية ببروتوكول مبادرة تنمية الإنتوساي لضمان الجودة، وعادةً لن تخضع المراجعات العابرة لهذا البروتوكول.

هذه المنفعة العامة العالمية مملوكة بشكل مشترك لمبادرة تنمية الإنتوساي (مسار عمل الأجهزة العليا للرقابة المعنية بمبادرة تنمية الإنتوساي) ومجموعة عمل الإنتوساي المعنية بتدقيق تكنولوجيا المعلومات، وهما المسؤولان عن الحفاظ على هذه المنافع العامة العالمية.

عملية مراجعة ضمان الجودة

أجرى السيد شورجو تشاترجي (من وحدة الدعم الاستراتيجي في مبادرة تنمية الإنتوساي) مراجعة لضمان جودة العملية المُتبعة في تطوير هذه المنافع العامة العالمية، بمقارنتها مع الإصدار 2.0 من بروتوكول ضمان الجودة. ويعد مراجع ضمان الجودة على دراية ببروتوكول مبادرة تنمية الإنتوساي لضمان جودة المنافع العامة العالمية ولم يشارك في تطوير المنافع العامة العالمية. وقد صُممت عملية مراجعة ضمان الجودة هذه للتأكيد لجميع الأطراف ذات العلاقة أن مبادرة تنمية الإنتوساي قد اتخذت جميع تدابير رقابة الجودة المذكورة أعلاه، والمُصممة لتلبية المستوى الثاني من ضمان الجودة.

نتائج مراجعة ضمان الجودة

خلصت مراجعة ضمان الجودة للعملية المتبعة في تطوير هذه المنافع العامة العالمية إلى أنه تم اتباع البروتوكول على النحو المطلوب للمستوى الثاني من ضمان الجودة من كافة النواحي.

الاستنتاج

استنادًا إلى مراجعة ضمان الجودة، تضمن مبادرة تنمية الإنتوساي ومجموعة عمل الإنتوساي المعنية بتدقيق تكنولوجيا المعلومات لمستخدمي هذه المنافع العامة العالمية أن هذه الوثيقة خضعت لعملية ضمان جودة تكافئ الإجراءات الواجبة اللازمة لإطار الإنتوساي للتصريحات المهنية (IFPP).

E. Gørrissen
Einar Gørrissen (Jan 24, 2023 14:49 GMT+1)

Einar Gørrissen
Director General
مبادرة تنمية الإنتوساي
19 ديسمبر 2022

Girish Chandra Murmu
Chair
مجموعة عمل الإنتوساي المعنية بتدقيق تكنولوجيا المعلومات

جدول المحتويات

مقدمة 1

قائمة الاختصارات 2

المقدمة 3

الفصل 1: تدقيق تقنية المعلومات 6

أولاً : ما هو تدقيق تقنية المعلومات؟ 6

ثانيًا. الخطوة 1: التخطيط لتدقيق تقنية المعلومات 9

ثالثا. الخطوة 2: تصميم تدقيق تقنية المعلومات 14

رابعا. الخطوة 3: إجراء تدقيق تقنية المعلومات 17

الخطوة الرابعة: الإبلاغ عن نتائج تدقيق تقنية المعلومات 22

السادس. المراجع وقراءات إضافية 24

الفصل 2: حوكمة تقنية المعلومات والإدارة 25

أولا. ما هي حوكمة تقنية المعلومات وإدارتها؟ 25

ثانيًا. العناصر الرئيسة لحوكمة وإدارة تقنية المعلومات 26

ثالثا. المخاطر على الهيئة الخاضعة للرقابة 30

رابعا. المراجع وقراءات إضافية 34

الفصل 3 : تطوير واكتساب تقنية المعلومات 35

أولا. ما هو تطوير واكتساب تقنية المعلومات؟ 35

ثانيًا. العناصر الرئيسة لاكتساب وتطوير تقنية المعلومات 36
ثالثا. المخاطر على الهيئة الخاضعة للرقابة 38
رابعا. المراجع وقراءات إضافية 39
الفصل 4: عمليات تقنية المعلومات 41
أولا. ما هي عمليات تقنية المعلومات؟ 41
ثانيًا. العناصر الرئيسة لعمليات تقنية المعلومات 41
ثالثا. المخاطر على الهيئة الخاضعة للرقابة 45
رابعا. ص المراجع ومزيد من القراءة 46
الفصل 5: الاستعانة بمصادر خارجية 48
أولا: ماذا يقصد بالاستعانة بمصادر خارجية؟ 48
ثانيًا. عناصر الاستعانة بمصادر خارجية 49
ثالثا. المخاطر على الهيئة الخاضعة للرقابة 52
رابعا. المراجع ومزيد من القراءات 53
الفصل 6: إدارة استمرارية العمل 55
ما هي إدارة استمرارية الأعمال؟ 55
ثانيًا. العناصر الرئيسة لإدارة استمرارية الأعمال 56
ثالثا. المخاطر على الهيئة الخاضعة للرقابة 61
رابعا. المراجع وقراءات إضافية 61
الفصل 7: أمن المعلومات 62
أولا. ما هو أمن المعلومات؟ 62
ثانيًا. عناصر أمن المعلومات 64
ثالثا. المخاطر على الهيئة الخاضعة للرقابة 70
رابعا. المراجع ومزيد من القراءة 71
الفصل 8: ضوابط التطبيق 73

أولا. ما هي ضوابط التطبيق..... 73

ثانيًا. العناصر الرئيسة لضوابط التطبيق..... 76

ثالثا. ضوابط نظام إدارة الواجهة والبيانات..... 79

رابعا. المخاطر الطارئة على الهيئة الخاضعة للرقابة 80

رابعا. ص المراجع ومزيد من القراءة..... 80

الأشكال

شكل1 : المراحل الشائعة لتدقيق تقنية المعلومات 9

شكل2 : تخطيط نموذجي لنظام تقنية المعلومات في مؤسسة 12

شكل3 : اعتبارات النطاق في تدقيق تقنية المعلومات 15

شكل4 : الضوابط العامة والتطبيق 16

شكل5 : قالب مصفوفة نتائج المراجعة 19

شكل6 : فهم توثيق تدقيق تقنية المعلومات 21

شكل7 : إطار حوكمة تقنية المعلومات العام 26

شكل8 : مجالات عمليات تقنية المعلومات 41

شكل9 : خطوات في إدارة التغيير 43

شكل10 : دورة مراجعة التطبيق 74

شكل11 : مثال ضوابط التطبيق 75

شكل12 : العناصر الرئيسة لضوابط التطبيق 76

شكل13 : أمثلة على ضوابط التطبيق 76

مقدمة

أصبحت مراجعة أنظمة وضوابط وعمليات تقنية المعلومات، والتي يشار إليها أيضًا باسم تدقيق تقنية المعلومات، أحد الموضوعات المركزية لعمليات المراجعة التي تجريها الأجهزة العليا للرقابة المالية والمحاسبة (SAIs) في جميع أنحاء العالم. هذه استجابة طبيعية للاعتماد الحاسم على أنظمة تقنية المعلومات لدعم الحكومة ومؤسسات القطاع العام. يجب أن تحمي أنظمة تقنية المعلومات المستخدمة بيانات المنظمة وأصولها بالإضافة إلى دعم المهام والأهداف المالية والأهداف المحددة الأخرى.

في حين أدى الاستخدام المتزايد لتقنية المعلومات إلى تحسين كفاءة الأعمال وتقديم خدمات أكثر فعالية، فقد جلب معها أيضًا مخاطر ونقاط ضعف مرتبطة، على سبيل المثال، برقمنة الخدمات وزيادة الاتصال بالأنظمة والشبكات الداخلية والخارجية الأخرى. إن دور تدقيق تقنية المعلومات في توفير ضمان أن العمليات المناسبة مطبقة لإدارة مخاطر تقنية المعلومات ونقاط الضعف ذات الصلة أمر ضروري إذا كان الجهاز الأعلى للرقابة المالية والمحاسبة يقدم تقارير ذات مغزى عن كفاءة وفعالية عمليات الحكومة والقطاع العام.

في عام 2014، عملت مجموعة العمل التابعة للمنظمة الدولية للمؤسسات العليا للرقابة المالية (INTOSAI) بخصوص تدقيق تقنية المعلومات (WGITA) ومبادرة INTOSAI للتنمية (IDI) بشكل مشترك لإنتاج أول دليل بخصوص تدقيق تقنية المعلومات بهدف تزويد مدققي الأجهزة العليا للرقابة المالية والمحاسبة بالمعايير والممارسات الجيدة المعترف بها عالميًا بشأن تدقيق تقنية المعلومات كما يطرح إصدار 2022 من الدليل تحديثًا لتفسيرات المجالات الرئيسة التي قد يُطلب من مدققي تقنية المعلومات النظر فيها أثناء إجراء عمليات تدقيق تقنية المعلومات.

يتبع كتيب WGITA / IDI مبادئ المراجعة العامة على النحو المنصوص عليه في المعايير الدولية للمؤسسات العليا للرقابة المالية والمحاسبة (ISSAI).[1] يستمد الدليل أيضًا من أطر عمل تقنية المعلومات المعترف بها دوليًا، بما في ذلك إطار عمل ISACA COBIT، ومعايير منظمة المعايير الدولية ((ISO، وأدلة تقنية المعلومات وأدلة بعض الأجهزة العليا للرقابة المالية والمحاسبة، في محاولة لتزويد المستخدمين بالمعلومات الأساسية والأسئلة الرئيسة اللازمة للتخطيط الفعال والأداء لعمليات تدقيق تقنية المعلومات.

قاد مشروع تحديث هذا الدليل رئيس WGITA، وهو الجهاز الأعلى للرقابة المالية والمحاسبة في الهند، والجهاز الأعلى للرقابة المالية والمحاسبة في الولايات المتحدة الأمريكية، و IDI. تود WGITA وIDI أن تشكر أعضاء الفريق الفرديين الذين عملوا بلا كلل في تطوير هذا التوجيه. ساهم مدققو تقنية المعلومات من الأجهزة العليا للرقابة المالية والمحاسبة في أستراليا والبرازيل وفيجي والهند والكويت والفلبين وتنزانيا والولايات المتحدة الأمريكية بشكل قيم من خلال تقديم أمثلة لتقارير تدقيق تقنية المعلومات. كما نتوجه بالشكر الجزيل للأجهزة العليا للرقابة التي قدمت ملاحظاتها وتعليقاتها القيمة على الدليل.

[1] www.issai.org.

قائمة الاختصارات

BCP خطة استمرارية الأعمال

نموذج نضج القدرات ® CMMI

DRP خطة التعافي من الكوارث

FISCAM دليل تدقيق ضوابط نظم المعلومات الفيدرالية

GAO مكتب المساءلة الحكومية، الولايات المتحدة الأمريكية

دليل الإنتوساي التوجيه

IDI مبادرة الإنتوساي للتنمية

IEC اللجنة الكهروتقنية الدولية

منظمة الإنتوساي الدولية للأجهزة العليا للرقابة المالية والمحاسبة

ISCP خطة الطوارئ لنظام المعلومات

ISO منظمة الدولية للتوحيد القياسي

المعايير الدولية للأجهزة العليا للرقابة المالية والمحاسبة (ISSAI) (في الوثائق القديمة يشار إليها أحيانًا بمعايير الإنتوساي)

ITIL مكتبة البنية التحتية لتقنية المعلومات

KPI مؤشر الأداء الرئيسي

المعهد الوطني للمعايير والتقنية NIST، وزارة التجارة الأمريكية

OLA اتفاق المستوى التشغيلي

مؤسسة **المراجعة** العليا

SDLC دورة حياة تطوير نظام

SLA اتفاقية مستوى خدمة

WGITA مجموعة العمل على تدقيق تقنية المعلومات

المقدمة

لقد غيرت الطبيعة العالمية لتقنية المعلومات الطريقة التي نعمل بها جميعًا بعدة طرق، ولم تعد مهنة المراجعة استثناءً. مع تقدم التقنية، اعتمدت الحكومات ومؤسسات القطاع العام الأخرى باستمرار ابتكارات تقنية المعلومات في أنظمة المعلومات الخاصة بها بهدف زيادة الكفاءة وتعزيز تقديم الخدمات العامة المختلفة.[2] كما تحول أسلوب تقديم الخدمات العامة بسرعة من المادية إلى الإلكترونية. وقد أدى هذا التحول إلى اضطرار المؤسسات الحكومية إلى العمل كمنصات رقمية لتقديم الخدمات للجمهور، فضلاً عن مزودي البنية التحتية لأنظمة تقنية المعلومات الداعمة لديهم. كما أن الرقمنة المستمرة للمعلومات، أو تغيير السجلات والبيانات من تنسيق تناظري إلى تنسيق رقمي، زاد أيضًا من الاعتماد الكلي على أنظمة تقنية المعلومات.

إن الوتيرة التي تتقدم بها التقنية أسرع من أي وقت مضى، مما له أيضًا آثار على عمليات تدقيق تقنية المعلومات. تزداد أنظمة تقنية المعلومات تعقيدًا وتنوعًا تقنيًا ومشتتة جغرافيًا. ترتبط هذه الأنظمة مع أنظمة وشبكات داخلية وخارجية أخرى، بما في ذلك الإنترنت، مما يزيد من تعقيدها. تقوم المنظمات الحكومية أيضًا بتخزين المزيد من معلوماتها على الأنظمة المستندة إلى السحابة،[3] بهدف شراء الخدمات بشكل أسرع وتقليل التكاليف. لا شك أن الاتجاه نحو الحوسبة في كل مكان وسهولة الوصول إلى المعلومات سيستمر.

بيد أنه، فقد أدى التقدم التكنولوجي إلى زيادة المخاطر ونقاط الضعف. والجدير بالذكر أن نمو أنظمة وشبكات تقنية المعلومات المستندة إلى الويب قد زاد من المخاطر الأمنية التي تواجه المنظمات الحكومية. تقوم هذه المنظمات بجمع ومعالجة كميات كبيرة من معلومات التعريف الشخصية،[4] والتي يمكن أن تشكل تحديات لضمان خصوصية هذه المعلومات. نتج عن جائحة كوفيد-19 أيضًا تحديات غير مسبوقة للمنظمات الحكومية التي كانت بحاجة إلى الاستمرار في تنفيذ مهامها مع ضمان قدرة موظفيها على أداء عملهم بأمان وفعالية.

هذه الاتجاهات، جنبًا إلى جنب مع التطور المتزايد للمتسللين وغيرهم من ذوي النوايا الخبيثة، تزيد من خطر تعرض البيانات الحساسة للاختراق. يمكن أن تؤدي الحماية غير الفاعلة لأنظمة وشبكات المنظمة إلى إعاقة تقديم الخدمات الحيوية. وعلى هذا النحو، يجب تحديد كل ثغرة جديدة، وتقييم المخاطر من حيث الاحتمالية والتأثير، والتخفيف من حدتها وفقًا لمدى استعداد المنظمة للمخاطر، والسيطرة عليها عند الاقتضاء.

مع زيادة الاستثمار والاعتماد على أنظمة تقنية المعلومات من قبل المنظمات الخاضعة للتدقيق، من الضروري لمدقق تقنية المعلومات اعتماد منهجية ونهج مناسبين. يمكن أن يساعد ذلك في ضمان أن المراجعة يمكن أن يحدد بشكل قاطع المخاطر التي تهدد سلامة البيانات، وتوافرها، وصلاحيتها، وإساءة استخدامها، والخصوصية، كما يوفر ضمانًا بأن الضوابط المخففة في موضعها الصحيح. في بيئة تدقيق تقنية المعلومات، فإن الضوابط هي العمليات والأدوات وآليات الرقابة الأخرى المطبقة لإدارة وظائف تقنية المعلومات وتجنب المخاطر ونقاط الضعف.

في نظام تقنية المعلومات النموذجي، خاصة عند تنفيذه في بيئة ضوابط غير كافية، تواجه المنظمة المدققة العديد من المخاطر التي يجب أن يكون مدقق تقنية المعلومات قادراً على تحديدها. حتى عندما تكون المنظمة الخاضعة للرقابة قد نفذت بعض تدابير الحد من المخاطر، يلزم إجراء تدقيق مستقل لتوفير تأكيد بأن ضوابط نظام المعلومات المناسبة

---

[2] يمكن تعريف أنظمة المعلومات على أنها مزيج من الأنشطة الاستراتيجية والإدارية والتشغيلية المتضمنة في جمع ومعالجة وتخزين وتوزيع واستخدام المعلومات والتقنيات ذات الصلة، بينما تشتمل تقنية المعلومات على الأجهزة والبرمجيات والاتصالات والمرافق الأخرى المستخدمة للإدخال وتخزين ومعالجة ونقل وإخراج البيانات.

[3] الحوسبة السحابية هي وسيلة لتمكين الوصول عند الطلب إلى مجموعات مشتركة من موارد الحوسبة القابلة للتكوين (مثل الشبكات والخوادم وتطبيقات التخزين والخدمات) التي يمكن توفيرها وإصدارها بسرعة.

[4] معلومات التعريف الشخصية هي أي معلومات يمكن استخدامها لتمييز أو تتبع هوية الفرد، مثل الاسم وتاريخ ومكان الميلاد وأنواع أخرى من المعلومات الشخصية التي يمكن ربطها بفرد، مثل المعلومات الطبية والتعليمية والمالية، ومعلومات التوظيف.

موجودة. يجب أن تتضمن عمليات المراجعة هذه تحديد ما إذا كانت ضوابط تقنية المعلومات العامة[5] وضوابط التطبيق[6] تم تصميمها لتقليل التعرض للمخاطر المختلفة وتعمل بكفاءة وفعالية.

بإيجاز، أدى الانتقال إلى أنظمة تقنية المعلومات والمعالجة الرقمية من قبل المنظمات الخاضعة للتدقيق في القطاع العام إلى الحاجة إلى قيام منظمات المراجعة بتطوير القدرات المناسبة لإجراء فحص شامل للضوابط المتعلقة بأنظمة تقنية المعلومات للوفاء بتفويضات المراجعة الشاملة. على وجه الخصوص، ثمة حاجة للتأكد من أن الضوابط الداخلية لتقنية المعلومات المتعلقة بسرية البيانات وسلامتها وصلاحيتها وتوافرها قد تم تبنيها من قبل المنظمات الحكومية.

محتوى الدليل وهيكله

يرمي هذا الدليل إلى تزويد مدققي تقنية المعلومات بإرشادات وصفية بخصوص المجالات المختلفة في تدقيق تقنية المعلومات وقد تم تطويره وفقًا لمتطلبات بروتوكول IDI لضمان جودة السلع العامة العالمية V2.0.[7]

في الفصل الأول من هذا الدليل، سيطلع القراء على لمحة عامة عن تعريف تدقيق تقنية المعلومات، وتفويضات الأجهزة العليا للرقابة المالية والمحاسبة، ونطاق وأهداف عمليات تدقيق تقنية المعلومات. كما يوفر شرحًا للضوابط العامة لتقنية المعلومات وضوابط التطبيقات والعلاقة بين الاثنين. يتم تفصيل مجالات التحكم هذه في الفصول اللاحقة. يصف الفصل الأول أيضًا عملية تدقيق تقنية المعلومات ومنهجية التقييم القائم على المخاطر لاختيار عمليات تدقيق تقنية المعلومات. وصف عملية تدقيق تقنية المعلومات هو وصف عام، يعتمد على طرق المراجعة القياسية[8] يتبع عند تدقيق أنظمة تقنية المعلومات. تهدف الجداول والرسوم البيانية المصاحبة لوصف عملية المراجعة إلى تقديم أمثلة توضيحية ويجب تكييفها مع ارتباطات المراجعة الفردية. يجب على مستخدمي الدليل النظر في عملية المراجعة في سياق المعلومات ذات الصلة في المعايير الدولية للأجهزة العليا للرقابة المالية والمحاسبة والأطر والمعايير الدولية الأخرى، وكذلك الرجوع إلى الأدلة والمبادئ التوجيهية لإجراءات المراجعة في الأجهزة العليا للرقابة المالية والمحاسبة الخاصة بهم للتخطيط وإجراء عمليات تدقيق محددة.

تقدم الفصول من 2 إلى 8 وصفًا تفصيليًا لمجالات تقنية المعلومات المختلفة التي ستساعد مدققي تقنية المعلومات في تحديد المجالات القابلة للتدقيق المحتملة. تم إدراج المخاطر على المستوى التنظيمي المتعلقة بمجال تقنية المعلومات في نهاية كل فصل، مما سيساعد مدققي تقنية المعلومات في تحديد المجالات القابلة للتدقيق عالية المخاطر. ستساعد الإرشادات المقدمة في كل مجال مدققي تقنية المعلومات في التخطيط، إما على مجال معين أو مجموعة من المجالات اعتمادًا على نطاق وهدف تدقيق تقنية المعلومات (على سبيل المثال، تدقيق الأداء أو المالي). على سبيل المثال، يمكن استخدام الإرشادات الخاصة بمراجعة حوكمة تقنية المعلومات للتخطيط لمراجعة آلية حوكمة تقنية المعلومات الخاصة بالمنظمة، أو لتخطيط تدقيق بيئة الضوابط العامة التي تعتبر حوكمة تقنية المعلومات جزءًا مهمًا منها.

يتضمن الملحق الأول من هذا الدليل نظرة عامة على المجالات الناشئة في تدقيق تقنية المعلومات ويوفر مراجع لمزيد من القراءة للمستخدم المهتم. يتضمن الملحق الثاني روابط لتقارير المراجعة التي حددتها الأجهزة العليا للرقابة المالية والمحاسبة بخصوص العالم، والتي يمكن أن تقدم أمثلة قيمة لمجموعة واسعة من مجالات تدقيق تقنية المعلومات التي تمت مناقشتها في الفصول 2-8 من هذا الدليل.

تضمن كتيب 2014 بخصوص تدقيق تقنية المعلومات مجموعة من الملاحق الإضافية مع إرشادات خطوة بخطوة بخصوص تطوير مصفوفة المراجعة. أدرجت ملاحق مصفوفة المراجعة قضايا المراجعة الرئيسة والمعايير والمعلومات المطلوبة وطرق التحليل. للحصول على كتيب 2014 بخصوص تدقيق تقنية المعلومات وملاحق مصفوفة المراجعة، يرجى زيارة: https://www.intosaicommunity.net/wgita/wp-content/uploads/2018/04/it-audit-handbook-english-version.pdf

---

[5] الضوابط العامة لتقنية المعلومات ليست محددة لأي تدفق أو تطبيق معاملات فردية وهي ضوابط على العمليات في تنفيذ تقنية المعلومات التي تدعم تطوير وتنفيذ وتشغيل نظام تقنية المعلومات. وستشمل عادةً حوكمة تقنية المعلومات، والتنظيم والهيكل، والضوابط المادية والبيئية، وتشغيل تقنية المعلومات، وأمن نظام المعلومات، واستمرارية الأعمال، وإدارة الوصول والتغيير.

[6] ضوابط التطبيق عبارة عن عناصر تحكم خاصة بنظام تقنية المعلومات، وتتضمن تعيين قواعد العمل في التطبيق وبالتالي توفير عناصر تحكم في الإسهامات والمعالجة والمخرجات والبيانات الرئيسة.

[7] البروتوكول متاح على http://www.idi.no/en/idi-library/global-public-goods.

[8] برجاء مراجعة، على سبيل المثال، المنظمة الدولية *للأجهزة العليا للرقابة المالية والمحاسبة، المعايير الدولية للأجهزة العليا للرقابة المالية والمحاسبة 100 (ISSAI): المبادئ الأساسية لرقابة القطاع العام* (2019) وإرشادات ISSAI 5100 *بشأن تدقيق نظم المعلومات* (2019).

التوجيه الفني بخصوص استخدام تقنيات المراجعة بمساعدة الكمبيوتر هو أيضًا خارج نطاق هذا الدليل. يتم تشجيع الأجهزة العليا للرقابة المالية والمحاسبة على تنظيم تدريب منفصل على تقنيات المراجعة بمساعدة الحاسوب لموظفيها. قد تنظر الأجهزة العليا للرقابة أيضًا في تسمية موظفيها في برنامج تنمية القدرات IDI على تدقيق تقنية المعلومات.

يرجى زيارة موقعي WGITA وIDI لمزيد من المعلومات بخصوص الموارد وبرامج التدريب القادمة.

WGITA: https://www.intosaicommunity.net/wgita/

IDI: http://www.idi.no

نأمل أن تجد الأجهزة العليا للرقابة المالية والمحاسبة وموظفي تدقيق تقنية المعلومات التابعين لها هذا الدليل أداة مفيدة في تعزيز معرفتهم وفهمهم لقضايا تدقيق تقنية المعلومات، وأن يساعدهم في التخطيط وإجراء عمليات تدقيق تقنية المعلومات.

قد يرغب قراء هذا الدليل أيضًا في الإشارة إلى منتجات IDI العالمية الأخرى التي تكمل هذا الدليل. وتشمل هذه *دليل تنفيذ رقابة أداء IDI*،[9] دليل تنفيذ المراجعة *المالي ISSAI*،[10] و*دليل تنفيذ رقابة الامتثال للمعايير الدولية للأجهزة العليا للرقابة*.[11]

[9] المنظمة الدولية لمبادرة تطوير المؤسسات العليا للرقابة المالية والمحاسبة، *دليل تنفيذ ISSAI لرقابة أداء رقابة الأداء*، الإصدار 1 (أغسطس 2021)، https://www.idi.no/work-streams/professional-sais/work-stream-library/performance-audit-issai-implementation-handbook. https://www.idi.no/work-streams/professional-sais/work-stream-library/performance-audit-issai-implementation-handbook..

[10] المنظمة الدولية لمبادرة تطوير أجهزة الرقابة العليا، *دليل تنفيذ الرقابة المالية ISSAI*، الإصدار 1 (8 ديسمبر 2020)، https://www.idi.no/news/professional-sais/financial-audit-issai-implementation-handbook -version-1-english-light-touch-review-2020.

[11] المنظمة الدولية لمبادرة تطوير الأجهزة العليا للرقابة المالية والمحاسبة، *دليل تنفيذ رقابة الامتثال ISSAI*، مسودة الإصدار 0 (8 يناير 2018)، https://www.idi.no/elibrary/professional-sais/issai-implementation-handbooks/handbooks- english / 803-Compliance-Audit-issai-Implementation-handbook-version-0-english.

الفصل 1: تدقيق تقنية المعلومات

كما ذكرنا سابقًا، أدى انتقال المؤسسات الحكومية إلى أنظمة تقنية المعلومات والمعالجة الرقمية إلى الحاجة إلى قيام مؤسسات التدقيق بتطوير القدرات المناسبة لإجراء فحص شامل للضوابط المتعلقة بأنظمة المعلومات للوفاء بولايات المراجعة الشاملة. على وجه الخصوص، تحتاج مؤسسات التدقيق إلى التأكد من أن المؤسسات الحكومية قد اعتمدت ضوابط تقنية المعلومات الداخلية المتعلقة بسرية البيانات وسلامتها وصلاحيتها وتوافرها.

يقدم هذا الفصل نظرة عامة على عملية تدقيق أنظمة تقنية المعلومات، والمعروفة أيضًا باسم تدقيق تقنية المعلومات. يعمل هذا الفصل كمقدمة وملخص للفصول من 2 إلى 8. على هذا النحو، فإن هذا الفصل يختلف عن جميع الفصول الأخرى من حيث التصميم والتفصيل.

كما ذكرنا سابقًا، فإن وصف عملية تدقيق تقنية المعلومات الموضحة في هذا الفصل عام، بناءً على طرق المراجعة القياسية، وهو انعكاس لمنهجية المراجعة التي تتبعها الأجهزة العليا للرقابة المالية والمحاسبة. على هذا النحو، يجب على المستخدمين النظر في عملية المراجعة الموصوفة في هذا الفصل في سياق المعلومات ذات الصلة في المعايير الدولية للأجهزة العليا للرقابة المالية والمحاسبة والمعايير الدولية الأخرى.

أولاً: ما هو تدقيق تقنية المعلومات؟

أ. شرط إجراء عمليات تدقيق تقنية المعلومات

تفويض المؤسسة العليا للرقابة المالية والمحاسبة (SAI) لإجراء تدقيق لأنظمة تقنية المعلومات وارد في ISSAI 1 - إعلان ليما.[12] وبالتالي، فإن تفويض الجهاز الأعلى للرقابة المالية والمحاسبة بمراجعة أنظمة تقنية المعلومات مستمد من التفويض العام للأجهزة العليا للرقابة لإجراء عمليات تدقيق الأداء والمالية والامتثال أو مزيج من هذه.[13]

- يركز **تدقيق الأداء** على ما إذا كانت التدخلات والبرامج والمؤسسات تعمل وفقًا لمبادئ الاقتصاد والكفاءة والفعالية، وما إذا كان ثمة مجال للتحسين.
  - يركز **اقتصاد** المراجعة على المراجعة على كيفية نجاح المنظمات الخاضعة للرقابة في تقليل تكلفة الموارد، مع مراعاة الجودة المناسبة لهذه الموارد.
  - تعني **كفاءة المراجعة** التساؤل عما إذا كانت الإسهامات قد وُضعت للاستخدام الأمثل أو المرضي، أو ما إذا كان من الممكن تحقيق نفس المخرجات أو ما شابهها بموارد أقل.
  - **فعالية المراجعة** تتعامل مع النتائج. عند تقييم الفاعلية، تنظر الأجهزة العليا للرقابة فيما إذا كانت سياسة أو برنامج أو نشاط حكومي يلبي أهدافه وكيفية تحقيقه.

  في عمليات تدقيق الأداء، يتم فحص أداء المؤسسة مقابل المعايير ذات الصلة التي تحدد الحالة المطلوبة أو المرغوبة فيما يتعلق بموضوع المراجعة وكذلك تمثل معايير أداء معقولة وقابلة للتحقيق. كما يتم تحليل أسباب الانحرافات عن تلك المعايير أو غيرها من المشاكل. تختبر عمليات تدقيق الأداء عادةً ما إذا كانت الحكومة تستخدم الموارد بشكل جيد لتحقيق أهداف سياستها. غالبًا ما تفحص عمليات المراجعة هذه تنفيذ سياسة أو سياسات.
- تركز **المراجعة المالي** على تحديد ما إذا كانت المعلومات المالية للمؤسسة معروضة وفقًا للتقرير المالي المطبق والإطار التنظيمي وتحديد دقة التقارير المالية. الغرض من المراجعة المالي هو تعزيز الثقة التي يمكن أن يتمتع بها المستخدمون المستهدفون في البيانات المالية. ويتحقق ذلك من خلال التعبير عن رأي المدقق بخصوص ما إذا كانت البيانات المالية قد تم إعدادها، من جميع النواحي الجوهرية، وفقًا لإطار التقرير المالي المنطبق. يمكن أن تتضمن المراجعة المالية اختبارًا تفصيليًا وموضوعيًا للمعلومات المالية.
- **تدقيق الامتثال** هو تقييم مستقل لما إذا كان موضوع معين يتبع السلطات المعمول بها المحددة كمعايير. يقوم مدقق الامتثال بتقييم ما إذا كانت الأنشطة والمعاملات المالية والمعلومات، من جميع النواحي الجوهرية، متوافقة مع السلطات التي تحكم المنظمة الخاضعة للرقابة. تضيف عمليات تدقيق الامتثال قيمة من خلال توفير ضمان مستقل للامتثال من قبل المنظمة الخاضعة للتدقيق بناءً على حكم مهني مستقل وتحليل سليم وقوي.

---

[12] المنظمة الدولية للأجهزة العليا للرقابة المالية والمحاسبة، *إعلان ليما*، الجزء السابع، القسم 22.

[13] المنظمة الدولية للأجهزة العليا للرقابة المالية والمحاسبة، *المعايير الدولية للأجهزة العليا للرقابة المالية والمحاسبة 100 (ISSAI): المبادئ الأساسية لرقابة القطاع العام*.

- تجمع **المراجعة المتكامل** بين أنواع مختلفة من عمليات المراجعة لتقييم التفاعل بين العمليات المالية والتشغيلية والتقنية على تحقيق أهداف الرقابة.[14] على سبيل المثال، قد تتضمن المراجعة المتكاملة للبيانات المالية لكيان ما تحليلاً لأوجه القصور في ضوابط أنظمة المعلومات.[15]

غالبًا ما تكون عمليات تدقيق تقنية المعلومات أحد المجالات الموضوعية في سياق تدقيق أوسع (أي الأداء، أو المالي، أو الامتثال). يمكن إجراء تدقيق تقنية المعلومات الذي لا يشكل جزءًا من الأداء أو المالية أو تدقيق الامتثال؛ ومع ذلك، فإن المبادئ العامة والإجراءات والمعايير والتوقعات المطبقة على عمليات المراجعة المالي والأداء والامتثال تنطبق أيضًا على عمليات تدقيق تقنية المعلومات.

ب. تعريف تدقيق تقنية المعلومات

عمليات تدقيق تقنية المعلومات هي فحص لجوانب استخدام المنظمة لتقنية المعلومات، بما في ذلك البنية التحتية لتقنية المعلومات والسياسات والإجراءات والتطبيقات واستخدام البيانات. كما تتضمن عمليات تدقيق تقنية المعلومات بانتظام تحليل الأنظمة والضوابط للتأكد من أنها تلبي احتياجات أعمال المنظمة دون المساس بالأمان والخصوصية والتكلفة وعناصر العمل الهامة الأخرى. وغالبًا ما تتضمن عمليات تدقيق تقنية المعلومات أيضًا الحصول على تأكيد بشأن ما إذا كان تطوير أنظمة تقنية المعلومات وتنفيذها وصيانتها يلبي أهداف العمل، ويحمي أصول المعلومات، ويحافظ على سلامة البيانات. غالبًا ما تتضمن عمليات تدقيق تقنية المعلومات تحديد حالات الانحراف عن المعايير، والتي تم تحديدها بدورها بناءً على نوع مهمة المراجعة (على سبيل المثال، مراجعة الأداء أو الأمور المالية أو الامتثال).

تختلف عمليات تدقيق تقنية المعلومات بناءً على أنواع عمليات المراجعة التي يتم إجراؤها من خلالها. علي سبيل المثال:

- في سياق المراجعة المالي، يمكن أن يكون تدقيق تقنية المعلومات على سبيل المثال فحصًا للضوابط العامة التي تضمن تشغيل أنظمة المعلومات التي تكمن وراء العمليات المالية للكيان، وفق ما هو موضح في بياناتها المالية.[16]
- في سياق تدقيق الأداء، يمكن أن يكون أحد الأمثلة على تدقيق تقنية المعلومات هو تحديد إلى أي مدى أدى اعتماد الوكالة للتقنية الجديدة إلى تحقيق فوائد قابلة للقياس على مستوى الحكومة ووفورات في التكاليف.[17]
- في سياق تدقيق الامتثال، يمكن أن يكون تدقيق تقنية المعلومات على سبيل المثال فحصًا لفعالية أنظمة المعلومات التي تنتج تقارير الامتثال، مما يمكّن الموظفين من إدارة عمليات الكيان والتحكم فيها.[18]

قد تتعامل عمليات تدقيق تقنية المعلومات مع مجموعة متنوعة من المجالات المتنوعة، مثل حوكمة تقنية المعلومات، واستثمارات تقنية المعلومات في مجالات مثل الاتصالات، وما إذا كانت ثمة ضوابط كافية لحماية البيانات لكيانات مثل الحكومات المحلية، وتحليل تطبيق التقنيات الجديدة مثل الذكاء الاصطناعي، أو التطوير،-اقتناء وتشغيل أنظمة تقنية المعلومات. تتعامل عمليات تدقيق تقنية المعلومات أيضًا مع جوانب كل من أمن المعلومات والأمن السيبراني، والتي ترتبط ارتباطًا وثيقًا.

---

[14] جامعة هارفارد، "ما هي المراجعة المتكامل؟"، https://rmas.fad.harvard.edu/faq/what-integrated-audit.

[15] على سبيل المثال، برجاء مراجعة: مكتب محاسبة الحكومة الأمريكية، *تقرير الإدارة: التحسينات مطلوبة في ضوابط نظم المعلومات في دائرة المالية العامة*، GAO-14-693R، (18 يوليو 2014)، https://www.gao.gov/products/GAO-14-693R.

[16] على سبيل المثال، برجاء مراجعة: مكتب محاسبة الحكومة الأمريكية، *تقرير الإدارة: التحسينات المطلوبة في ضوابط نظام معلومات مكتب الخدمات المالية المتعلقة بجدول الديون الفيدرالية*، GAO-22-105569، (17 مارس 2022)، https://www.gao.gov/products/GAO-22- 105569.

[17] على سبيل المثال، برجاء مراجعة: مكتب محاسبة الحكومة الأمريكية، *الحوسبة السحابية: زادت الوكالات من الاستخدام والفوائد المحققة، غير أن بيانات التكلفة والادخار تحتاج إلى تتبع أفضل*، GAO-19-58، (4 أبريل 2019)، https://www.gao.gov/products/gao-19-58.

[18] على سبيل المثال، راجع مكتب محاسبة الحكومة الأمريكية، *المدفوعات غير الصحيحة: مطلوب إرشادات إضافية لتحسين الرقابة على الوكالات ذات البرامج* غير المتوافقة، GAO-19-14، (7 ديسمبر 2018)، https://www.gao.gov/products/gao-19-14.

- يمكن تعريف **أمن المعلومات** على أنه قدرة بيئة تقنية المعلومات[19] لحماية المعلومات وموارد النظام، سواء كانت رقمية أو تناظرية، فيما يتعلق بالسرية والتوافر والنزاهة.[20]يشمل أمن المعلومات التدابير اللازمة للتحكم في هذه التهديدات ومنعها واكتشافها وتوثيقها ومكافحتها. يسمح أمن المعلومات للمؤسسة بحماية البنية التحتية لنظام المعلومات الخاص بها من المستخدمين غير المصرح لهم.
- **الأمن السيبراني** هو عملية حماية المعلومات الرقمية عن طريق منع الهجمات الإلكترونية واكتشافها والرد عليها.[21]يتضمن الأمن السيبراني الاستراتيجية والسياسة والمعايير المتعلقة بأمن الفضاء السيبراني والعمليات فيه. وهي تشمل، من بين أمور أخرى، الحد من التهديد والضعف، والاستجابة للحوادث، والمرونة والتعافي، وضمان المعلومات.[22]

يتمثل أحد الاختلافات الرئيسة بين أمن المعلومات والأمن السيبراني في أن الأمن السيبراني يركز بشكل أكثر دقة على حماية المعلومات الرقمية، بينما يركز أمن المعلومات بشكل أوسع على حماية جميع موارد نظام المعلومات. من بين هذين المجالين، يركز هذا الدليل بشكل أساسي على أمن المعلومات، على الرغم من أن العديد من العناصر الرئيسة لأمن المعلومات تنطبق أيضًا على الأمن السيبراني. يجري إعداد وثيقة توجيه تدقيق منفصلة بشأن الأمن السيبراني وحماية البيانات كجزء من مشروع INTOSAI WGITA آخر.

ج. مراحل تدقيق تقنية المعلومات

تشمل المراحل الأولية لتدقيق تقنية المعلومات تحديد النطاق والتخطيط والتصميم والتنفيذ والإبلاغ عن نتائج المراجعة. يتم وصف كل مرحلة من هذه المراحل بمزيد من التفصيل أدناه. ويركز القسم الثاني على تخطيط المراجعة، والقسم الثالث بخصوص تصميم المراجعة، والقسم الرابع بخصوص إجراء المراجعة، والقسم الخامس بخصوص الإبلاغ عن نتائج المراجعة.

---

[19] تتكون بيئة تقنية المعلومات من تطبيقات تقنية المعلومات والبنية التحتية الداعمة والعمليات التي يستخدمها الكيان لدعم العمليات التجارية وتحقيق استراتيجيات الأعمال.

[20] المعهد الوطني للمعايير والتقنية، *المسرد*، (2021). https://csrc.nist.gov/glossary.

[21] المعهد الوطني للمعايير والتقنية، *إطار عمل تحسين الأمن السيبراني للبنية التحتية الحرجة، الإصدار 1.1* (2018).

[22] المبادرة الوطنية لشغل وظائف ودراسات *الأمن السيبراني، مسرد مصطلحات الأمن السيبراني* (Gaithersburg، MD: 10 مارس 2022)، https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.

شكل1 : المراحل الشائعة لتدقيق تقنية المعلومات

ملحوظة: يهدف هذا الشكل إلى تقديم مثال توضيحي ويجب تكييفه مع ارتباطات المراجعة الفردية.

المصدر: مجهول.

ثانيًا. الخطوة 1: التخطيط لتدقيق تقنية المعلومات

التخطيط هو جزء أساسي من أي تدقيق، بما في ذلك تدقيق تقنية المعلومات. في معظم الأجهزة العليا للرقابة، يتم التخطيط لعمليات المراجعة على ثلاثة مستويات: التخطيط الاستراتيجي؛ التخطيط الكلي أو السنوي؛ والتخطيط الجزئي أو على مستوى المنظمة. يجب اعتبار التخطيط عملية مستمرة طوال عملية المراجعة، حيث يتم اكتشاف معلومات إضافية قد تؤثر على الخطة الأصلية. يتطلب المراجعة الذي يتبع نتائج تدقيق سابق كجزء من نهج تدقيق مستمر تخطيطًا مشابهًا. ومع ذلك، في ظل نهج المراجعة المستمر، يجب تقليل بعض الخطوات، مثل فهم المنظمة، كنتيجة للمعلومات التي تم جمعها بالفعل.

أ. تخطيط استراتيجي

إن الخطة الاستراتيجية للجهاز الأعلى للرقابة المالية والمحاسبة هي عبارة عن تنبؤ طويل المدى (3-5 سنوات) لأهداف وغايات الرقابة، بما في ذلك أنظمة تقنية المعلومات والمنظمات ذات الصلة الخاضعة لسلطة الجهاز الأعلى للرقابة المالية والمحاسبة. في بعض الأجهزة العليا للرقابة المالية والمحاسبة، قد يتم تضمين قائمة فقط من مجالات تقنية المعلومات الجديدة والناشئة للتدقيق في خططهم الاستراتيجية. يمكن أن يشمل ذلك النظر في الأساليب الجديدة لتطوير النظام (على سبيل المثال، البرمجة الرشيقة)، أو الاستحواذ أو الحوسبة السحابية في القطاع العام، أو اعتماد تقنيات جديدة، مثل الذكاء الاصطناعي أو بلوكتشين. توفر عملية التخطيط الاستراتيجي والخطة الاستراتيجية للجهاز الأعلى للرقابة الأسلوب والاتجاه لأهداف تدقيق تقنية المعلومات في الجهاز للمستقبل. على سبيل المثال، كما تمت مناقشته في الفصل 3 بخصوص تطوير تقنية المعلومات واكتسابها، قد تتنبأ المؤسسة التي تخطط لتعديل منهجيات دورة حياة تطوير النظام بإجراء تدقيق للتحقق من حالة التبديل وتقدمه.

ب. التخطيط الكلي والنهج القائم على المخاطر

يتم إجراء المستوى الكلي لتخطيط المراجعة عادة على أساس دورة سنوية على مستوى الجهاز الأعلى للرقابة المالية والمحاسبة لاختيار مجالات المراجعة، واعتمادًا على الجهاز، يتم صياغة عملية لتحديد المجالات التي سيتم تدقيقها سنويًا.[23] مع الانتشار السريع لأنظمة تقنية المعلومات الحديثة عبر الحكومات ومحدودية الموارد المتاحة للأجهزة العليا للرقابة المالية والمحاسبة، أ ***سيكون النهج القائم على المخاطر*** لتحديد الأولويات واختيار المواضيع المناسبة مناسبا. وبالإضافة إلى اعتبارات اختيار أنظمة تقنية المعلومات للمراجعة، عند اتخاذ قرار بشأن موضوعات المراجعة، يجب على المؤسسات أيضًا مراعاة المعلومات مثل النفقات الإجمالية لتقنية المعلومات، والاتصال بالكيانات الخارجية الأخرى، ونضج عمليات تقنية المعلومات والحوكمة. ولا يفوتنا في هذا المقام أن نذكر أنه، سيتعين على الجهاز الأعلى للرقابة المالية والمحاسبة تضمين عمليات تدقيق إلزامية،

[23] سيكون لتنظيم الأجهزة العليا للرقابة المالية والمحاسبة في جميع أنحاء العالم هياكل مختلفة. تشير المرحلة الأولى هنا إلى التكوين الميداني النموذجي للجهاز الأعلى للرقابة المالية والمحاسبة، حيث يتم تنفيذ التخطيط على المستوى العالمي أو الموافقة عليه في المقر الرئيسي ويتم إجراء المراجعة الفعلي على المستوى الميداني.

مثل تلك التي يطلبها القانون أو التي يطلبها البرلمان أو الكونجرس أو غيرها من المنظمات الرقابية.

عادة ما تقوم الأجهزة العليا للرقابة المالية والمحاسبة بمراجعة العديد من المنظمات التي تستخدم أنظمة معلومات مختلفة. قد تكون ثمة تطبيقات مختلفة لوظائف وأنشطة مختلفة وقد يكون ثمة عدد من منشآت الكمبيوتر في مواقع جغرافية مختلفة.

تعتمد الاعتبارات الخاصة بكيفية وأنظمة المعلومات المراد تدقيقها جزئيًا على فهم المخاطر الكامنة في المؤسسة. تتكون **المخاطر الكامنة** من احتمال أن تؤدي بعض ميزات أنظمة تقنية المعلومات الخاصة بالمنظمة الخاضعة للرقابة، بطبيعتها، إلى تأثير سلبي على أداء الوظيفة المنوطة بتنفيذها من قبل المنظمة. على سبيل المثال، نظام تقنية المعلومات المطلوب لإتاحة المعلومات لجميع أفراد الجمهور يحمل مخاطر الأداء الكامنة التي تتجاوز الحد الأقصى المتوقع للمستخدم، قد يفشل نظام المعلومات في الاستجابة ولن تكون المعلومات متاحة لأي مستخدم. في حين أن المنظمة قد تتبنى ضوابط للتخفيف من المخاطر الكامنة، في كثير من الحالات، قد تضطر ببساطة إلى تحمل وجودها ضمن مستوى مخاطر مقبول.

في حين أن ثمة مخاطر متأصلة في أنظمة المعلومات، فإن هذه المخاطر تؤثر على الأنظمة المختلفة بطرق مختلفة. على سبيل المثال، يمكن أن تكون مخاطر عدم التوفر حتى لمدة ساعة خطيرة بالنسبة لنظام الفوترة في متجر تجزئة مزدحم، ويمكن أن تكون مخاطر التعديل غير المصرح به مصدرًا للاحتيال وخسائر محتملة لنظام مصرفي عبر الإنترنت. قد تؤثر البيئات الفنية التي تعمل فيها الأنظمة أيضًا على المخاطر المرتبطة بالأنظمة.[24] يساعد النهج القائم على المخاطر في اختيار أنظمة تقنية المعلومات للمراجعة المدقق في تحديد أولوية عمليات المراجعة.

مثال: خطوات في نهج قائم على المخاطر

1. تحديد عالم المراجعة الذي سيشمل قائمة بجميع المنظمات أو الوحدات الخاضعة للرقابة التي تخضع لاختصاص الجهاز الأعلى للرقابة المالية والمحاسبة.
2. ضع قائمة بنظم المعلومات المستخدمة في المنظمة / الوحدات الخاضعة للتدقيق.
3. تحديد العوامل التي تؤثر على أهمية النظام للمؤسسة للقيام بوظائفها وتقديم الخدمة.
4. تخصيص وزن للعوامل الحرجة. يمكن القيام بذلك بالتشاور مع المنظمة الخاضعة للرقابة.
5. تجميع المعلومات لجميع الأنظمة عبر جميع المؤسسات، و بناءً على الدرجات التراكمية- ضع الأنظمة / المؤسسات في ترتيب حسب الأولوية للتدقيق.
6. إعداد خطة تدقيق سنوية تحدد الأولوية والنهج والجدول الزمني لعمليات تدقيق تقنية المعلومات. يمكن إجراء هذا التمرين على فترات سنوية وبالتالي يمكن أن يكون خطة متكررة.

لاستخدام إطار عمل لتقييم المخاطر، يحتاج الجهاز الأعلى للرقابة المالية والمحاسبة إلى بعض الحد الأدنى من المعلومات عبر الوكالات، والتي يتم جمعها عادةً من خلال مسح أو تقييمات ذاتية للرقابة. يتم سرد مثال لعملية كيفية تقييم المخاطر لتحديد أنظمة تقنية المعلومات المحتملة للتدقيق في مربع "خطوات في نهج قائم على المخاطر"، على اليمين.[25] بالنسبة للمؤسسات ذات التفويضات الأوسع، سيكون من الضروري تضييق نطاق المراجعة المحتمل، على سبيل المثال، لمنظمات معينة أو موضوعات تقنية المعلومات، قبل تنفيذ هذه الخطوات.

لإجراء التقييمات القائمة على المخاطر للأنظمة التي تعتمد على تقنية المعلومات، قد تختار الأجهزة العليا للرقابة منهجية مناسبة لغرضها. كما قد تتراوح هذه المنهجيات من التصنيفات البسيطة لملف بيانات المخاطر لبيئة تقنية المعلومات مثل حسابات عالية ومتوسطة ومنخفضة إلى حسابات أكثر تعقيدًا ورقمية والتي تحدد تصنيف المخاطر بناءً على البيانات الموضوعية التي تم جمعها من المنظمة الخاضعة للرقابة. سيعتمد التصنيف على فهم الجهاز الأعلى للرقابة المالية والمحاسبة للمنظمة وبيئتها والحكم المهني لفريق تدقيق تقنية المعلومات في الجهاز. على سبيل المثال، كما تمت مناقشته أكثر في الفصل 4، قد يختار الجهاز الأعلى للرقابة المالية والمحاسبة تحديد أنظمة تقنية المعلومات المراد تدقيقها بناءً على أي منها نفذ أهم التغييرات وإضافة معايير إدارة التغيير إلى قائمته الخاصة بمجالات المخاطر المحتملة.

تعتبر عملية تقييم المخاطر هي إحدى الطرق لاختيار المنظمة الخاضعة للرقابة لتدقيق تقنية المعلومات، إلا أن الأجهزة العليا للرقابة المالية والمحاسبة تختار أيضًا المنظمات الخاضعة للتدقيق على أساس دوري، باستخدام عمليات تدقيق إلزامية أو بناءً على طلبات محددة من هيئات الرقابة (على سبيل المثال، مؤتمر أو برلمان أو هيئة تشريعية).

ج. التخطيط الجزئي

[24] س. أنانثا سايانا، جمعية المراجعة والرقابة على نظم المعلومات.

[25] يمكن العثور على مثال آخر لمنهجية تقييم المخاطر لأنظمة المعلومات، ودليل للمدققين بخصوص كيفية تقييم المخاطر عند التخطيط لأعمال المراجعة، على: مجتمع ممارسات المراجعة الداخلي، *تقييم المخاطر في تخطيط المراجعة* (أبريل 2014)، https://www.pempal.org/sites/pempal/files/event/attachments/cross_day-2_4_pempal-iacop-risk-assessment-in-audit- Planning_eng.pdf.

يتضمن التخطيط الجزئي وضع خطة تدقيق مفصلة لمنظمة المراجعة المختارة، بدءًا من تحديد أهداف المراجعة. ستساعد خطة المراجعة المدققين في إعداد برنامج تدقيق تقنية المعلومات. ستكون الخطوة الأساسية في تطوير برنامج المراجعة هي الحصول على فهم واضح للمؤسسة وأنظمة تقنية المعلومات الخاصة بها. يرمي هذا الدليل إلى مساعدة المدقق بمجرد وضع خطة لتعبئة مصفوفة المراجعة بأهداف محددة لكل مجال (على سبيل المثال، الحوكمة وأمن المعلومات) التي سيتم التحقيق فيها. يتطلب التخطيط على المستوى الجزئي فهماً للمنظمة، وبعض التقييم الأولي للضوابط لتسهيل التخطيط التفصيلي للتدقيق، واعتبارات تخصيص الموارد والموظفين لضمان أن فريق المراجعة يتكون من أعضاء يتمتعون بشكل جماعي بالكفاءة لإجراء عمليات تدقيق تقنية المعلومات تحقيق الأهداف المرجوة. على سبيل المثال، بحسب ما نوقش في الفصل 6 بخصوص إدارة استمرارية الأعمال، قد تخطط المنظمة لمراجعة معايير إضافية في مجال تخطيط التعافي من الكوارث للأنظمة الحيوية للعمليات على مستوى المنظمة.

i. التعرف على المنظمة

يتم تحديد مدى معرفة المنظمة والعمليات التي يتطلبها مدقق تقنية المعلومات إلى حد كبير من خلال طبيعة المنظمة ومستوى التفاصيل التي يتم تنفيذ أعمال المراجعة فيها. ستختلف عمليات تدقيق تقنية المعلومات، على سبيل المثال، بناءً على نطاق ما يتم تدقيقه - من نظام تقنية معلومات فردي إلى مؤسسة واحدة أو منطقة حكومية أو حتى دولة بأكملها. يجب أن تشمل المعرفة بالمنظمة الأعمال والمخاطر المالية والمتأصلة التي تواجه المنظمة وأنظمة تقنية المعلومات الخاصة بها. يجب أن يشمل أيضًا مدى اعتماد المنظمة على الاستعانة بمصادر خارجية لتحقيق أهدافها وإلى أي مدى تم تخطيط العمليات التجارية للمنظمة في بيئة تقنية المعلومات.[26] يجب على المدقق استخدام هذه المعلومات في تحديد المشاكل المحتملة، وصياغة الأهداف ونطاق العمل، وأداء العمل، والنظر في إجراءات الإدارة التي يجب أن يكون مدقق تقنية المعلومات في حالة تأهب بشأنها. يوضح الشكل 2 تخطيطًا نموذجيًا لنظام تقنية المعلومات في مؤسسة ما.

[26] عادة ما تقوم المنظمات التي تجرى بخصوص من دليل إلى بيئة إلكترونية بإجراء عملية إعادة هندسة عملية الأعمال. قد يكون من الممكن أن يتم تنفيذ بعض العمليات التجارية يدويًا جنبًا إلى جنب مع أنظمة تقنية المعلومات أو أن المنظمة قد طورت عمليات آلية غير فعالة أو غير فعالة من خلال تكرار عملياتها اليدوية. كما ستقدم هذه السيناريوهات الخاصة مجالات اهتمام محددة لمراجعي تقنية المعلومات.

شكل2 : تخطيط نموذجي لنظام تقنية المعلومات في مؤسسة

المصدر: مجهول.

سيكون للتطبيق النموذجي الذي يشكل جوهر نظام تقنية المعلومات في مؤسسة ما مجموعة تكنولوجية - مزيج من لغات البرمجة وأطر العمل والأدوات التي يبني عليها المطورون لإنشاء التطبيق. يمكن أن تشتمل مجموعة التقنية على نظام إدارة قاعدة بيانات مع قواعد بيانات محددة، وبرمجيات (برامج) ترسم قواعد العمل في النظام من خلال وحدات محددة، وواجهة (واجهات) مستخدم أمامية مدعومة ببرنامج تطبيقات الشبكة إذا كانت ثمة بيئة متصلة بالشبكة. توجد قواعد البيانات وبرامج التطبيقات على الخوادم، وهي عبارة عن أجهزة أو برامج عالية السعة بشكل أساسي قادرة على استضافة قواعد بيانات وتطبيقات كبيرة ومتعددة. يمكن أن تكون الخوادم خاصة بمتطلبات المستخدم المختلفة، مثل خوادم البيانات وخوادم التطبيقات وخوادم الإنترنت والخوادم الوكيلة.

قبل الشروع في تقييم الضوابط في نظام المعلومات، يجب على المدققين تطوير فهم لهيكل النظام والبيانات الأساسية ومصادرها بغية تحديد أدوات وتقنيات المراجعة المطلوبة. بناءً على فهم مدققي تقنية المعلومات لنظام المعلومات والمنظمة الخاضعة للرقابة، قد يقررون نهجهم في تدقيق تقنية المعلومات.

تشمل أنشطة المراجعة الأخرى التي يمكن أن تكون مفيدة في فهم المنظمة الخاضعة للرقابة

- رسم خرائط العمليات التجارية للجهة الخاضعة للرقابة،
- تحديد تفاعل الكيان مع أقرانه أو البيئة الخارجية،
- سرد الأنشطة التجارية التي تعتبر بالغة الأهمية لأهداف وغايات المنظمة الخاضعة للرقابة، و
- سرد جميع حلول تقنية المعلومات التي يستخدمها الكيان.

الأهمية النسبية

الأهمية النسبية أو الملاءمة والأهمية، يجب تحديد قضايا تدقيق تقنية المعلومات ضمن الإطار العام للجهاز الأعلى للرقابة المالية والمحاسبة لتقرير سياسة الأهمية النسبية لتقرير المراجعة. وقد يختلف منظور الأهمية النسبية اعتمادًا على طبيعة ارتباط تدقيق تقنية المعلومات.[27] يجب على المدقق النظر في الأهمية النسبية للأمر في سياق، على سبيل المثال، البيانات المالية أو طبيعة المنظمة أو النشاط. يمكن أيضًا تعريف الأهمية النسبية في سياق تقنية المعلومات بمصطلحات غير مالية.

يجب على مدقق تقنية المعلومات تحديد ما إذا كان أي نقص في تقنية المعلومات يمكن أن يصبح جوهريًا. يجب تقييم أهمية الضوابط العامة لتقنية المعلومات فيما يتعلق بتأثيرها على ضوابط التطبيق (أي ما إذا كانت ضوابط التطبيق المرتبطة غير فعالة أيضًا). وإذا كان النقص في التطبيق ناتجًا عن الرقابة العامة على تقنية المعلومات، فهي مادية. فعلى سبيل المثال، إذا كان حساب الضريبة المستند إلى التطبيق خاطئًا ماديًا وكان ناتجًا عن ضعف ضوابط التغيير في الجداول الضريبية، فقد يصبح قرار الإدارة بعدم

[27] تنص الفقرة 41 من *المعايير الدولية للأجهزة العليا للرقابة المالية* على أنه "غالبًا ما يتم النظر إلى الأهمية النسبية من حيث القيمة، وغير أن لها أيضًا جوانب كمية ونوعية أخرى. قد تجعل الخصائص الملازمة لعنصر ما أو مجموعة عناصر مادة ما بطبيعتها. قد تكون المسألة أيضًا جوهرية بسبب السياق الذي تحدث فيه".

تصحيح عجز عام في التحكم في تقنية المعلومات وانعكاسه المرتبط ببيئة التحكم جوهريًا عند تجميعه مع غيره السيطرة على أوجه القصور التي تؤثر على بيئة الرقابة.[28]

تخصيص الموارد وتكوين فريق المراجعة

يتطلب تدقيق تقنية المعلومات تخصيصًا محددًا للموارد، خاصةً الموظفين الذين هم على دراية جيدة بأنظمة وعمليات وآليات تقنية المعلومات النموذجية التي تحكم التنفيذ الناجح لتقنية المعلومات. بالإضافة إلى موارد الموظفين المناسبة،[29] الميزانية المناسبة والبنية التحتية، وأي متطلبات أخرى يتم تحديدها يجب توفيرها أيضًا. يجب تحديد الجدول الزمني للمراجعة، إن أمكن، بالتشاور مع المنظمة الخاضعة للرقابة.

قد تضمن الأجهزة العليا للرقابة أن فريق المراجعة يتكون من أعضاء يتمتعون مجتمعين بالكفاءة لإجراء عمليات تدقيق تقنية المعلومات لتحقيق الأهداف المرجوة. يمكن اكتساب المعرفة والمهارات والكفاءات اللازمة من خلال مزيج من بناء القدرات، مثل التدريب أو زيادة الخبرة أثناء العمل؛ تجنيد؛ ومشاركة الموارد الخارجية، وفقًا للخطة الاستراتيجية للجهاز.

قد تنظر الأجهزة العليا للرقابة في خيارات مختلفة لتخصيص الموارد البشرية لعمليات تدقيق تقنية المعلومات، مثل ما يلي:

- إنشاء مجموعة مركزية مع متخصصي تقنية المعلومات الذين يساعدون فرق المراجعة الأخرى في الجهاز الأعلى للرقابة المالية والمحاسبة لإجراء عمليات المراجعة هذه أو نشر متخصصين في تقنية المعلومات.
- إنشاء مجموعة أو وظيفة تدقيق تقنية المعلومات مخصصة يُعهد إليها بمسؤولية إجراء جميع عمليات تدقيق تقنية المعلومات للجهاز الأعلى للرقابة المالية والمحاسبة والتي تتفاعل مع الفرق الأخرى التي لديها معرفة قديمة بالمنظمة الخاضعة للرقابة.
- استخدم مزيجًا من المدققين العامين ذوي المعرفة الواسعة بتقنية المعلومات والمدققين المتخصصين ذوي الخبرة الأكثر تركيزًا في مجال واحد أو عدد قليل من مجالات تقنية المعلومات المحددة.
- تضمين موارد الموظفين الداخلية الأخرى كأعضاء مؤقتين في فريق تدقيق تقنية المعلومات.

قد تستخدم الأجهزة العليا للرقابة موارد خارجية، مثل مستشاري تقنية المعلومات والمقاولين والمتخصصين والخبراء لإجراء عمليات تدقيق في تقنية المعلومات في حالة وجود قيود داخلية على الموارد، أو إذا كانت الموارد الخارجية تعتبر أكثر ملاءمة أو فعالة من حيث التكلفة. يجب أن تضمن الأجهزة العليا للرقابة أن مثل هذه الموارد الخارجية مدربة تدريباً كافياً وحساسة لإرشادات السلوك المهني، وكذلك لعمليات ومنتجات تدقيق تقنية المعلومات المطبقة على الجهاز الأعلى للرقابة المالية والمحاسبة. يجب مراقبة هذا العمل بشكل كافٍ من خلال عقد موثق، أو اتفاقية مستوى خدمة، أو اتفاقية عدم إفشاء. قد تكون ثمة حاجة إلى عناية خاصة فيما يتعلق بالحفاظ على السرية، وخاصة فيما يتعلق بالمعلومات الخاضعة للرقابة، من قبل الموارد الخارجية.

عند تدقيق أنظمة تقنية المعلومات، قد تضمن الأجهزة العليا للرقابة أن فرق تدقيق تقنية المعلومات لديها القدرة بشكل جماعي على القيام بما يلي:

- فهم العناصر التقنية لنظام تقنية المعلومات، بما في ذلك جميع الأمثلة ذات الصلة للتطبيق قيد الاستخدام، حتى تتمكن من الوصول إلى البنية التحتية لتقنية المعلومات واستخدامها لعملية المراجعة.
- فهم تخطيط العمليات التجارية في منطق البرمجة لنظام تقنية المعلومات.
- فهم منهجية المراجعة، بما في ذلك معايير المراجعة ذات الصلة والمبادئ التوجيهية المطبقة على الجهاز.
- فهم تقنيات تقنية المعلومات لجمع أدلة المراجعة من الأنظمة الآلية.
- فهم أدوات تدقيق تقنية المعلومات لجمع وتحليل وإعادة إنتاج نتائج هذا التحليل أو إعادة أداء الوظائف التي تم تدقيقها.
- فهم كيفية تقييم ومقارنة التكاليف، مثل الجهد والموارد، والفوائد المستمدة من تنفيذ نظام تقنية المعلومات.
- تحديد مزايا وعيوب ومخاطر الأعمال لاكتساب تقنية المعلومات وممارسات الاستعانة بمصادر خارجية واستراتيجيات.
- تحديد ما إذا كانت أهداف مشروع تقنية المعلومات قد تحققت مع إيلاء الاعتبار الواجب للجودة والنطاق، وضمن الجداول الزمنية والتكاليف المدرجة في الميزانية.

---

[28] *مفاهيم الأهمية النسبية لمعلومات المراجعة*، إرشادات ISACA (G6).

[29] موارد الموظفين المناسبة تعني الموظفين الذين لديهم فهم لأنظمة المعلومات ويمكنهم إجراء استخراج البيانات وتحليلها إذا لزم الأمر، حيث تتطلب عمليات تدقيق تقنية المعلومات دائمًا استخدام مهارات تقنية المعلومات لإجراء عمليات المراجعة. يجب على الجهاز الأعلى للرقابة أن يشير إلى 100 الفقرة 39 من ISSAI بشأن توفير الكفاءة اللازمة لموظفيه قبل إجراء تدقيق على تقنية المعلومات.

- فهم الخدمات والمتطلبات والمواصفات لضمان اختيار البائعين الموثوق به والفعال من حيث التكلفة وللتحقق من وجود المحتويات الأساسية لعقود البائعين.

بالإضافة إلى ذلك، بالنسبة لعمليات المراجعة المالي، قد تضمن الأجهزة العليا للرقابة أيضًا أن فرق المراجعة لديها خبرة كافية بشكل عام في إجراء عمليات تدقيق البيانات المالية وفهم البيانات المالية.

ثالثا. الخطوة 2: تصميم تدقيق تقنية المعلومات

أ. أهداف تدقيق تقنية المعلومات

يمكن أن تختلف أهداف تدقيق تقنية المعلومات بناءً على مجموعة متنوعة من العوامل، مثل نوع المراجعة العام (أي الأداء أو المالي أو الامتثال)، أو المنظمة أو المنظمات قيد المراجعة، أو نوع عمليات تقنية المعلومات قيد المراجعة، أو المخاطر الرئيسة للمؤسسة أو المنظمات وعوامل أخرى.

بعض الأمثلة على أهداف المراجعة هي

- لتدقيق الأداء، للتأكد من أن موارد تقنية المعلومات تسمح بتحقيق الأهداف التنظيمية بكفاءة وفعالية، وأن الضوابط ذات الصلة فعالة في منع واكتشاف وتصحيح حالات الزيادة، وكذلك الإسراف وعدم الكفاءة في استخدام وإدارة نظم المعلومات؛
- بالنسبة لعمليات المراجعة المالي، لتقييم الضوابط ذات الصلة التي لها تأثير على موثوقية البيانات من أنظمة المعلومات، والتي بدورها لها تأثير على البيانات المالية للمنظمة المدققة؛ أو لتقييم العمليات التي تدخل في عمليات منطقة معينة، مثل نظام كشوف المرتبات أو نظام المحاسبة المالية؛ و
- لتدقيق الامتثال، لضمان امتثال عمليات نظم المعلومات للقوانين والسياسات والمعايير المطبقة على المنظمة الخاضعة للرقابة.

قد يغطي نطاق عمليات تدقيق تقنية المعلومات مجالات محددة من تنفيذ تقنية المعلومات، مثل

- اقتناء وتطوير وتنفيذ أنظمة تقنية المعلومات،
- عمليات التشغيل والصيانة،
- إدارة التغيير،
- ادارة الوصول،
- أمن المعلومات واستمرارية الأعمال،
- القيمة مقابل المال المقدم من خلال أنظمة تقنية المعلومات، و
- تخطيط موارد المؤسسة أو أنظمة تقنية المعلومات المعقدة / المتخصصة الأخرى.
- تخطيط موارد المؤسسة أو أنظمة تقنية المعلومات المعقدة / المتخصصة الأخرى.

إذا كان تدقيق تقنية المعلومات جزءًا من مهمة المراجعة، فيجب على الجهاز الأعلى للرقابة التأكد من أن فريق المراجعة ككل يعمل بطريقة متكاملة لتحقيق الهدف الشامل للتدقيق. على سبيل المثال، لتحقيق التكامل الفاعل، قد تنظر الأجهزة العليا للرقابة

- توثيق شامل للعمل الذي يتعين على مدققي تقنية المعلومات القيام به،
- صياغة بروتوكول لتبادل المعلومات بين مدققي تقنية المعلومات والمراجعين الآخرين، و
- تحديد أنظمة المعلومات وأهداف الرقابة التي تدخل في نطاق المراجعة.

بعد تطوير هدف (أهداف) المراجعة ونهجها، غالبًا ما يصيغ مدققو تقنية المعلومات أسئلة تدقيق محددة من شأنها توجيه أعمال المراجعة. يجب أن تنبثق أسئلة المراجعة من هدف (أهداف) المراجعة العام، وعادة ما تكون أكثر تحديدًا من حيث أنها تتناول الموضوعات التي ستصفها أو تقيمها أثناء المراجعة. الهدف هو أن تغطي أسئلة المراجعة جميع جوانب هدف (أهداف) المراجعة. أسئلة المراجعة إما **وصفية** (بمعنى أنها تصف حالة) أو **تقييمية** (بمعنى أنها تقيم حالة مقابل معايير ويمكن أن تكون معيارية أو تحليلية).

ب. نطاق ومنهجية تدقيق تقنية المعلومات

لدى مدققي تقنية المعلومات العديد من الخيارات عند تحديد نطاق المراجعة. أسئلة النطاق النموذجية التي يجب مراعاتها مدرجة في الشكل 3.

شكل3 : اعتبارات النطاق في تدقيق تقنية المعلومات

ملحوظة: يهدف هذا الشكل إلى تقديم مثال توضيحي ويجب تكييفه مع ارتباطات المراجعة الفردية.

المصدر: Performance Audit Subcommittee Development Team.

غالبًا ما يُطلب من مدقق تقنية المعلومات تقييم السياسات والإجراءات التي توجه البيئة العامة لتقنية المعلومات في المنظمة الخاضعة للرقابة، والتأكد من أن الضوابط المقابلة وآليات الإنفاذ في مكانها الصحيح. يشمل تحديد نطاق تدقيق تقنية المعلومات تحديد مدى تدقيق المراجعة؛ تغطية أنظمة تقنية المعلومات ووظائفها؛ عمليات تقنية المعلومات التي يتعين تدقيقها؛ مواقع أنظمة تقنية المعلومات التي سيتم تغطيتها بما في ذلك الأطراف الثالثة، مثل مقدمي الخدمات السحابية أو الخارجيين، الذين تشكل بيئات التحكم الخاصة بهم جزءًا من بيئة التحكم الخاصة بالكيان الخاضع للرقابة؛ والفترة الزمنية التي سيغطيها المراجعة.[30]

يجوز للأجهزة العليا للرقابة اختيار الفترة الزمنية لتحليل المراجعة (على سبيل المثال، سنة واحدة أو 3 سنوات) في تحديد نطاق ارتباط تدقيق تقنية المعلومات. قد تكون ثمة حاجة أيضًا لعملية تدقيق لتنتهي في تاريخ محدد. يجب اختيار فترة زمنية ذات صلة بالأهداف المحددة لارتباط المراجعة.

بمجرد تحديد نطاق المراجعة، تحدد فرق تدقيق تقنية المعلومات المنهجية أو الخطوات المحددة التي يخططون لاتخاذها لأداء أهداف المراجعة وفقًا للنطاق. من خلال تحديد تفاصيل المنهجية، تضمن فرق المراجعة بشكل أفضل أن الخطوات التي يخططون لاتخاذها ممكنة فيما يتعلق بالبيانات التي يخططون لجمعها، وأنهم لا يؤدون خطوات تدقيق خارجية، وأن نتائج خطوات المراجعة المتخذة ستسمح للفريق للتحدث عن أهداف المراجعة.

يجب إطلاع المنظمة الخاضعة للرقابة على النطاق والأهداف ومعايير التقييم الخاصة بالمراجعة التي يجب مناقشتها معهم حسب الضرورة. يجوز للجهاز الأعلى للرقابة، إذا لزم الأمر، كتابة خطاب الارتباط إلى المنظمة الخاضعة للرقابة حيث قد يحدد أيضًا شروط هذه الارتباطات.

ج. ضوابط عامة لتقنية المعلومات والتطبيقات

كما ذكرنا سابقًا، يتم تعريف عمليات تدقيق تقنية المعلومات على أنها فحص الضوابط المتعلقة بأنظمة تقنية المعلومات، بغية تحديد حالات الانحراف عن المعايير. **الضوابط** هي العمليات والأدوات وآليات الرقابة الأخرى المطبقة لإدارة وظائف تقنية المعلومات وتجنب المخاطر ونقاط الضعف. سيتم تحديد الضوابط التي يتم تقييمها في تدقيق تقنية المعلومات من خلال هدف ونطاق المراجعة.

تستخدم الضوابط للتخفيف من المخاطر التي تتعرض لها المنظمة. وعلى وجه الخصوص، فهناك ثمة أنواع من المخاطر ذات الصلة بضوابط تدقيق تقنية المعلومات:

- تتكون **مخاطر التحكم** من احتمال فشل ضوابط تقنية المعلومات التي تم تبنيها من قبل المنظمة المدققة في التخفيف من الأثر السلبي الذي تم تصميمها استجابة له. على سبيل المثال، قد يعتمد نظام المعلومات المطلوب لضمان تقييد الوصول إلى البيانات السرية على الأفراد المصرح لهم التحكم في طلب تقديم اسم مستخدم وكلمة مرور من قبل الأفراد الذين يحاولون الوصول. تتمثل مخاطر التحكم في هذه الحالة في أن اسم المستخدم وكلمة المرور ليسا آمنين بشكل كاف ويمكن تخمينهما من قبل الأفراد غير المصرح لهم من خلال المحاولات المتكررة، مما يؤدي إلى فقدان السرية والتأثير السلبي المحتمل على المنظمة. المنظمة التي تصر على استخدام كلمات مرور آمنة وغير تافهة تحتوي على مزيج من الرموز الأبجدية والرقمية والخاصة وتضمن أن يمنع نظام المعلومات الوصول إلى اسم المستخدم بعد عدد معين من المحاولات

[30] يشمل الموقع الخوادم الخلفية (التطبيق أو البيانات) ومواقع المستخدمين والشبكات بطريقة عامة، كما يحدد المواقع المادية التي سيتم تغطيتها في شبكة موزعة عبر المباني أو المدن أو البلدان، إذا كان ذلك ممكنًا.

الفاشلة للوصول سيكون أقل السيطرة على المخاطر من تلك التي لا تحتوي على هذه الميزات. يمكن أيضًا استخدام المصادقة متعددة العوامل لتقليل مخاطر التحكم في مثل هذه الحالة.

- تتكون **مخاطر الاكتشاف** من احتمال عدم اكتشاف المدقق لغياب أو فشل أو عدم كفاية ضوابط تقنية المعلومات المعتمدة من قبل المنظمة، والتي قد يكون لها تأثير سلبي محتمل على المنظمة.
- **المخاطر المتبقية** هي المستوى المتبقي من المخاطر بعد تطبيق الضوابط، ويمكن تقليلها بشكل أكبر من خلال تحديد تلك المجالات التي تتطلب المزيد من السيطرة. يمكن تحديد مستوى مقبول من هدف المخاطر من قبل الإدارة (قابلية المخاطرة).

في سياق تقنية المعلومات، تنقسم الضوابط إلى فئتين، والتي تظهر في الشكل 4: الضوابط العامة وضوابط التطبيق. تعتمد الفئات على مدى تأثير عنصر التحكم وما إذا كان مرتبطًا بأي تطبيق معين.

شكل4 : الضوابط العامة والتطبيق

المصدر: مجهول.

الضوابط العامة لتقنية المعلومات هي أساس هيكل التحكم في تقنية المعلومات. هذه تتعلق بالبيئة العامة التي يتم فيها تطوير أنظمة تقنية المعلومات وتشغيلها وإدارتها وصيانتها. الضوابط العامة هي إجراءات يدوية أو آلية تهدف إلى ضمان سرية وسلامة وتوافر المعلومات في البيئة المادية التي يتم من خلالها تطوير أنظمة المعلومات وصيانتها وتشغيلها. تضع الضوابط العامة إطارًا للرقابة الشاملة لأنشطة تقنية المعلومات وتوفر ضمانًا بأن أهداف الرقابة العامة مطبقة.

يتم تنفيذ الضوابط العامة باستخدام عدد من الأدوات مثل السياسة والتوجيه والإجراءات بالإضافة إلى تنفيذ هيكل إداري مناسب، بما في ذلك إدارة أنظمة تقنية المعلومات الخاصة بالمؤسسة. تتضمن أمثلة الضوابط العامة تطوير

وتنفيذ استراتيجية تقنية المعلومات وسياسة أمن تقنية المعلومات، وإنشاء لجنة توجيهية لتقنية المعلومات، وتنظيم موظفي تقنية المعلومات لفصل المهام المتضاربة، وإنشاء أدوار النظام والامتيازات المناسبة لدور الشخص، والتخطيط للوقاية من الكوارث والتعافي منها.

الضوابط العامة لتقنية المعلومات ليست خاصة بتدفقات المعاملات الفردية أو حزم المحاسبة أو التطبيقات المالية الخاصة. الهدف من الضوابط العامة لتقنية المعلومات هو ضمان التطوير والتنفيذ المناسبين للتطبيقات وملفات البرامج والبيانات وعمليات الكمبيوتر.

ضوابط التطبيق هي ضوابط محددة تنفرد بها أنظمة المعلومات في كل تطبيق. ضوابط التطبيق هي إجراءات يدوية أو مؤتمتة تعتمد على تقنية المعلومات داخل نظام معلومات تؤثر على معالجة المعاملات وقد تتعلق بالتحقق من صحة بيانات الإسهامات والمعالجة الدقيقة للبيانات وتسليم بيانات المخرجات والضوابط المتعلقة بسلامة البيانات الرئيسة. تنطبق على شرائح التطبيق وتتعلق بالمعاملات والبيانات الموجودة. على سبيل المثال، في تطبيق الدفع عبر الإنترنت، يمكن أن يتمثل أحد ضوابط الإسهامات في أن تاريخ انتهاء صلاحية بطاقة الائتمان يجب أن يتجاوز تاريخ المعاملة، ويجب تشفير التفاصيل التي تم إدخالها.

قد يكون لتصميم وتنفيذ الضوابط العامة لتقنية المعلومات تأثير كبير على فعالية ضوابط التطبيق. تزود الضوابط العامة التطبيقات بالموارد التي تحتاجها للتشغيل وتضمن عدم إمكانية إجراء الاستفسارات والتغييرات غير المصرح بها على التطبيقات (أي أنها محمية من إعادة البرمجة) أو البيانات الأساسية (على سبيل المثال، المجموعة الكبيرة من بيانات المعاملات).

مناطق العناصر الحرجة لعناصر التحكم العامة على مستوى التطبيق هي[31]

- إدارة الأمن،
- التحكم في الوصول / الفصل بين وصول المستخدم،

[31] مكتب محاسبة الحكومة الأمريكية، *دليل تدقيق ضوابط نظام المعلومات الفيدرالية (FISCAM)*، GAO-09-232G، (2 فبراير 2009)، https://www.gao.gov/products/gao-09-232g.

- إدارة التكوين / إدارة التغيير،
- إدارة العمليات، و
- التخطيط للطوارئ.

تعمل ضوابط التطبيق على المعاملات الفردية أو المجموعات وتضمن أن المعاملات يتم إدخالها ومعالجتها وإخراجها بشكل صحيح. يؤثر تصميم وفعالية تشغيل ضوابط تقنية المعلومات العامة بشكل كبير على مدى إمكانية الاعتماد على ضوابط التطبيق من قبل الإدارة لإدارة المخاطر.

د. لماذا تعتبر ضوابط تقنية المعلومات مهمة لمدقق تقنية المعلومات؟

بشكل عام، يُطلب من مدقق تقنية المعلومات اختبار الضوابط المتعلقة بالتقنية. نظرًا لأن المزيد والمزيد من المؤسسات تعتمد على تقنية المعلومات لأتمتة عملياتها، فإن الخط الذي يقسم دور مدقق تقنية المعلومات والمراجع غير المتخصص في تقنية المعلومات يتقلص أيضًا بسرعة. كحد أدنى، يُطلب من جميع المدققين فهم بيئة الرقابة للمؤسسة الخاضعة للرقابة بغية تقديم ضمان بشأن الضوابط الداخلية العاملة في المنظمة. وفقًا للمبادئ الأساسية ISSAL لمراجعة القطاع العام، "يجب أن يحصل المدققون على فهم لطبيعة الكيان / البرنامج الذي سيتم تدقيقه".[32] وهذا يشمل فهم الضوابط الداخلية، فضلا عن الأهداف والعمليات والبيئة التنظيمية والأنظمة والعمليات التجارية المعنية.

تعتمد كل منطقة تحكم على مجموعة من أهداف الرقابة التي تضعها المنظمة بغية التخفيف من مخاطر الرقابة، بما في ذلك المتطلبات الفنية المطبقة لأنظمة المنظمة. يتمثل دور المدقق في فهم مخاطر الأعمال وتقنية المعلومات المحتملة التي تواجه المنظمة الخاضعة للرقابة، وبالتالي تقييم ما إذا كانت الضوابط المستخدمة كافية لتلبية هدف الرقابة. في حالة الضوابط العامة لتقنية المعلومات، من المهم للمدقق أن يفهم الفئات الواسعة ومدى الضوابط العامة في التشغيل، وتقييم الرقابة الإدارية وتوعية الموظفين في المنظمة لنفسه، ومعرفة مدى فعالية الضوابط في بغية تقديم ضمان. إذا كانت الضوابط العامة ضعيفة، فإنها تقلل بشدة من موثوقية الضوابط المرتبطة بتطبيقات تقنية المعلومات الفردية.

في الفصول اللاحقة، مثل الفصل 8 بخصوص ضوابط التطبيق، تمت مناقشة بعض المجالات الرئيسة لضوابط تقنية المعلومات العامة وضوابط التطبيقات بالتفصيل.

رابعا. الخطوة 3: إجراء تدقيق تقنية المعلومات

يتضمن إجراء تدقيق تقنية المعلومات خطوات رئيسية مثل جمع أدلة المراجعة التي تكون كافية ومناسبة وذات صلة وموثوقة؛ إجراء تقييم أولي للضوابط، مثل السياسات والإجراءات، لتقييم موثوقيتها؛ والاختبار الموضوعي التفصيلي للمجالات ذات الأولوية للتأكد من درجة عمل عنصر التحكم بشكل صحيح.

أ. جمع أدلة المراجعة

i. شهادة

يجب أن تكون نتائج المراجعة مدعومة بالأدلة، لذا فإن كمية ونوعية الأدلة التي تم الحصول عليها مهمة. هذا يعني أن مدقق تقنية المعلومات سيحتاج إلى دراسة وتقييم الأدلة التي يخططون للحصول عليها، أو التي حصلوا عليها، للتأكد من كفايتها وملاءمتها. تشير الكفاية إلى كمية الأدلة التي تم جمعها. الملاءمة تشير إلى جودة الأدلة، وما إذا كانت موثوقة وذات صلة. يمكن للمدققين تقييم ما إذا كانت الأدلة ملائمة وموثوقة من خلال مراعاة، من بين أمور أخرى، طبيعة مصدر الدليل وسمعة المصدر؛ الضوابط التي تديرها الجهة الخاضعة للرقابة، ووجود أدلة متناقضة أو مؤكدة، والطرق والنماذج والافتراضات المستخدمة في إعداد المعلومات في الدليل.

تعتبر مصفوفة نتائج المراجعة إحدى الأدوات المفيدة لتقييم أدلة المراجعة وتطوير الاستنتاجات والتوصيات. تتيح هذه الأداة للمدققين تحديد ما إذا كانت النتائج والتوصيات، إن وجدت، تستند إلى أدلة كافية ومناسبة. يقدم الشكل 5 مثالاً على نموذج مصفوفة نتائج المراجعة.[33]

---

[32] المنظمة الدولية للأجهزة العليا للرقابة المالية والمحاسبة، *ISSAL 100*، الفقرة 45.

[33] يمكن العثور على رسم توضيحي لمصفوفة نتائج المراجعة المكتملة في الصفحة 174 من مبادرة تطوير المنظمة الدولية للمؤسسات العليا للرقابة المالية والمحاسبة، *دليل تنفيذ تدقيق الأداء المعايير الدولية للأجهزة العليا للرقابة المالية*، الإصدار 1 (أغسطس 2021)، https://www.idi.no/work-streams / professional-sais / work-stream-library / performance-Audit-isai-application-handbook.

شكل5 : قالب مصفوفة نتائج المراجعة

النتيجة	بيان النتيجة (الموقف المكتشف)	معظم الأحداث ذات الصلة التي تم التعرف عليها في إطار العمل.
	المعايير	المعلومات المستخدمة لتحديد إذا ما كان الأداء المتوقع لهدف عملية التدقيق مُرضٍ، يتجاوز التوقعات، أو غير مُرضٍ.
	الأدلة والتحليل	نتيجة تطبيق طرق تحليل البيانات أو تقييم الأدلة. يمكن الإشارة إلى الأساليب المستخدمة لمعالجة المعلومات التي تم جمعها في إطار العمل والنتائج المتحققة.
	الأسباب	الأسباب وراء الحادث المكتشف. ربما يكون متعلقًا بعملية التشغيل أو التصميم للهدف من عملية التدقيق. ربما يكون خارجا عن سيطرة المدير. يجب أن تكون أي توصية ذات صلةٍ بالأسباب.
	التأثيرات	الأسباب المتعلقة بالأسباب والأدلة المتوافقة ربما يكون أداة القياس لأهمية النتائج.
هل النتائج كافية (نعم/لا)؟ وإذا لم، ما هو العمل المتبقي الضروري لمعالجة أي فجوات في الدليل؟		خذ الدليل الذي لديك بعين الاعتبار لكل عنصر للنتيجة وإذا ما كان كافيًا ومناسبًا. إذا لم يكن الدليل الحالي كافيًا لكل عنصر، ، ما هو العمل المتبقي الضروري لمعالجة أي فجوات في الدليل؟
الممارسات الجيدة		الأعمال التي تم تحديدها والتي تؤدي إلى الأداء الجيد. ربما تدعم التوصيات.
التوصيات		المقترحات لمعالجة الأسباب (أو أوجه القصور) التي تم تحديدها.

ملحوظة: يهدف هذا الشكل إلى تقديم مثال توضيحي ويجب تكييفه مع ارتباطات المراجعة الفردية.

المصدر: Adapted from U.S. GAO and SAI Brazil.

المرحلة 1 - التقييم الأولي لضوابط تقنية المعلومات

يجب على مدقق تقنية المعلومات إجراء تقييم أولي لضوابط تقنية المعلومات - الضوابط العامة والتطبيقية - في النظام لاستنباط فهم للتأكيد على أنها موثوقة وكافية لتحقيق هدف المراجعة.

قد يشمل نطاق تقييم ضوابط تقنية المعلومات تقييم ما إذا كان

- تم تحديد سياسة تقنية المعلومات واعتمادها وإبلاغها؛
- وجود هيكل حوكمة تقنية المعلومات وتشغيله؛
- الضوابط تعكس بدقة المتطلبات الفنية لأنظمة المعلومات الأساسية؛
- تم إجراء جرد لأصول نظام المعلومات بشكل دوري وتم تحديد متطلبات الزيادة والاستبدال والإزالة؛
- أن تكون عمليات تقاسم البنية التحتية والخدمات المشتركة لأنظمة المعلومات مع المنظمات العامة الأخرى قائمة وعاملة؛
- تم تحديد عمليات تطوير واكتساب وصيانة تقنية المعلومات واعتمادها وإبلاغها (بما في ذلك إدارة التغيير)؛
- تم تحديد عمليات تقنية المعلومات (الاستعانة بمصادر داخلية، والاستعانة بمصادر خارجية، واتفاقيات الخدمة) واعتمادها وإبلاغها؛
- تم اعتماد تدابير لضمان الأمن المادي وظروف العمل المادية المقصودة؛
- تم اعتماد تدابير لتدريب وتوعية الموارد البشرية لضمان سرية وسلامة وتوافر المعلومات وكذلك الامتثال لسياسة تقنية المعلومات ومتطلبات هيكل الإدارة؛

- تم اعتماد تدابير لضمان السرية والنزاهة وتوافر مختلف طرق وقنوات الاتصال؛
- تم اعتماد تدابير لإدارة الامتثال القانوني؛
- تم اعتماد تدابير لإدارة استمرارية الأعمال وإدارة التعافي من الكوارث؛
- تم اعتماد تدابير لضمان اكتمال ودقة وصلاحية وسرية المعاملات والبيانات التي يتم إجراؤها كجزء من العمليات التجارية؛ و
- تم اعتماد تدابير لضمان المعالجة المناسبة، والدقيقة، والكاملة للمعلومات بين مكونات النظام، مثل بين التطبيقات.

اعتمادًا على الهدف من المراجعة، قد يهتم المدققون بتصميم وتنفيذ وفعالية تشغيل الضوابط. إذا كان المدقق معنيًا بتصميم عنصر التحكم، فقد يكون من الكافي إجراء مقابلة أو فحص لقواعد العمل الموثقة. إذا كان المدقق معنيًا بتنفيذ الضوابط، فقد لا يكون الاستفسار كافيًا، وقد يكون من الضروري إجراء جولة تفصيلية - أسلوب تدقيق لتأكيد فهم الضوابط - أو إجراء تحليل للبيانات لإثبات تنفيذ الرقابة.. أخيرًا، قد يُطلب من المدقق الذي لديه مخاوف بشأن الفاعلية التشغيلية للرقابة أن يخطط لاختبار عينة من المعاملات لإثبات أن الرقابة قد عملت بفعالية طوال الفترة ذات الصلة.

قد ينظر المدققون أيضًا في كيفية تأثير الأدلة المتعلقة بالضوابط العامة على طبيعة وتوقيت ومدى الإجراءات والأدلة المطلوبة للحصول على تأكيد بخصوص تشغيل ضوابط التطبيق. على سبيل المثال، يجب على المدققين أيضًا النظر في الأدلة التي تدعم الوصول المنطقي للموظفين إلى أنظمة تقنية المعلومات وإدارة التغيير داخل بيئة الإنتاج. إذا حصل المدققون على أدلة مراجعة كافية ومناسبة فيما يتعلق بفاعلية أدوات الرقابة العامة، فقد يكونون قادرين على استنتاج الفاعلية التشغيلية لإجراءات مراقبة التطبيق المؤتمتة. يمكن القيام بذلك عن طريق اختبار عينة أصغر من المعاملات لأن فعالية بيئة تقنية المعلومات العامة توفر دليلاً للمراجعين بخصوص فعالية مراقبة التطبيق في الفترة ذات الصلة. في حالة إجراءات التحكم اليدوي في التطبيق، قد يتعين على المدققين اختبار حجم عينة مناسب لمستوى الثقة المحدد.

المرحلة 2 - الاختبار الموضوعي

بناءً على تقييم ضوابط تقنية المعلومات، قد يحدد المدققون المجالات ذات الأولوية لإجراء الاختبارات الموضوعية، والتي تتضمن اختبارًا تفصيليًا لضوابط تقنية المعلومات من خلال استخدام تقنيات مختلفة للاستعلام عن البيانات واستخراجها وتحليلها. في الاختبار الموضوعي، تم تصميم الاختبارات لإثبات التأكيدات وفقًا لأهداف المراجعة.

من بين التقنيات المستخدمة من قبل مدققي تقنية المعلومات لتحليل البيانات الإبلاغ عن الاستثناءات، حيث يتم توثيق الانحرافات عن الأداء المتوقع؛ مقارنة الملفات التقسيم الطبقي، فرز عناصر البيانات في مجموعات متميزة؛ أخذ العينات؛ وشيكات مكررة. ثمة خيار آخر لاختبار حل النظام وهو نهج "الخيط والعقدة"، والذي يتقدم في عملية تجارية واحدة في كل مرة لتحديد نقاط النشاط المهمة وما إذا كانت ضوابط تقنية المعلومات المناسبة والملائمة موجودة في كل نقطة نشاط. يجب أن يكون مدققو تقنية المعلومات على دراية بهذه الخيارات وأن يستخدموا الأدوات المناسبة للتحليل. يمكن للمدققين استخدام برنامج تدقيق معمم أو متخصص لإجراء تحليل المعلومات.

عند إجراء اختبار موضوعي، يجب على مدققي تقنية المعلومات التأكد من أن الأدلة الإلكترونية التي تم جمعها وتوثيقها كافية وموثوقة ودقيقة للحفاظ على ملاحظات المراجعة. قد تتكون هذه الأدلة الإلكترونية من ملفات البيانات، وسجلات المستخدمين، والنماذج التحليلية، وتقارير نظم المعلومات الإدارية، ويجب جمعها وتخزينها بشكل مناسب بحيث تكون متاحة للتأكيد على دقة وصحة عملية المراجعة.

يجب على مدقق تقنية المعلومات أيضًا اختيار تقييم مناسب للمخاطر واستخدام تقنيات أخذ العينات لاستخلاص استنتاجات مناسبة بناءً على عمليات تحقق كافية إحصائيًا على بيانات محدودة. وبشكل عام، من الممارسات الجيدة الاستعانة بخبير أو إحصائي داخل المنظمة لاختيار وتحديد طريقة أخذ العينات.

حيثما يسمح حجم البيانات ونقلها وتخزينها وقدرتها على المعالجة، يمكن أيضًا إجراء تقييم مخاطر عالي الجودة على جميع السكان لتحديد الاتجاهات المرتبطة بفهم المدقق للأعمال. على سبيل المثال، يمكن للمدقق الحصول على قائمة بجميع المستخدمين وتواريخ تسجيل الدخول الأخيرة للنظام ومقارنتها بقائمة تواريخ المغادرة الرسمية للحصول على تحليل بنسبة 100 بالمائة. وهذا من شأنه أن يمكّن المدقق من تحديد المعاملات أو نقاط البيانات الشاذة لتشكيل جزء من العينة بطريقة أكثر استهدافًا للمخاطر.

ب. التعامل مع المنظمة الخاضعة للرقابة

توصي المعايير الدولية للأجهزة الرقابية بأن يقوم المدققون بإنشاء اتصال فعال طوال عملية المراجعة وإبقاء المنظمة الخاضعة للرقابة على علم بجميع الأمور المتعلقة بالمراجعة.[34] بالنسبة لتدقيق تقنية المعلومات، قد يطلب المدققون التعاون والدعم اللازمين من المنظمة الخاضعة للتدقيق في استكمال المراجعة، بما في ذلك الوصول إلى السجلات والمعلومات. قد يحدد المدققون طريقة الوصول إلى البيانات الإلكترونية بالصيغة اللازمة للسماح بالتحليل، بالتشاور مع المنظمة الخاضعة للرقابة. سيكون أسلوب

[34] المنظمة الدولية *للأجهزة العليا للرقابة المالية والمحاسبة* .ISSAI 100

الوصول إلى البيانات خاصًا بالجهاز.

ج. توثيق تدقيق تقنية المعلومات

توثيق تدقيق نظم المعلومات هو سجل أعمال المراجعة المنفذة والأدلة الداعمة للنتائج والاستنتاجات. يجب ضمان الحفاظ على النتائج والأدلة من قبل مدققي تقنية المعلومات بحيث تتوافق مع متطلبات الموثوقية والاكتمال والكفاية والصحة. من المهم أيضًا لمدققي تقنية المعلومات التأكد من الحفاظ على عملية المراجعة لتمكين التحقق اللاحق من إجراءات التحليل. هذا ينطوي على تقنيات التوثيق المناسبة.

يتضمن التوثيق سجلاً لـ

- تخطيط وإعداد نطاق وأهداف المراجعة؛
- برامج المراجعة.
- الأدلة التي تم جمعها على أساس الاستنتاجات التي تم التوصل إليها؛
- جميع أوراق العمل، بما في ذلك الملفات العامة المتعلقة بالمنظمة والنظام؛
- النقاط التي تمت مناقشتها في المقابلات توضح بوضوح موضوع المناقشة، والشخص الذي تمت مقابلته، والمنصب والتسمية، والوقت، والمكان؛
- الملاحظات حيث لاحظ المراجع أداء العمل:
  - يجب أن تتضمن الملاحظات على الأقل المكان والزمان وسبب الملاحظة والأشخاص المعنيين؛
- التقارير والبيانات التي تم الحصول عليها من النظام مباشرة من قبل المدقق أو المقدمة من قبل الموظفين المدققين:
  - يجب على مدقق تقنية المعلومات التأكد من أن هذه التقارير تحمل مصدر التقرير، والتاريخ والوقت، والظروف التي تمت تغطيتها؛
  - خيار واحد لالتقاط هذه التفاصيل هو استخدام لقطة الشاشة؛ و
- أي تعليقات وتوضيحات أضافها المدققون في نقاط مختلفة من التوثيق فيما يتعلق بالمخاوف والشكوك والحاجة إلى معلومات إضافية:
  - يجب على المدقق العودة إلى هذه التعليقات لاحقًا وإضافة ملاحظات ومراجع بخصوص كيف وأين تم حلها.

قد تحتوي الأدلة التي تم جمعها أثناء تدقيق تقنية المعلومات على الطوابع الزمنية والتفاصيل اللازمة التي تحتوي على خطوات تحليل البيانات التي تم إجراؤها بحيث يكون ثمة وضوح بشأن وقت إنشاء الدليل وتخزينه وتعديله آخر مرة، للتخفيف من مخاطر التغييرات اللاحقة. يقدم الشكل 6 أمثلة لما يجب أن يتوقعه مدقق تقنية المعلومات ليكون قادرًا على فهمه من توثيق المراجعة.

شكل6 : فهم توثيق تدقيق تقنية المعلومات

ما الذي يتعين على المدقق الخبير أن يفهمه من توثيق عملية التدقيق؟	
✓ النتائج التي تم التوصل إليها نتيجة للأمور المهمة السابقة. ✓ القرارات المهمة أو الرئيسة التي اتخذت للتوصل إلى هذه النتائج.	✓ طبيعة ووقت ونطاق العمل المؤدى ✓ نتائج عملية التدقيق والأدلة المتاحة ✓ الأمور المهمة التي تنشأ خلال عملية التدقيق (على سبيل المثال، التغييرات في نطاق أو منهج التدقيق والقرارات المتعلقة بعامل المخاطرة الجديد الذي يتم تحديده خلال التدقيق والإجراءات المتخذة كنتيجة لعدم الاتفاق بين الكيان المدقق والفريق، إلخ).

ملحوظة: يهدف هذا الشكل إلى تقديم مثال توضيحي ويجب تكييفه مع ارتباطات المراجعة الفردية.

المصدر: Performance Audit Subcommittee Development Team.

كما هو الحال مع جميع وثائق المراجعة، يجب الاحتفاظ بوثائق تدقيق تقنية المعلومات وحمايتها من أي تعديل وحذف غير مصرح به. قد تطور الأجهزة العليا للرقابة المالية والمحاسبة معايير جديدة للاحتفاظ بوثائق تدقيق تقنية المعلومات أو تكييف المعايير الحالية لتلبية متطلبات الاحتفاظ بالوثائق المتعلقة بمراجعة تقنية المعلومات. يجب أن تكون فترة الاستبقاء وظيفة من اختصاص الجهاز الأعلى للرقابة المالية والمحاسبة والنظام الأساسي (الأنظمة) الذي يحكم أنشطته. يمكن إيلاء اهتمام خاص لوسائل الإعلام، والتنسيق، والعمر المتوقع، ومتطلبات التخزين لهذه البيانات، للتأكد من أن البيانات قابلة للقراءة ضمن الإطار الزمني المحدد في سياسة الاحتفاظ بالبيانات وأرشفتها في كل

جهاز. قد يستلزم ذلك تحويل البيانات من تنسيق إلى آخر لمواكبة التقدم التكنولوجي والتقادم.

في حالة فحص التقارير الفنية التي أعدها مدققون الطرف الثالث بخصوص موضوعات تقنية محددة، قد يتبنى المدققون إجراءات مناسبة لضمان موثوقية بعض جوانب الأداء أو المالية أو الامتثال. إذا، نتيجة لهذه الإجراءات، يتم الاعتماد على محتويات هذه التقارير، يجب الكشف عن حقيقة الاعتماد بشكل مناسب.

للحفاظ على البيانات الإلكترونية، يجب على الأجهزة العليا للرقابة المالية والمحاسبة توفير نسخة احتياطية من البيانات الواردة من المنظمة الخاضعة للرقابة ونتائج الاستفسارات والتحليل. يجب أن تبقى وثائق المراجعة سرية ويجب الاحتفاظ بها لفترة حسبما يقرره الجهاز أو يفرضه القانون. كما يجب أن تشكل مسودات المراجعة والتقارير النهائية جزءًا من توثيق المراجعة. عندما تتم مراجعة أعمال المراجعة من قبل نظير أو رئيس، ينبغي أيضًا تسجيل الملاحظات الناشئة عن المراجعة في الوثائق.

د. المراجعة الإشرافية

يجب الإشراف على عمل موظفي المراجعة بشكل صحيح أثناء المراجعة، ويجب مراجعة العمل الموثق من قبل أحد كبار موظفي المراجعة.[35] كما يجب على كبار موظفي المراجعة تقديم التوجيه اللازم، والتدريب، ودور التوجيه أثناء المراجعة.

الخطوة الرابعة: الإبلاغ عن نتائج تدقيق تقنية المعلومات

يجب أن يتبع تقرير تدقيق تقنية المعلومات المخطط العام لنظام التقارير الذي يتبعه الجهاز الأعلى للرقابة المالية والمحاسبة. يجب أن تقيس تقارير تدقيق تقنية المعلومات الجوانب الفنية المبلغ عنها بناءً على مستوى التفاصيل المطلوبة من قبل جمهور التقرير.

يجب على مدقق تقنية المعلومات تقديم تقرير عن النتائج في الوقت المناسب، ويجب أن تكون النتائج بناءة ومفيدة للمنظمة الخاضعة للرقابة وكذلك مفيدة لأصحاب المصلحة الآخرين. يمكن تقديم التقرير إلى السلطات المختصة حسب اختصاصات الجهاز الأعلى للرقابة المالية والمحاسبة وتدقيق تقنية المعلومات.

يجب أن يكون المدققون على دراية بالحاجة إلى الحد من استخدام المصطلحات الفنية وحساسية المعلومات المقدمة (على سبيل المثال، كلمات المرور وأسماء المستخدمين والمعلومات الشخصية) في التقرير. على الرغم من الطبيعة الفنية لتدقيق تقنية المعلومات، يجب على المدققين التأكد من أن التقرير مفهوم تمامًا من قبل الإدارة العليا للمؤسسة الخاضعة للرقابة وأصحاب المصلحة وعامة الناس. كجزء من هذه العملية، يجب أن يكون مدققو تقنية المعلومات على دراية بأن جمهورهم هم خبراء آخرون في تقنية المعلومات وعامة الناس، وأنهم سيحتاجون إلى تفسير المحتوى الفني لهذا الأخير.

يجب على المدققين النظر في التأثير السلبي المحتمل للتقرير بمجرد نشر تقرير تدقيق تقنية المعلومات. على سبيل المثال، إذا كشف تقرير تدقيق تقنية المعلومات عن بعض المخاطر الأمنية في نظام المعلومات الخاص بمؤسسة خاضعة للرقابة، وتم الإبلاغ عن نفس المخاطر قبل اعتماد الضوابط اللازمة للتخفيف من المخاطر، فقد تتعرض نقاط ضعف نظام المعلومات للجمهور. في مثل هذا السيناريو، قد ينظر المدققون في الخيارات - مثل الإبلاغ فقط بعد اعتماد الضوابط الضرورية، أو عدم الإبلاغ عن المخاطر الأمنية الدقيقة بالكامل لتجنب التأثير السلبي المحتمل على المنظمة الخاضعة للرقابة، أو تقديم تقرير سري منفصل / مرفق يكون غير مخصص للتداول على نطاق أوسع.

لُطفًا راجع الملحق الثاني للحصول على روابط لتقارير المراجعة المحددة من قبل الأجهزة العليا للرقابة المالية والمحاسبة بخصوص العالم والمتعلقة بفصول هذا الدليل. يمكن أن تقدم تقارير المراجعة هذه أمثلة قيمة لمجموعة واسعة من مجالات تدقيق تقنية المعلومات التي تمت مناقشتها في هذا الدليل.

أ. مراحل الإبلاغ

تعتمد تقارير تدقيق تقنية المعلومات على تقاليد الأجهزة العليا للرقابة المالية والمحاسبة وبيئاتها القانونية. غالبًا ما يتكون إعداد التقارير خلال عملية المراجعة من مراحل مثل:

1. مشروع تقرير

تبدأ عملية إعداد التقارير بمناقشة المسودة الأولى للتقرير. يتم إرسال هذه المسودة، بعد الموافقة عليها والموافقة عليها داخليًا داخل الجهاز الأعلى للرقابة المالية والمحاسبة، إلى إدارة الجهاز الخاضع للرقابة قبل الاجتماع الختامي. ثم يتم إدراج المشروع كمسألة للمناقشة في الجلسة الختامية. يسمح هذا بتحديد أي صياغة تحريضية و/ أو أخطاء في الوقائع و/ أو تناقضات يتم تحديدها أو تصحيحها أو التخلص منها في مرحلة مبكرة. بمجرد أن تناقش المنظمة المدققة والمدقق محتويات المسودة، يقوم المدقق بإجراء التعديلات

[35] المنظمة الدولية *للأجهزة العليا للرقابة المالية والمحاسبة*، *ISSAI 100*، الفقرات 38 و39 و50.

اللازمة ويرسل إلى المنظمة المدققة مسودة رسمية.

2. رسالة ادارية

خطاب الإدارة هو المسودة الرسمية المقدمة إلى المنظمة الخاضعة للرقابة حتى تتمكن من الرد على الملاحظات المطروحة. يسمح هذا للإدارة بالتركيز على النتائج والاستنتاجات والتوصيات في المسودة الرسمية التي يتلقونها. في هذه المرحلة، من واجب الإدارة كتابة التعليقات / الردود رسميًا إلى المدقق ومعالجة جميع النتائج.

3. تقرير المراجعة النهائي

عندما يتم استلام تعليقات المنظمة الخاضعة للرقابة، يقوم المدقق بعد ذلك بإعداد رد يشير إلى موقف المراجعة. يتم تحقيق ذلك من خلال تجميع تعليقات المدقق واستجابة المنظمة في تقرير واحد، وهو تقرير المراجعة (تقرير المراجعة النهائي).

عند الإبلاغ عن المخالفات أو حالات عدم الامتثال للقوانين أو اللوائح، يجب على المدققين أن يضعوا في اعتبارهم وضع نتائجهم في المنظور الصحيح. يمكن إعداد تقارير عن المخالفات بغض النظر عن مؤهلات رأي المراجع.

تميل تقارير المراجعة، بحكم طبيعتها، إلى احتواء انتقادات مهمة، ولكن لكي تكون بناءة، يجب أن تتناول أيضًا الإجراءات العلاجية المستقبلية من خلال دمج بيانات من المنظمة الخاضعة للرقابة أو المدقق، بما في ذلك الاستنتاجات أو التوصيات.[36] اعتمادًا على الجهاز الأعلى للرقابة المالية والمحاسبة، قد يكون المتلقي النهائي لتقرير الإدارة هم المسؤولون عن إدارة عمليات المؤسسة أو أولئك المسؤولين عن الإشراف على الاتجاه الاستراتيجي للكيان والالتزامات المتعلقة بمساءلة الكيان.

في عمليات المراجعة التي تتضمن أعمال تدقيق تقنية المعلومات، قد يتم إرسال نتيجة تدقيق تقنية المعلومات، في بعض الحالات، إلى المنظمة من خلال خطاب منفصل. في هذه الحالات، قد يكون من المهم شرح كيفية ارتباط نتيجة أعمال المراجعة بالاتصالات الأخرى التي تشكل جزءًا من نفس الأداء، أو المالية، أو تدقيق الامتثال وكيف يمكن أن تكون نتائج أعمال تدقيق تقنية المعلومات ذات صلة بالجهاز الأعلى للرقابة المالية والمحاسبة الناتج. تقرير المراجعة.

4. صياغة الاستنتاجات والتوصيات

يجب أن تستند نتائج المراجعة والاستنتاجات والتوصيات إلى الأدلة. عند صياغة الاستنتاجات، يجب على مدقق تقنية المعلومات مراعاة الأهمية النسبية للأمر في سياق طبيعة المراجعة أو المنظمة الخاضعة للتدقيق.[37] بغية الإبلاغ المتوازن، يجب أيضًا الإبلاغ عن الإنجازات الجديرة بالملاحظة التي تقع ضمن ولاية الجهاز الأعلى للرقابة المالية والمحاسبة.

يجب على مدققي تقنية المعلومات وضع استنتاجات بناءً على النتائج بناءً على الأهداف. يجب أن تكون الاستنتاجات ذات صلة ومنطقية وغير متحيزة. يجب تجنب الاستنتاجات الشاملة المتعلقة بغياب الضوابط والمخاطر، عندما لا تكون مدعومة باختبار موضوعي مثل اختبار التحكم.

يجب على مدققي تقنية المعلومات تقديم التوصيات عندما يتم إثبات إمكانية حدوث تحسن كبير في العمليات والأداء من خلال النتائج. يجب على المدققين أيضًا الإبلاغ عن حالة النتائج والتوصيات الهامة غير المصححة من عمليات المراجعة السابقة والتي تؤثر على أهداف المراجعة الحالية. يمكن أن تشجع التوصيات البناءة التحسينات. تكون التوصيات بناءة للغاية عندما تكون موجهة إلى حل سبب المشكلات المحددة، وتكون موجهة نحو العمل ومحددة، وموجهة إلى الأطراف التي لديها سلطة التصرف، وتكون مجدية، وفعالة من حيث التكلفة.

5. القيود والقيود على تدقيق تقنية المعلومات

كما ينبغي الإشارة إلى القيود المفروضة على تدقيق تقنية المعلومات في التقرير. تتمثل القيود النموذجية في عدم كفاية الوصول إلى البيانات والمعلومات، ونقص التوثيق الكافي لعملية تقنية المعلومات، وقيادة مدقق تقنية المعلومات إلى ابتكار طرقه الخاصة في التحقيق والتحليل لاستخلاص النتائج. يجب الإشارة إلى أي قيد أو قيد آخر يواجهه مدقق تقنية المعلومات ويؤثر على نطاق المراجعة أو التنفيذ في التقرير بشكل مناسب.

6. استجابة الإدارة

في حالة تقارير تدقيق تقنية المعلومات، من المهم للغاية الحصول على رد على ملاحظات المراجعة. يجب أن يعقد مدققو تقنية المعلومات اجتماعات مع إدارة الوكالة على أعلى

---

[36] المنظمة الدولية للأجهزة العليا للرقابة المالية والمحاسبة، *ISSAL 100*، الفقرة 51.

[37] المنظمة الدولية *للأجهزة العليا للرقابة المالية والمحاسبة، ISSAL 100*، الفقرة 50.

مستوى وأن يوثقوا استجابتهم. إذا فشلت هذه الجهود، يجب الاحتفاظ بالأدلة الكافية بخصوص الجهود المبذولة في السجل وذكرها في التقرير.

السادس. المراجع وقراءات إضافية

مجتمع المراجعة الداخلي من الممارسين. *تقييم المخاطر في تخطيط المراجعة*. https://www.pempal.org/sites/pempal/files/event/attachments/cross_day-2_4_pempal-iacop-risk-assessment-in-audit-planning_eng.pdf. أبريل 2014.

مبادرة تطوير المنظمة الدولية للأجهزة العليا للرقابة المالية والمحاسبة. *مبادرة الإنتوساي للتنمية (IDI) برنامج تدقيق أفروساي / تقنية المعلومات الإلكترونية*.

مبادرة تطوير المنظمة الدولية للأجهزة العليا للرقابة المالية والمحاسبة. *دليل تنفيذ المعايير الدولية للأجهزة العليا للرقابة المالية لرقابة الأداء*، الإصدار 1. *https://www.idi.no/work-streams/professional-sais/work-stream-library/performance-audit-issai-implementation-handbook*. أغسطس 2021.

المنظمة الدولية للأجهزة العليا للرقابة المالية والمحاسبة. *المعايير الدولية للأجهزة العليا للرقابة المالية 100 (ISSAI): المبادئ الأساسية لرقابة القطاع العام*. 2019.

المنظمة الدولية للأجهزة العليا للرقابة المالية والمحاسبة. *المعايير الدولية للأجهزة العليا للرقابة المالية 200 (ISSAI): المبادئ الأساسية للرقابة المالية*. 2019.

المنظمة الدولية للأجهزة العليا للرقابة المالية والمحاسبة. *المعايير الدولية للأجهزة العليا للرقابة المالية 300 (ISSAI): المبادئ الأساسية لرقابة الأداء*. 2019.

المنظمة الدولية للأجهزة العليا للرقابة المالية والمحاسبة. *المعايير الدولية للأجهزة العليا للرقابة المالية 400 (ISSAI): المبادئ الأساسية لرقابة الامتثال*. 2019.

المنظمة الدولية للأجهزة العليا للرقابة المالية والمحاسبة. *GUID 5100: إرشادات بشأن تدقيق نظم المعلومات*. 2019.

إيساكا. *دليل مراجعة CISA*، الطبعة 27.

إيساكا. *إطار عمل COBIT 2019: أهداف الحوكمة والإدارة*. *https://www.isaca.org/resources/cobit*. تشرين الثاني (نوفمبر) 2018.

إيساكا. *إطار تدقيق تقنية المعلومات (ITAF): إطار الممارسات المهنية لتدقيق تقنية المعلومات*، الطبعة الرابعة. 22 أكتوبر 2020.

مكتب محاسبة الحكومة الأمريكية. *دليل تدقيق ضوابط نظام المعلومات الفيدرالي* (FISCAM). https://www.gao.gov/products/gao-09-232g. 2 فبراير 2009.

الفصل 2: حوكمة تقنية المعلومات والإدارة

1. ما هي حوكمة تقنية المعلومات وإدارتها؟

يمكن اعتبار حوكمة تقنية المعلومات بمثابة الإطار العام الذي يوجه عمليات تقنية المعلومات في أي مؤسسة للتأكد من أنها تلبي احتياجات العمل الحالية وأنها تتضمن خططًا للاحتياجات والنمو في المستقبل. إنه جزء لا يتجزأ من حوكمة المؤسسة ويتألف من القيادة التنظيمية، والهياكل والعمليات المؤسسية، والآليات الأخرى (على سبيل المثال، إعداد التقارير والتعليقات، والإنفاذ، والموارد) التي تضمن أن أنظمة تقنية المعلومات تحافظ على الأهداف والاستراتيجيات التنظيمية مع موازنة المخاطر والإدارة الفاعلة مصادر.

من المهم أن نفهم أنه وفقًا لإطار عمل COBIT الخاص بـISACA، ثمة تمييز واضح بين الحوكمة والإدارة:[38]

- تضمن **الحوكمة** تقييم احتياجات أصحاب المصلحة وشروطهم وخياراتهم لتحديد أهداف المؤسسة المتوازنة والمتفق عليها؛ يتم تحديد الاتجاه من خلال تحديد الأولويات واتخاذ القرار: ويتم مراقبة الأداء والامتثال مقابل الاتجاه والأهداف المتفق عليها.
- تخطط **الإدارة** وتبني وتدير وتراقب الأنشطة بما يتماشى مع الاتجاه الذي تحدده هيئة الحوكمة لتحقيق أهداف المؤسسة.

تلعب حوكمة تقنية المعلومات دورًا رئيسيًا في تحديد بيئة الرقابة وتضع الأساس لإنشاء ممارسات رقابة داخلية سليمة وإعداد التقارير على المستويات الوظيفية للإشراف الإداري والمراجعة. من الأهمية بمكان ضمان ذلك

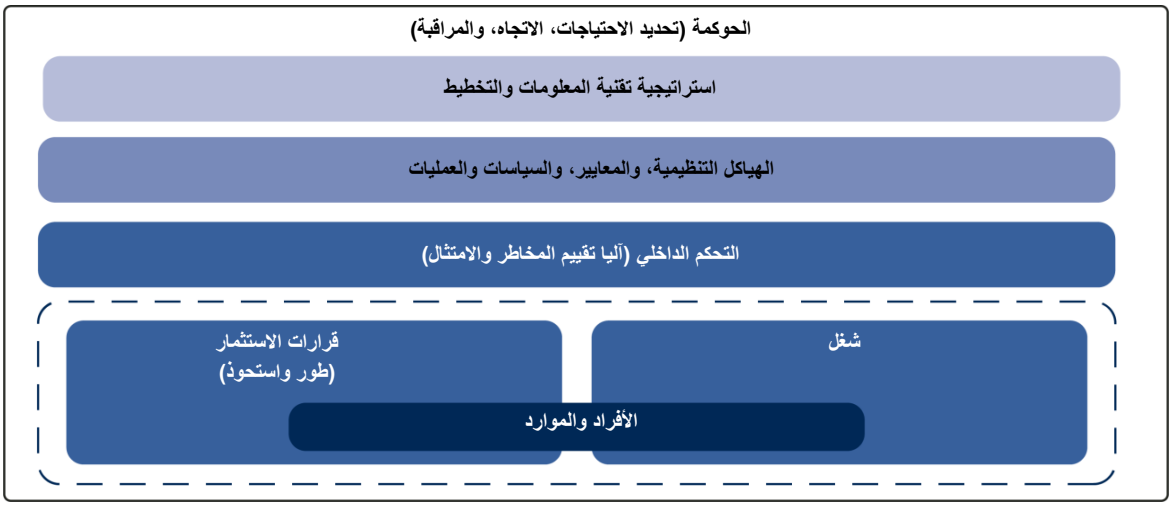
- يتم تقييم احتياجات أصحاب المصلحة والشروط والخيارات لتحديد أهداف الشركة المتوازنة المتفق عليها؛
- يتم تحديد الاتجاه من خلال تحديد الأولويات واتخاذ القرار؛ و
- يتم مراقبة الأداء والامتثال مقابل التوجهات والأهداف المتفق عليها.

في العديد من المنظمات، تقع مسؤولية الحوكمة على عاتق مجلس الإدارة، تحت قيادة الرئيس. قد يتم تفويض مسؤوليات حوكمة محددة إلى هياكل تنظيمية خاصة على مستوى مناسب، لا سيما في المؤسسات الأكبر والمعقدة.

يتم تمثيل إطار حوكمة تقنية المعلومات العام في الشكل 7.

[38] برجاء مراجعة *القسم الرابع: المراجع ومزيد من القراءة* لهذا الفصل ل مراجع وموارد إضافية تتعلق بأفضل ممارسات وأطر إدارة وإدارة تقنية المعلومات.

شكل7 : إطار حوكمة تقنية المعلومات العام



المصدر: مجهول.

أ. تحديد الاحتياجات والتوجيه والمراقبة

تعد حوكمة تقنية المعلومات مكونًا رئيسيًا في الحوكمة الشاملة للشركات. يجب أن يُنظر إلى حوكمة تقنية المعلومات على أنها الطريقة التي تخلق بها تقنية المعلومات قيمة تتناسب مع استراتيجية حوكمة الشركة الشاملة للمؤسسة ولا يُنظر إليها أبدًا على أنها تخصص بحد ذاتها. عند اتباع هذا النهج، سيُطلب من جميع أصحاب المصلحة المشاركة في عملية صنع قرار حوكمة تقنية المعلومات. هذا يخلق قبولًا مشتركًا للمسؤولية عن الأنظمة الهامة ويضمن اتخاذ القرارات المتعلقة بتقنية المعلومات ودفعها حسب احتياجات العمل.

لكي تضمن حوكمة تقنية المعلومات أن الاستثمارات في تقنية المعلومات تولد قيمة تجارية، وأن يتم التخفيف من المخاطر المرتبطة بتقنية المعلومات، فمن الضروري وضع هيكل تنظيمي بأدوار محددة جيدًا لمسؤولية المعلومات والعمليات التجارية والتطبيقات والبنية التحتية في المكان.

يقوم مجلس الإدارة بتقييم الخيارات الاستراتيجية، وتوجيه الإدارة العليا بشأن الخيارات الاستراتيجية المختارة، ومراقبة الإنجازات. عناوين الإدارة

- التنظيم الشامل والاستراتيجية والأنشطة الداعمة لتقنية المعلومات؛
- تحديد واقتناء وتنفيذ حلول تقنية المعلومات ودمجها في العمليات التجارية؛
- التسليم التشغيلي ودعم خدمات تقنية المعلومات، بما في ذلك الأمن؛ و
- مراقبة الأداء ومطابقة تقنية المعلومات مع أهداف الأداء الداخلية وأهداف الرقابة الداخلية والمتطلبات الخارجية.

من الضروري أيضًا إشراك حوكمة تقنية المعلومات في العملية لتحديد احتياجات العمل الجديدة أو المحدثة ثم توفير حلول تقنية المعلومات المناسبة (وغيرها) لمستخدم الأعمال. أثناء تطوير أو الحصول على الحل لاحتياجات العمل، تضمن حوكمة تقنية المعلومات أن الحلول المختارة تستجيب للعمل وأن التدريب والموارد اللازمة (مثل الأجهزة والأدوات وقدرة الشبكة) متاحة لتنفيذ الحل. يمكن تنفيذ أنشطة المراقبة من قبل فريق المراجعة الداخلي أو مجموعة ضمان الجودة، والتي تقدم تقارير دورية عن نتائجها إلى الإدارة.

ثانيًا. العناصر الرئيسة لحوكمة وإدارة تقنية المعلومات[39]

أ. استراتيجية تقنية المعلومات والتخطيط

تمثل استراتيجية تقنية المعلومات المواءمة المتبادلة بين استراتيجية تقنية المعلومات والأهداف الاستراتيجية للأعمال. يجب أن تراعي الأهداف الاستراتيجية لتقنية المعلومات

[39] العناصر الرئيسة الواردة في فصل حوكمة تقنية المعلومات هذا مدعومة من قبل *COBIT 5 Framework* و *COBIT 2019* و *ISO 38500* مع الاستخدام المكثف لتعريفاتهم وأمثلتهم.

الاحتياجات الحالية والمستقبلية للأعمال، وقدرة تقنية المعلومات الحالية على تقديم الخدمات، ومتطلبات الموارد.[40] يجب أن تأخذ الاستراتيجية بعين الاعتبار البنية التحتية وتقنية المعلومات الحالية، والاستثمارات، ونموذج التسليم، والموارد بما في ذلك التوظيف، ووضع خطة تدمجها في نهج مشترك لدعم أهداف العمل.

من المهم لمدقق تقنية المعلومات مراجعة استراتيجية تقنية المعلومات الخاصة بالمنظمة ليس فقط لاكتساب فهم كافٍ للمؤسسة غير أنه أيضًا بغية تقييم المدى الذي كانت فيه حوكمة تقنية المعلومات جزءًا من عملية صنع القرار في الشركة.

بدون استراتيجية تقنية المعلومات، ثمة خطر متزايد يتمثل في عدم تحديد المؤسسات لكيفية تلبية تقنية المعلومات لاحتياجات العمل الحالية والمستقبلية للمؤسسة. وعلاوة على ذلك، بدون خطة استراتيجية محدثة لتقنية المعلومات - مرتبطة بالخطة الاستراتيجية الشاملة للمؤسسة والتي تتضمن الأهداف ومقاييس الأداء والاستراتيجيات والترابط بين المشاريع - تخاطر المؤسسات بالافتقار إلى تعريف واضح لما تريد تحقيقه باستخدام تقنية المعلومات والاستراتيجيات لتحقيق تلك النتائج.

ب. الهياكل التنظيمية والمعايير والسياسات والعمليات

تعتبر الهياكل التنظيمية عنصرًا رئيسيًا في حوكمة تقنية المعلومات في توضيح أدوار مختلف هيئات الإدارة والحوكمة عبر الأعمال وصنع القرار. يجب عليهم تعيين تفويضات محددة بوضوح لاتخاذ القرار ومراقبة الأداء. يجب دعم الهياكل التنظيمية بالمعايير والسياسات والإجراءات المناسبة، والتي ينبغي أن تعزز القدرة على صنع القرار.

تتأثر الهياكل التنظيمية في مؤسسة القطاع العام **بأصحاب المصلحة** (أي جميع المجموعات أو المنظمات أو الأعضاء أو الأنظمة التي تؤثر أو يمكن أن تتأثر بإجراءات المنظمة). تشمل الأمثلة على أصحاب المصلحة الخارجيين المهمين البرلمان والكونغرس و / أو الكيانات الحكومية الأخرى والمواطنين. تتأثر الهياكل التنظيمية أيضًا **بالمستخدمين**، الداخليين والخارجيين.

المستخدمون الداخليون هم مديرو الأعمال والأقسام الوظيفية الذين يمتلكون العمليات التجارية، والأفراد داخل المنظمة الذين يتفاعلون مع العمليات التجارية. المستخدمون الخارجيون هم الوكالات والأفراد والجمهور الذين يستخدمون المنتجات أو الخدمات التي تقدمها منظمة (على سبيل المثال، الإدارات الأخرى والمواطنون). ثمة تأثير آخر على الهياكل التنظيمية يتمثل في **مقدمي الخدمة**: شركة أو وحدة أو شخص، خارجيًا وداخليًا، يقدم خدمة.

تظهر الحاجة إلى وظائف تقنية المعلومات من المستخدمين وأصحاب المصلحة. في جميع الحالات، يجب أن يتم تفويض الهياكل التنظيمية والأدوار والمسؤوليات التنظيمية المناسبة للحوكمة من هيئة الإدارة، مما يوفر ملكية واضحة ومساءلة للقرارات والمهام الهامة. يجب أن يشمل ذلك العلاقات مع موفري خدمات تقنية المعلومات الأساسيين من الأطراف الثالثة.[41]

يشتمل الهيكل التنظيمي لتقنية المعلومات عادةً على **لجنة توجيهية لتقنية المعلومات**، وهي الجزء المركزي من الهيكل التنظيمي. تتألف اللجنة التوجيهية لتقنية المعلومات من أعضاء من الإدارة العليا والعليا وتتحمل مسؤولية مراجعة وتأييد وتخصيص الأموال لاستثمارات تقنية المعلومات بالإضافة إلى ضمان تحقيق الأهداف والغايات الرئيسة المخصصة للمؤسسة. يجب أن تكون اللجنة التوجيهية مفيدة في استنباط قرارات الأعمال التي يجب توفير التقنية لها لدعم الاستثمارات التجارية وكذلك الموافقة على كيفية الحصول على هذه التقنية. عادة ما تكون قرارات الاستثمار التي تتضمن حلول "البناء مقابل الشراء" من مسؤولية اللجنة التوجيهية لتقنية المعلومات بشكل عام بعد التوصيات المناسبة من المجموعات أو اللجان المعينة.

تلعب اللجنة التوجيهية دورًا حاسمًا في تعزيز القبول الضروري وتقديم الدعم الإداري للبرامج التي تنطوي على تغييرات في المنظمة. في العديد من مؤسسات القطاع العام، تعتبر وظائف اللجنة التوجيهية لتقنية المعلومات جزءًا من وظيفة الإدارة. من المهم ملاحظة أن حوكمة تقنية المعلومات معقدة ومتعددة الأوجه. تخدم الهياكل الإدارية المختلفة مثل اللجنة التوجيهية أغراضًا مختلفة وتتميز بأدوار ومسؤوليات مختلفة بناءً على مجموعة متنوعة من العوامل، بما في ذلك الاحتياجات التنظيمية والقطاع التنظيمي والبيئة التنظيمية. على الرغم من أن الأدوار والمسؤوليات الرئيسة التي تشكل وظيفة الإدارة يمكن أن تختلف باختلاف البلدان والقطاعات (على سبيل المثال، مؤسسات القطاع العام مقابل مؤسسات القطاع الخاص)، تشمل الأمثلة ما يلي:

- **الرئيس التنفيذي** هو أكبر مسؤول مسؤول عن الإدارة الكلية للمنظمة.
- **المدير المالي** هو أكبر مسؤول مسؤول عن جميع جوانب الإدارة المالية، بما في ذلك المخاطر المالية والضوابط.
- **مدير العمليات** هو أكبر مسؤول مسؤول عن عمل المنظمة.

---

[40] المنظمة الدولية للتوحيد القياسي *ISO 38500*.

[41] إيساكا، *COBIT 2019*.

- **رئيس إدارة المخاطر** هو أكبر مسؤول مسؤول عن إدارة المخاطر عبر المؤسسة. قد يكون لرئيس إدارة المخاطر وظائف مخاطر تقنية المعلومات للإشراف على المخاطر المتعلقة بتقنية المعلومات.
- **كبير مسؤولي الخصوصية** هو شخص كبير مسؤول عن مراقبة المخاطر وتأثيرات الأعمال لقوانين الخصوصية، وتوجيه وتنسيق تنفيذ السياسات والأنشطة التي تضمن تلبية توجهات الخصوصية.
- **رئيس قسم المعلومات** هو شخص كبير مسؤول عن إدارة وتشغيل قدرات تقنية المعلومات الخاصة بالمؤسسة. في العديد من مؤسسات القطاع العام، قد يتم تنفيذ المهام التي يؤديها كبير مسؤولي المعلومات من قبل مجموعة أو إدارة لديها المسؤوليات والسلطات والموارد اللازمة.
- **كبير مسؤولي التقنية** هو شخص كبير قد تشمل مسؤولياته، على سبيل المثال، ضمان أن استخدام المنظمة للتقنية يتسم بالكفاءة والفعالية، ودمج أفضل الممارسات والإجراءات في تنفيذ قدرات تقنية المعلومات، وتوفير الخبرة اللازمة لاعتماد التقنيات الناشئة في منظمة.
- **كبير مسؤولي أمن المعلومات** هو أكبر مسؤول مسؤول عن أمن جميع أشكال معلومات المؤسسة.
- **كبير موظفي الموارد البشرية** هو أكبر مسؤول مسؤول عن مواءمة سياسات وإجراءات الموارد البشرية مع المهمة التنظيمية والأهداف الاستراتيجية.
- **رئيس قسم المعرفة** هو أكبر مسؤول مسؤول عن إدارة جميع أشكال المعرفة داخل المؤسسة.

بدون هيكل تنظيمي محدد جيدًا، بما في ذلك لجنة توجيهية لتقنية المعلومات، قد تفتقر المؤسسات إلى كيان مسؤول عن اتخاذ قرارات العمل التي يجب توفير التقنية لها لدعم استثمارات الأعمال وكذلك الموافقة على كيفية الحصول على هذه التقنية. وعلاوة على ذلك، قد تفتقر المنظمات إلى الدعم الإداري اللازم للبرامج. ونتيجة لذلك، قد تحدث هذه الأنشطة بطريقة غير متسقة وغير منظمة وقد لا تؤدي إلى تحقيق قيمة مقابل المال أو عدم تحقيق أهداف البرنامج أو الاستثمار.

ج. المعايير والسياسات والعمليات

يتم اعتماد المعايير والسياسات من قبل المنظمة والموافقة عليها من قبل الإدارة العليا. تضع السياسات إطارًا عالي المستوى للعمليات اليومية من أجل تلبية الأهداف التي حددها مجلس الإدارة. تحدد المعايير تدابير قابلة للقياس من أجل تلبية السياسات. يتم دعم المعايير والسياسات من خلال العمليات التي تحدد كيفية إنجاز العمل أو التدابير والتحكم فيها. يتم تحديد هذه الأهداف من قبل الإدارة العليا لإنجاز مهمة المنظمة وفي نفس الوقت للامتثال للمتطلبات التنظيمية والقانونية.

المعايير والسياسات والعمليات المقابلة تحتاج إلى المراجعة والتعديل على أساس منتظم وتحتاج إلى إبلاغ جميع المستخدمين المعنيين في المنظمة بشكل دوري. يحتاج موظفو قسم تقنية المعلومات أيضًا إلى التدريب على كيفية تطبيق واستخدام هذه السياسات والمعايير والعمليات في عملياتهم اليومية. يجب أن تعكس السياسات والمعايير والعمليات المقابلة التحديثات على التقنية والتهديدات الجديدة، والتغييرات المهمة في العمليات، والبيئة الجديدة والمتطلبات التنظيمية. عادة ما تكون معايير المنظمة هي التي سيستخدمها تدقيق تقنية المعلومات كموضوع لها، حيث يمكن مراجعة هذه التدابير على أساسها.

السياسات والعمليات المقابلة تحتاج إلى مراجعة وتعديل حسب الحاجة. يجب إبلاغ جميع المستخدمين المعنيين في المنظمة على أساس دوري. يجب أن تعكس السياسات التحديثات على التقنية الجديدة والتهديدات والتغييرات المهمة في العمليات والبيئة والمتطلبات التنظيمية. تتضمن بعض السياسات الرئيسة التي توجه حوكمة تقنية المعلومات ما يلي:

- **سياسة الموارد البشرية:** تتعامل سياسة الموارد البشرية مع التوظيف والتدريب وإنهاء الوظيفة وغيرها من وظائف المنظمة. إنه يتعامل مع أدوار ومسؤوليات مختلف الموظفين داخل المنظمة بالإضافة إلى المهارات أو التدريب المطلوب منهم امتلاكه لأداء واجباتهم. قد تحدد سياسة الموارد البشرية أيضًا الأدوار والمسؤوليات والفصل بين الواجبات. ومع ذلك، يمكن أيضًا تفويض هذه الوظيفة إلى قسم مخصص في المؤسسات الكبيرة والمعقدة.
- **سياسات الاحتفاظ بالوثائق والمستندات:** يعد توثيق أنظمة المعلومات والتطبيقات والأدوار الوظيفية وأنظمة إعداد التقارير والوتيرة نقطة مرجعية مهمة لمواءمة عمليات تقنية المعلومات مع أهداف العمل. تمكّن سياسات الاحتفاظ بالوثائق المناسبة من تتبع وإدارة التغييرات التكرارية لهندسة المعلومات في المؤسسة.
- **سياسة الاستعانة بمصادر خارجية:** غالبًا ما تهدف التعهيد الخارجي لتقنية المعلومات إلى السماح لإدارة المنظمة بتركيز جهودها على أنشطة الأعمال الأساسية. قد تكون الحاجة إلى الاستعانة بمصادر خارجية مدفوعة أيضًا بالحاجة إلى تقليل تكاليف التشغيل. تضمن سياسة الاستعانة بمصادر خارجية تطوير وتنفيذ مقترحات عمليات الاستعانة بمصادر خارجية ووظائفها بطريقة تعود بالفائدة على المنظمة. أحد الأمثلة الأكثر شيوعًا لخدمات تقنية المعلومات التي يتم الاستعانة بمصادر خارجية لها اليوم هو الحوسبة السحابية، والتي تتيح الوصول إلى الشبكة عند الطلب لمجموعة من موارد الحوسبة القابلة للتكوين (على سبيل المثال، الشبكات والخوادم والتخزين والخدمات الأخرى). لُطفًا راجع الفصل 5 لمزيد من المعلومات بخصوص الاستعانة بمصادر خارجية والحوسبة السحابية.
- **سياسة العمل عن بعد:** يجب على المنظمات وضع سياسات وإرشادات العمل عن بعد للتأكد من أن القوى العاملة لديها جاهزة للعمل عن بعد. تتمثل إحدى الممارسات الرئيسة لتسهيل العمل عن بُعد في إنشاء اتفاقيات عمل مكتوبة عن بُعد لاستخدامها بين الموظفين والمديرين. يجب أن تحدد اتفاقيات العمل عن بُعد ترتيبات العمل المحددة بين المدير والموظف قبل أن يبدأ الموظف العمل عن بُعد، ويجب أن تحدد واجبات وتوقعات الوظيفة، ومعايير الأداء، والنتائج القابلة للقياس والتسليمات.

- **سياسة أمن وخصوصية تقنية المعلومات:** تحدد هذه السياسة متطلبات حماية أصول المعلومات، وقد تشير إلى إجراءات أو أدوات أخرى بخصوص كيفية حمايتها. يجب أن تكون السياسة متاحة لجميع الموظفين المسؤولين عن أمن المعلومات، بما في ذلك مستخدمي أنظمة الأعمال الذين لهم دور في حماية المعلومات (أي سجلات الموظفين وبيانات الإسهامات المالية). برجاء مراجعة الفصل 7 لمزيدٍ من المعلومات بخصوص أمن تقنية المعلومات وسياسة الخصوصية.
- **سياسة إدارة البيانات:** تقوم المنظمات بجمع البيانات من العديد من الموارد، مثل أنظمة المعاملات والماسحات الضوئية وأجهزة الاستشعار والوسائط الاجتماعية والأجهزة الذكية وغيرها. لذلك، تحتاج المؤسسات إلى تحديد السياسات والإجراءات الخاصة بكيفية إدارة البيانات طوال دورة الحياة، مثل جمع البيانات وتخزينها وأمانها والتخلص منها. لُطفًا راجع الفصل 4 لمزيد من المعلومات بخصوص إدارة البيانات.

المنظمات التي تفتقر إلى سياسات ومعايير للعمليات اليومية معرضة بشكل متزايد لخطر عدم تحقيق الأهداف المتعلقة بتقنية المعلومات. على سبيل المثال، تعتبر سياسة الموارد البشرية مهمة لإدارة التوظيف والتدريب، وسياسة أمن تقنية المعلومات مهمة لضمان حماية أصول المعلومات.

د. التحكم الداخلي

كما ذكرنا سابقًا، فإن الرقابة الداخلية هي عملية إدخال وتنفيذ نظام من التدابير والإجراءات لتحديد ما إذا كانت أنشطة المنظمة وما زالت متوافقة مع السياسات والمعايير والخطط المعتمدة. إذا لزم الأمر، يتم اتخاذ التدابير التصحيحية اللازمة حتى يمكن تحقيق أهداف السياسة.

تحافظ الرقابة الداخلية على نظام تقنية المعلومات في مساره الصحيح. تشمل الضوابط الداخلية إدارة المخاطر والامتثال للإجراءات والتعليمات الداخلية والتشريعات واللوائح الخارجية؛ تقارير إدارية دورية ومخصصة؛ فحوصات التقدم ومراجعة الخطط والمراجعات والتقييمات والمراقبة.[42]

بدون الضوابط الداخلية، تواجه المؤسسات خطرًا متزايدًا يتمثل في عدم امتثال أنظمة تقنية المعلومات للسياسات والمعايير والقوانين واللوائح الداخلية.

7. إدارة المخاطر

يجب أن تشكل إدارة مخاطر تقنية المعلومات جزءًا لا يتجزأ من استراتيجية وسياسات إدارة المخاطر في الشركة. تتضمن إدارة المخاطر تحديد المخاطر المتعلقة بالتطبيقات الحالية والبنية التحتية لتقنية المعلومات، والإدارة المستمرة، بما في ذلك المراجعة الدورية والتحديث من قبل إدارة المخاطر ومراقبة استراتيجيات التخفيف. يجب أن تكون إدارة مخاطر تقنية المعلومات جزءًا من إدارة المخاطر الشاملة داخل المؤسسة.

يساعد تطوير خطة إدارة المخاطر على تسهيل عملية إدارة المخاطر. تعمل الخطة على توثيق عملية تحديد وتقييم المخاطر. كما يوثق العمليات والأدوات والإجراءات المستخدمة لإدارة المخاطر والتحكم فيها في جميع مراحل المشروع. لُطفًا راجع الفصل 3 بشأن تطوير تقنية المعلومات واكتسابها لمزيد من المعلومات بخصوص إدارة المخاطر.

8. آلية الامتثال

تحتاج المنظمات إلى آلية امتثال تضمن اتباع جميع السياسات والمعايير والإجراءات المرتبطة بها. من المهم إنشاء ثقافة تنظيمية حيث يفهم الموظفون تأثير عدم الامتثال للسياسات والمعايير والإجراءات المذكورة. قد تشمل آلية دعم الامتثال أيضًا مجموعة ضمان الجودة وموظفي الأمن والأدوات الآلية. يجب مراجعة تقرير عدم الامتثال من قبل الإدارة المناسبة والتعامل مع قضايا عدم الامتثال الجادة أو المتكررة. قد تختار الإدارة التعامل مع عدم الامتثال للتدريب التنشيطي أو الإجراءات المعدلة أو حتى إجراءات العقاب المتصاعدة اعتمادًا على طبيعة عدم الامتثال (على سبيل المثال، الانتهاكات الأمنية والتدريب الإلزامي المفقود).

يمكن أن يوفر الضمان المستقل، في شكل عمليات تدقيق داخلية أو خارجية (أو مراجعات)، ملاحظات في الوقت المناسب بخصوص امتثال تقنية المعلومات لسياسات المنظمة ومعاييرها وإجراءاتها وأهدافها العامة. يجب إجراء عمليات المراجعة هذه بطريقة غير متحيزة وموضوعية حتى يتم تزويد المديرين بتقييم عادل لمشروع تقنية المعلومات الذي يتم تدقيقه.

بدون وجود آلية امتثال، قد تفتقر المنظمات إلى ضمان موثوق بأن العملية ومنتجات العمل المختارة يتم تنفيذها كما هو مخطط لها وتلتزم بوصف العملية والمعايير والإجراءات.

هـ. قرارات الاستثمار

[42] حوكمة تقنية المعلومات في القطاع العام: أولوية قصوى، "*WGITA IntoIT*"، العدد رقم. 25، (أغسطس 2007).

يجب أن تزود حوكمة تقنية المعلومات مستخدمي الأعمال بحلول لمتطلباتهم الجديدة أو المعدلة. يمكن تحقيق ذلك من قبل قسم تقنية المعلومات من خلال قرارات الاستثمار إما لتطوير (بناء) برامج أو أنظمة جديدة أو الحصول عليها من البائعين على أساس فعال من حيث التكلفة. من أجل اتخاذ قرارات استثمارية ناجحة، تتطلب أفضل الممارسات عادةً اتباع نهج منضبط حيث يتم تحديد المتطلبات وتحليلها وترتيبها حسب الأولوية والموافقة عليها؛ تحليل التكلفة والعائد الذي يتم إجراؤه بين الحلول المتنافسة؛ والحل الأمثل المحدد (على سبيل المثال، الحل الذي يوازن بين التكلفة والمخاطر ويلبي عددًا كبيرًا من أهداف المنظمة).

يعد تطوير دراسة الجدوى وتحديد احتياجات المستخدم وإبراز فرص وفوائد الحل أداة قيمة لتوجيه قرارات الاستثمار. يمكن أن تبدأ دراسة الجدوى كاستراتيجية عالية المستوى وتتطور إلى وصف تفصيلي للمهام الرئيسة والمعالم والمسؤوليات والأدوار. تُعد دراسة الجدوى بمثابة أداة ديناميكية تتطلب تحديثات مستمرة لتعكس الوضع الحالي والنظر في مستقبل المبادرة. لُطفًا راجع الفصل 3 لمزيد من المعلومات بخصوص تطوير تقنية المعلومات واكتسابها.

و. عمليات تقنية المعلومات

عمليات تقنية المعلومات هي عادة التشغيل اليومي للبنية التحتية لتقنية المعلومات لدعم احتياجات العمل. تتيح عمليات تقنية المعلومات المُدارة بشكل صحيح تحديد الاختناقات والتخطيط للتغييرات المتوقعة في السعة (على سبيل المثال، موارد إضافية للأجهزة أو الشبكة)، وقياس الأداء للتأكد من أنه يلبي الاحتياجات المتفق عليها لأصحاب الأعمال، وتوفير مكتب المساعدة ودعم إدارة الحوادث لمستخدمي موارد تقنية المعلومات. لُطفًا راجع الفصل 4 لمزيد من المعلومات بخصوص عمليات تقنية المعلومات.

ز. الناس والموارد

يوصى بأن تضمن الإدارة من خلال التقييمات المنتظمة تخصيص موارد كافية لتقنية المعلومات لتلبية احتياجات المنظمة، وفقًا للأولويات المتفق عليها وقيود الميزانية. علاوة على ذلك، يجب احترام الجانب الإنساني من خلال السياسات والممارسات وقرارات تقنية المعلومات، والتي يجب أن تأخذ في الاعتبار الاحتياجات الحالية والمستقبلية للمشاركين في العملية. يجب أن تقيّم إدارة الحوكمة بانتظام ما إذا كان يتم استخدام الموارد وتحديد أولوياتها حسب متطلبات أهداف العمل.

يمكن للمؤسسات الاستفادة من إدارة القوى العاملة في مجال تقنية المعلومات والتخطيط الذي يتناول التخطيط الاستراتيجي، ويضمن تلبية كفاءات تقنية المعلومات واحتياجات التوظيف، ويتضمن ممارسات التوظيف والتوظيف، والتدريب وتطوير القوى العاملة، وإدارة الأداء. تشمل العناصر الرئيسة للتخطيط السليم للقوى العاملة

- إنشاء والحفاظ على عملية تخطيط القوى العاملة،
- تطوير الكفاءة ومتطلبات الموظفين،
- تقييم الكفاءة واحتياجات التوظيف بانتظام،
- تقييم الثغرات في الكفاءات والتوظيف،
- وضع استراتيجيات وخطط لمعالجة الفجوات في الكفاءات والتوظيف،
- تنفيذ الإجراءات لمعالجة الثغرات، ورصد التقدم المحرز في معالجة الثغرات، و
- رفع التقارير إلى القيادة بشأن التقدم المحرز في معالجة الثغرات.

ثالثا. المخاطر على الهيئة الخاضعة للرقابة

يحتاج المدققون إلى فهم وتقييم المكونات المختلفة لهيكل حوكمة تقنية المعلومات لتحديد ما إذا كانت قرارات تقنية المعلومات والتوجيهات والموارد والإدارة والمراقبة تدعم استراتيجيات وأهداف المنظمة. لإجراء التقييم، يحتاج المدققون إلى معرفة المكونات الرئيسة لحوكمة تقنية المعلومات وإدارتها، بالإضافة إلى المخاطر المرتبطة بعدم كفاية كل مكون في الكيان.

تتطلب المراقبة والتحليل والتقييم المستمر للمقاييس المرتبطة بمبادرات حوكمة تقنية المعلومات رؤية مستقلة ومتوازنة لتسهيل تحسين عمليات تقنية المعلومات. يلعب المراجعة دورًا مهمًا في التنفيذ الناجح لحوكمة تقنية المعلومات من خلال تقديم توصيات في التخفيف من المخاطر المرتبطة بالجوانب التالية لحوكمة تقنية المعلومات وإدارتها:

- مواءمة وظيفة تقنية المعلومات مع مهمة المنظمة ورؤيتها وقيمها وأهدافها واستراتيجياتها؛
- تحقيق أهداف الأداء التي وضعتها المنظمة ووظيفة تقنية المعلومات؛
- المتطلبات القانونية والبيئية والمتعلقة بجودة المعلومات والائتمانية والأمن والخصوصية؛
- البيئة الرقابية للمنظمة؛

- المخاطر الكامنة في بيئة أمن المعلومات؛ و
- استثمار / نفقات تقنية المعلومات.

تواجه كل منظمة تحدياتها الفريدة حيث تختلف القضايا البيئية والسياسية والجغرافية والاقتصادية والاجتماعية الفردية الخاصة بها. على الرغم من أن هذه ليست قائمة شاملة، إلا أن النتائج المعروضة أدناه تمثل مخاطر شائعة قد تنجم عن عدم وجود إدارة مناسبة لتقنية المعلومات.

أ. أنظمة تقنية المعلومات غير الفاعلة وغير الفاعلة

غالبًا ما تكون أنظمة الإدارة العامة التي تهدف إلى خدمة المجتمع أو الأعمال التجارية أو تعزيز وظائف الوكالات الحكومية حلولًا معقدة وواسعة النطاق. وبالتالي، يجب أن تكون مصممة بشكل صحيح، ومصممة خصيصًا للاحتياجات الحقيقية للمؤسسة، ومنسقة بكفاءة، وتشغيلها بكفاءة. قد يؤدي الافتقار إلى ملكية الأعمال على العمليات والتطبيقات والبيانات إلى سوء إدارة تقنية المعلومات. يمكن أن يكون ضعف إدارة تقنية المعلومات على المستوى الحكومي وعلى مستوى المؤسسة أول عقبة أمام وجود أنظمة تقنية معلومات جيدة الجودة.

ب. تصور أن تقنية المعلومات تقدم مساهمة منخفضة في قيمة الأعمال

قد يتم اشتقاق قيمة تجارية قليلة أو معدومة من استثمارات تقنية المعلومات الرئيسة التي لا تتوافق استراتيجيًا مع أهداف المنظمة ومواردها. يعني هذا التوافق الاستراتيجي الضعيف أنه حتى تقنية المعلومات ذات الجودة العالية قد لا تساهم بكفاءة وفعالية في تحقيق الأهداف العامة للمؤسسة. تتمثل إحدى طرق ضمان التوافق في إشراك المستخدمين وأصحاب المصلحة الآخرين الذين يفهمون الأعمال في اتخاذ قرارات تقنية المعلومات. يمكن لأصحاب المصلحة هؤلاء المساهمة في تطوير دراسة الجدوى لضمان التوافق مع أهداف المنظمة ومواردها.

ج. عدم مشاركة قسم تقنية المعلومات في المؤسسة

توصلت الأبحاث إلى أن المؤسسات الرائدة تتبنى وتستخدم نهجًا على مستوى المؤسسة لإدارة تقنية المعلومات يتضمن، من بين أشياء أخرى

- المسؤولية عن "سلعة تقنية المعلومات:" أي أشياء مثل خدمات البريد الإلكتروني وخدمات مكتب المساعدة والحصول على الأجهزة والبرامج؛
- الإشراف على الأنظمة الخاصة بالبعثات؛ و
- مسؤوليات واضحة بين قسم تقنية المعلومات في المؤسسة وأي وحدات أو مكونات أعمال.

بدون سلطة ورقابة مركزية، قللت المنظمة من التأكيد على أن الاستثمارات في تقنية المعلومات يتم تنسيقها على مستوى المنظمة وأنها توفر مزيجًا مناسبًا من القدرات التي تدعم احتياجات المهمة مع تجنب الازدواجية غير الضرورية.

د. التعرض لأمن المعلومات ومخاطر الخصوصية

إن المنظمة التي ليس لديها ضوابط وهياكل وعمليات وسياسات مناسبة لأمن المعلومات معرضة بشكل أكبر لخطر حوادث وانتهاكات أمن المعلومات والخصوصية. وتشمل هذه المخاطر، من بين أمور أخرى، اختلاس الأصول؛ الكشف غير المصرح به عن المعلومات؛ الوصول غير المصرح به وقابلية التعرض للهجمات المنطقية والمادية، والهجمات الإلكترونية، والتعطيل وعدم توفر المعلومات، وسوء استخدام المعلومات، وعدم الامتثال لقوانين وأنظمة البيانات الشخصية، وعدم التعافي من الكوارث. يجب أن تحدد سياسة أمن تقنية المعلومات الأصول التنظيمية (أي البيانات والمعدات والعمليات التجارية) التي تحتاج إلى الحماية والارتباط بالإجراءات والأدوات وضوابط الوصول المادي التي تحمي هذه الأصول.

يجب أن تتضمن هياكل الحوكمة على المستوى التنفيذي للمؤسسة سياسات وإجراءات وعمليات لإدارة ومراقبة أمن معلومات المنظمة وحماية الخصوصية. يجب أن توضح هذه الوثائق أولويات المهمة والموارد المتاحة والتسامح العام لمخاطر أمن المعلومات. يجب أن يكون لدى المنظمة أيضًا عملية قائمة لدعم الامتثال لأنشطة أمن المعلومات مع قوانين ولوائح وإرشادات أمن المعلومات والخصوصية المعمول بها. من بين أمور أخرى، يجب على الأفراد المسؤولين عن حماية الأنظمة والبيانات تقديم تقارير إلى الإدارة المناسبة وأن يتم تدريبهم بشكل مناسب.

تم تعريف هياكل إدارة أمن المعلومات بمزيد من التفصيل في مواد مرجعية أخرى، ولا يُقصد بذلك أن تكون قائمة شاملة لهياكل إدارة أمن المعلومات. تشمل المواد المرجعية الأخرى المتعلقة بأمان المعلومات والخصوصية

- إيساكا. *إطار عمل COBIT 2019: أهداف الحوكمة والإدارة*. 2019.

- المنظمة الدولية للتوحيد القياسي / اللجنة الكهروتقنية الدولية. *ISO / IEC 27001:2013 - تقنية المعلومات - تقنيات الأمن - أنظمة إدارة أمن المعلومات - المتطلبات.*
- المعهد الوطني للمعايير والتقنية. *NIST Special Publication* 800-53، *Security and Privacy Controls for Information Systems and Organization*، rev. 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. سبتمبر 2020.
- المعهد الوطني للمعايير والتقنية. *منشور NIST الخاص 800-37، إطار عمل إدارة المخاطر لأنظمة المعلومات والمنظمات: نهج دورة حياة النظام للأمان والخصوصية.* https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final. ديسمبر 2018.

هـ. قيود نمو الأعمال

قد يؤدي عدم كفاية أو نقص تخطيط تقنية المعلومات إلى تقييد نمو الأعمال بسبب نقص موارد تقنية المعلومات أو الاستخدام غيرالفاعل للموارد الحالية. تتمثل إحدى طرق التخفيف من هذه المخاطر في تطوير استراتيجية تقنية المعلومات وتحديثها بشكل دوري، والتي من شأنها تحديد الموارد والخطط لتلبية الاحتياجات المستقبلية للأعمال.

و. إدارة الموارد غير الفاعلة

لتحقيق أفضل النتائج بأقل التكاليف، يجب على المنظمة إدارة موارد تقنية المعلومات الخاصة بها بفعالية وكفاءة. يعد ضمان وجود ما يكفي من الموارد التقنية والأجهزة والبرامج والموارد البشرية مع المعرفة والخبرات المناسبة المتاحة لتقديم خدمات تقنية المعلومات هو العامل الرئيسي في تحقيق قيمة من الاستثمارات في تقنية المعلومات. تحديد ومراقبة استخدام موارد تقنية المعلومات في اتفاقية مستوى الخدمة،[43] على سبيل المثال، يسمح للمؤسسة بمعرفة ما إذا كانت متطلبات الموارد كافية لتلبية احتياجات العمل بشكل موضوعي.

تساعد الاستفادة من تخطيط القوى العاملة لضمان توافر الموظفين ذوي المهارات المناسبة على تحسين إدارة الموارد البشرية. إن استخدام الاستراتيجيات التي تمت مناقشتها سابقًا لتخطيط القوى العاملة سيفيد المنظمة من خلال إنشاء العملية واستخدامها لتحديد احتياجات التوظيف والمهارات الرئيسة واستنباط استراتيجيات لتلبية هذه الاحتياجات.

ز. اتخاذ القرار غير الكافي

قد تؤدي هياكل إعداد التقارير السيئة إلى اتخاذ قرارات غير ملائمة. قد يؤثر ذلك على قدرة المنظمة على تقديم خدماتها وقد يمنعها من تحقيق أهدافها. تساعد اللجان التوجيهية والمجموعات التنظيمية الأخرى ذات التمثيل المناسب في اتخاذ القرارات التي تؤثر على المنظمة.

ح. فشل المشروع

تفشل العديد من المنظمات في النظر إلى أهمية حوكمة تقنية المعلومات. يأخذون في مشاريع تقنية المعلومات دون فهم كامل لمتطلبات المنظمة للمشروع وكيف يرتبط هذا المشروع بأهداف المنظمة. بدون هذا الفهم، تكون مشاريع تقنية المعلومات أكثر عرضة للفشل. ومن الأخطاء الشائعة أيضًا أن التطبيقات المكتسبة أو المطورة لا تفي بالحد الأدنى من معايير الأمان والبنية. قد تتكبد هذه المشاريع تكاليف إضافية لصيانة وإدارة الأنظمة والتطبيقات غير القياسية. **دورة حياة تطوير نظام** محددة (SDLC) واستخدامه في التطوير والاستحواذ هو وسيلة لتقليل مخاطر فشل المشروع. لُطفًا راجع الفصل 3 بخصوص تطوير تقنية المعلومات والحصول عليها لمزيد من المعلومات بخصوص منهجيات SDLC.

i. مشكلات التبعية للطرف الثالث (البائع) أو تقديم الخدمة بواسطة متعهد تقنية المعلومات

إذا لم تتحكم العمليات المناسبة في الاستحواذ وعملية الاستعانة بمصادر خارجية، فقد تواجه المنظمة موقفًا تعتمد فيه تمامًا على بائع أو مقاول واحد. أولاً، هذه بيئة عالية المخاطر لأنه إذا خرج البائع من السوق أو فشل في تقديم الخدمات المتعاقد عليها، فستكون المنظمة في وضع صعب. تشمل المخاطر الأخرى، على سبيل المثال، النزاعات بخصوص الملكية الفكرية والأنظمة وخروقات البيانات الشخصية وقواعد البيانات. قد تحتاج المنظمات التي تستعين بمصادر خارجية أو تتعاقد بانتظام مع البائعين للحصول على حلول إلى سياسة الاستعانة بمصادر خارجية أو الاستحواذ التي تحدد ما قد يتم الاستعانة بمصادر خارجية أو لا. من المهم أيضًا للمؤسسات تحديد وإدارة مخاطر سلسلة التوريد عند تطوير منتجات وخدمات تقنية المعلومات والحصول عليها. لُطفًا راجع الفصل 7 بشأن أمن المعلومات لمزيد من المعلومات بخصوص إدارة سلسلة التوريد.

[43] تحدد اتفاقية مستوى الخدمة المتطلبات والمسؤوليات المحددة لمقدم الخدمة وتضع توقعات العملاء.

سيساعد الإشراف الفاعل على العقود ومراقبتها على معالجة المخاطر المرتبطة بالاعتماد على مورد طرف ثالث. يجب أن تحدد العقود اتفاقيات مستوى الخدمة وحقوق وصول الطرف الثالث. تساعد المراقبة الدقيقة لأداء الطرف الثالث، بما في ذلك تحديثات الحالة المنتظمة والمراجعات القابلة للتسليم، على ضمان الوفاء بمسؤوليات المقاول. عندما تحدد أنشطة الإشراف والمراقبة أوجه القصور في أداء الطرف الثالث، يمكن للمؤسسة اتخاذ إجراءات تصحيحية.

يجب على المدققين والمؤسسات ملاحظة أن موردي الطرف الثالث (لتضمين الخدمات السحابية ووظائف "المكتب الخلفي" التي يوفرها موردو الجهات الخارجية) يشكلون جزءًا من بيئة الرقابة الخاصة بالمنظمة. لذلك، قد يكون التطبيق والضوابط العامة التي يديرها الطرف الثالث أيضًا في نطاق تدقيق تقنية المعلومات، بالإضافة إلى أي ضوابط مثل المراقبة والإشراف على أنشطة المورد.

ي. انعدام الشفافية والمساءلة

المساءلة والشفافية عنصران مهمان من عناصر الحكم الرشيد. الشفافية هي قوة قوية، عندما يتم تطبيقها باستمرار، يمكن أن تساعد في مكافحة الفساد وتحسين الحوكمة وتعزيز المساءلة.[44] في غياب الهياكل التنظيمية والاستراتيجيات والإجراءات والضوابط الرقابية الملائمة، قد تفشل المؤسسة في أن تكون خاضعة للمساءلة والشفافية بشكل كامل.

ك. عدم الامتثال للبيانات القانونية والتنظيمية

يحتاج أصحاب المصلحة إلى مزيد من التأكيد على أن المنظمات تمتثل للقوانين واللوائح وتتوافق مع ممارسات حوكمة الشركات الجيدة في بيئة عملها. بالإضافة إلى ذلك، نظرًا لأن تقنية المعلومات قد مكنت عمليات تجارية شبه سلسة بين المؤسسات، فثمة أيضًا حاجة متزايدة للمساعدة في ضمان أن العقود تتضمن متطلبات مهمة متعلقة بتقنية المعلومات في مجالات مثل الخصوصية والسرية والملكية الفكرية والأمن.[45] يجب أن تتضمن السياسات المختلفة التي تمتلكها المنظمة، مثل أمن تقنية المعلومات والاستعانة بمصادر خارجية والموارد البشرية، الأطر القانونية والتنظيمية ذات الصلة.

ل. إنفاق غير معروف أو مرتفع للغاية أو غير كاف على تقنية المعلومات

غالبًا ما تجد المؤسسات أنها ليست على دراية بالمبلغ الكامل الذي تنفقه على تقنية المعلومات، أو أن الإنفاق على تقنية المعلومات أعلى من المتوقع. قد يكون هذا بسبب عدم وجود مؤسسة مركزية واحدة أو فرد مسؤول عن جميع النفقات المتعلقة بتقنية المعلومات، أو لأن وحدات العمل داخل المؤسسة قد لا تصنف التكاليف المتعلقة بتقنية المعلومات بشكل مناسب. تتطلب أفضل الممارسات آليات اتخاذ قرارات الاستثمار في تقنية المعلومات (أي مجالس حوكمة تقنية المعلومات) للموافقة على جميع النفقات المتعلقة بتقنية المعلومات. يجب اتخاذ قرارات الاستثمار في تقنية المعلومات بناءً على مجموعة الاحتياجات داخل المنظمة. بدون هذا الإشراف، قد لا تكون المنظمة قادرة على ضمان تلبية أولويات تقنية المعلومات الخاصة بها.

بالإضافة إلى خطر عدم معرفة المؤسسة بإنفاقها الكامل على تقنية المعلومات، أو أن إنفاقها على تقنية المعلومات قد يكون مرتفعًا بشكل مفرط، فقد تجد المؤسسة أن ميزانية تقنية المعلومات الخاصة بها غير كافية لتلبية احتياجات العمل الجديدة أو التهديدات الناشئة. تجد العديد من المؤسسات أن معظم ميزانيات تقنية المعلومات الخاصة بها تُنفق على صيانة أنظمتها الحالية وبنيتها التحتية. على سبيل المثال، غالبًا ما تنفق المؤسسات أجزاء كبيرة من ميزانية تقنية المعلومات الخاصة بها على تراخيص البرامج والدعم والصيانة ذات الصلة. نظرًا لأن تحديد تراخيص البرامج واستخدامها ليس بالأمر السهل بدون الأدوات المناسبة والمعرفة المتخصصة، فثمة خطر متزايد يتمثل في إنفاق الأموال على البرامج غير المستخدمة.

للتحكم بشكل أفضل في الإنفاق على تقنية المعلومات، من المهم أن تحدد المؤسسة احتياجات وأهداف أعمال تقنية المعلومات الخاصة بها، وتحديد المشاريع التي لا تساهم في تلبيتها، واتخاذ القرارات بناءً على محفظة تقنية المعلومات ككل. على سبيل المثال، غالبًا ما يُشار إلى الحوسبة السحابية على أنها تساعد في تقليل التكاليف التشغيلية، ومع ذلك، اعتمادًا على الخدمة والتكوين واستخدام الخدمة السحابية، يمكن أن تكون الحوسبة السحابية أكثر تكلفة. يجب أن تقيّم الإدارة الجيدة لتقنية المعلومات نماذج الأعمال الجديدة هذه قبل أن يتم تنفيذها.

م. عدم وجود عملية برمجية منفذة

يمكن أن يؤدي عدم تنفيذ عملية البرنامج إلى خلق حالات لا تفي فيها البرامج المشتراة أو المطورة باحتياجات و / أو معايير العمل. قد تحدث المواقف التالية:

---

[44] المنظمة الدولية للأجهزة العليا للرقابة المالية والمحاسبة، *INTOSAI-P 20، مبادئ الشفافية والمساءلة*، ص 5.

[45] *إطار عمل COBIT 5، الملحق E - المبدأ 5 - التوافق.*

- اقتناء / تطوير البرامج التي لا تلبي احتياجات مجال عمل المنظمة،
- اقتناء / تطوير البرمجيات دون فحص الجودة،
- تطوير برمجيات لم يتم تنفيذها لأنها تفتقر إلى الجودة القياسية،
- تطوير برمجيات غير مكتملة أو غير مطابقة للمواصفات، و
- انقطاع أو عدم اكتمال مشاريع تطوير البرمجيات.

رابعا. المراجع وقراءات إضافية

المحكمة الفيدرالية للحسابات في البرازيل. *احصل عليه: تقنيات تقييم الحوكمة لتقنية المعلومات: دليل WGITA لأجهزة الرقابة العليا*. 2016.

إيساكا. المستند التقني - *الخصوصية في الممارسة 2021: اتجاهات خصوصية البيانات والتنبؤات والتحديات*. https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whppip. 2021.

إيساكا. *إطار عمل COBIT 2019: أهداف الحوكمة والإدارة*. 2019.

إيساكا. *إطار عمل COBIT 5: إطار الحوكمة لحوكمة وإدارة تقنية المعلومات الخاصة بالمؤسسات*. 2012.

إيساكا. *دليل مراجعة CISA*، الطبعة 27.

إيساكا. *إدارة البائعين باستخدام COBIT 5*. 2016.

المنظمة الدولية للتوحيد القياسي / اللجنة الكهروتقنية الدولية. *ISO / IEC 38500: 2015 تقنية المعلومات - حوكمة تقنية المعلومات للمؤسسة*. https://www.iso.org/standard/62816.html. فبراير 2015.

المعهد الوطني للمعايير والتقنية. *إطار عمل تحسين الأمن السيبراني للبنية التحتية الحرجة*، الإصدار 1.1. https://www.nist.gov/cyberframework/framework. أبريل 2018.

منظمة التعاون الاقتصادي والتنمية. *مبادئ G20 / OECD لحوكمة الشركات*. http://www.oecd.org/corporate/principles-corporate-governance. 30 نوفمبر 2015.

مكتب محاسبة الحكومة الأمريكية. *تقنية المعلومات: تحتاج الوكالات إلى التنفيذ الكامل لأنشطة تخطيط القوى العاملة الرئيسة*. GAO-20-129. https://www.gao.gov/products/gao-20-129. 30 أكتوبر 2019

مكتب محاسبة الحكومة الأمريكية. *مكتبة الكونجرس: القيادة القوية اللازمة لمعالجة نقاط الضعف* الخطيرة في إدارة تقنية المعلومات. GAO-15-315. https://www.gao.gov/products/gao-15-315. 31 مارس 2015.

مكتب محاسبة الحكومة الأمريكية. *إدارة استثمار تقنية المعلومات: إطار لتقييم وتحسين نضج العملية (يحل محل AIMD-10.1.23)*. GAO-04-394G. https://www.gao.gov/products/gao-04-394g. 1 مارس 2004.

الفصل 3: تطوير واكتساب تقنية المعلومات

1. ما هو تطوير واكتساب تقنية المعلومات؟

نظرًا لأن دور تقنية المعلومات أصبح حاسمًا لتحقيق أهداف العمل وتوفير قدرات متزايدة للمستخدمين، فقد سعت المؤسسات بشكل متزايد إلى تحديث الحلول القديمة وتطوير حلول تقنية المعلومات الجديدة واكتسابها. يمكن تحقيق حلول تقنية المعلومات الجديدة من خلال تطويرها داخليًا أو الحصول عليها خارجيًا من خلال التعاقد أو الاستعانة بمصادر خارجية (لُطفًا راجع الفصل 5 للحصول على معلومات إضافية بخصوص الاستعانة بمصادر خارجية). غالبًا ما يتم استخدام مجموعة من الأساليب. يجب أن تختار المنظمات تطوير حلول تقنية المعلومات أو الحصول عليها بناءً على النهج الأفضل الذي يلبي احتياجات المنظمة. في بعض الأحيان يتم شراء حلول تقنية المعلومات ودمجها مع الحلول الحالية للمؤسسة. في أوقات أخرى، يتم تطوير حلول جديدة داخليًا للتعويض عن نقص الوظائف المتاحة في السوق.

بغض النظر عما إذا كانت المنظمة تتخذ نهجًا داخليًا أو خارجيًا لتطوير حلول تقنية المعلومات واكتسابها وتنفيذها، يجب التخطيط للعملية بحيث يمكن إدارة المخاطر وتعظيم فرص النجاح. بالإضافة إلى ذلك، يجب تحديد متطلبات هذه الحلول وتحليلها وتوثيقها وتحديد أولوياتها. يجب على المنظمات أيضًا توظيف وظيفة ضمان الجودة والاختبار لضمان جودة هذه الحلول بشكل أفضل.

عادة ما يتم بناء الحلول أو الحصول عليها من خلال هيكل فريق المشروع. على الرغم من أن المؤسسات قد لا تضفي الطابع الرسمي على مشروع في بعض الأحيان، إلا أنها لا تزال بحاجة إلى إنجاز الأنشطة الرئيسة المشتركة المرتبطة بتخطيط وتنفيذ عملية تطوير أو اكتساب (على سبيل المثال، تحديد المتطلبات وإدارة المخاطر).

وفقًا لـ *Capability Maturity Model® Integration (CMMI) لغرض الاستحواذ*، الإصدار 1.3 من معهد هندسة البرمجيات، تكتسب المؤسسات بشكل متزايد قدرات نظرًا لأن المنتجات والخدمات متاحة بسهولة وعادة ما تكون أرخص من تطويرها داخليًا. ومع ذلك، فإن مخاطر الحصول على منتجات لا تلبي هدف العمل أو تفشل في إرضاء المستخدمين أمر حقيقي للغاية. يجب إدارة هذه المخاطر لغرض الاستحواذ لتلبية أهداف العمل ورسالته بنجاح. عندما يتم ذلك بطريقة منضبطة، اقتناء تقنية المعلومات يمكن أن تحسن الكفاءات التشغيلية للمؤسسة من خلال الاستفادة من قدرات الموردين لتقديم حلول عالية الجودة بسرعة وبتكلفة أقل وباستخدام التقنية الأكثر ملاءمة.

يتطلب الحصول على منتج أو حل أن يكون لدى المؤسسة فهم لاحتياجات ومتطلبات العمل الخاصة بها على النحو المحدد من خلال عملية حوكمة تقنية المعلومات الخاصة بها (لُطفًا راجع الفصل 2 لمزيد من المعلومات بخصوص حوكمة تقنية المعلومات وإدارتها). يجب أن تشمل عملية تحديد المتطلبات جميع أصحاب المصلحة المعنيين (مالكي العمليات) الذين يشاركون في عملية الأعمال، مثل المستخدمين النهائيين والموظفين التقنيين الذين قد يحتاجون في النهاية إلى صيانة ودعم النظام. عند الحصول على الخدمات (على سبيل المثال، مكتب المساعدة وأتمتة سطح المكتب) يجب أن يتضمن تحديد المتطلبات قسم تقنية المعلومات الذي سيتعامل مع مزود الخدمة. يجب تحديد أولويات المتطلبات بحيث إذا كان المشروع يعاني من نقص في الميزانية أو قيود التكلفة الأخرى، فيمكن تأجيل متطلبات معينة إلى عمليات الإنشاء أو الاستحواذ المستقبلية عند الاقتضاء.

تأتي عملية تطوير واكتساب تقنية المعلومات مع عدد من المسؤوليات الإدارية. غالبًا ما تستخدم المنظمات منهجية SDLC لتوفير هيكل إدارة المشروع والمساعدة في الوفاء بهذه المسؤوليات. عادة ما تكون ثمة خمس مراحل في SDLC: (1) البدء، (2) التطوير والاستحواذ، (3) التنفيذ، (4) التشغيل والصيانة، (5) التخلص. تمت مناقشة منهجيات SDLC بمزيد من التفصيل في القسم التالي.

أ. منهجيات المشروع

ثمة العديد من منهجيات SDLC المختلفة التي يمكن استخدامها لتطوير أنظمة تقنية المعلومات، والتي تتراوح من نموذج الشلال التقليدي إلى النموذج الحلزوني والنماذج التكرارية، مثل نموذج Agile.

- يبدأ **نموذج الشلال** بتطوير المتطلبات ويستمر بالتتابع عبر مراحل أخرى - التصميم والبناء والاختبار - باستخدام مخرجات مرحلة واحدة كمدخل إلى المرحلة التالية لتطوير منتج نهائي في النهاية. يسمح هذا النموذج بتحديد حالة مشروع التطوير وتتبعها بسهولة بناءً على المرحلة الحالية من المشروع.
- يستخدم **النموذج الحلزوني** نهجًا قائمًا على المخاطر لبناء نظام تدريجيًا عن طريق التدوير خلال مراحل التطوير الأربع. باستخدام هذا النموذج، تبدأ كل دورة حلزونية أو تدريجية عادةً بتحديد أهداف التطوير ونطاق الزيادة. بعد ذلك، يتم تقييم الحلول البديلة واستخدام تقنيات إدارة المخاطر لتحديد وتقليل المخاطر. ثم يتم تطوير منتج للزيادة (مثل نموذج أولي). أخيرًا، يتم تقييم المنتج لتحديد ما إذا كانت الأهداف الأولية للزيادة قد تحققت.
- يركز **نموذج Agile** على مراحل تطوير قصيرة المدى وصغيرة النطاق تنتج شرائح من منتج وظيفي. يعمل هذا النموذج بمراحل مماثلة لنموذج الشلال التقليدي - المتطلبات والتصميم والبناء والاختبار - ولكنه يستخدم دورة تطوير أقصر لتحقيق تكرارات متعددة في أطر زمنية مماثلة. تم تحديد الأساليب الأقصر والأكثر تدريجيًا لتطوير تقنية

المعلومات على أنها تنطوي على إمكانية تحسين طريقة تطوير تقنية المعلومات وتنفيذها.[46]

ثمة أطر أخرى مرتبطة بـ Agile وتستخدم العديد من نفس المبادئ والممارسات. من الأمثلة على ذلك:

- يؤكد نموذج **DevOps** على التعاون بين التطوير وعمليات تقنية المعلومات وضمان الجودة بهدف زيادة إصدارات البرامج بشكل متكرر. تتوافق قيم DevOps الإجمالية مع Agile، وتعتبر DevOps توسعًا لممارسات التنفيذ السريع في جميع مجالات دورة حياة المنتج.
- يقسم **التطوير التكراري** العمل إلى أجزاء أصغر تُعرف باسم التكرارات، بهدف التصميم والتطوير والاختبار في دورات.

وفقًا لـ *CMMI للتطوير* التابع لمعهد هندسة البرمجيات، الإصدار 1.3، عند إنشاء منهجية التطوير والاكتساب التنظيمي، يجب على المنظمة تحديد المتطلبات والإرشادات التي يمكن تخصيصها لمشروع معين والحفاظ عليها. يجب أن تستند هذه المتطلبات والإرشادات إلى نموذج التطوير المختار وقضايا أخرى، مثل احتياجات العملاء والتكلفة والجدول الزمني والصعوبة الفنية.

على الرغم من أن المنظمات قد تختار من بين مجموعة متنوعة من منهجيات المشروع، إلا أن ثمة أفضل الممارسات الرئيسة التي، عند اعتمادها، تزيد من احتمالية النجاح في تطوير واكتساب المنتجات أو الخدمات. وتشمل هذه، على سبيل المثال، تطوير المتطلبات وإدارتها، وإدارة المخاطر، وإدارة المشروع، والاختبار، والإشراف على البائعين (سواء أثناء الاستحواذ أو فيما بعد إذا كانوا يعملون أو يدعمون النظام)، والتدريب الداخلي. تتم مناقشة هذه المجالات بمزيد من التفصيل في القسم التالي.

بغض النظر عن منهجية المشروع المختارة، فإن التوثيق المناسب هو عامل مهم. بالإضافة إلى ذلك، ينبغي إيلاء الاهتمام لضمان توفر الوثائق أيضًا بعد اكتمال التطوير. في الحالات التي تعتمد فيها المؤسسة على حل مطور لتوصيل المتطلبات ومواءمة سجلات المستخدم ومراقبة التطوير، من الشائع أن يتعذر الوصول إلى الوثائق بعد نهاية التطوير، مما يجعل من الصعب على المؤسسات تتبع مدى وامتثال ذلك تم إنتاجه.

ثانيًا. العناصر الرئيسة لاكتساب وتطوير تقنية المعلومات

أ. إجراء دراسة الجدوى

على الرغم من وجود تفسيرات لمنهجية المشروع تستخدم مراحل مختلفة وأسماء مختلفة، قد تنظر المنظمات في مرحلة دراسة الجدوى كخطوة أولية، قبل تحديد المتطلبات. يمكن أن تساعد دراسة الجدوى في تحليل الفوائد والحلول لمنطقة المشكلة المحددة. أهداف دراسة الجدوى هي

- تحديد الحاجة بوضوح؛
- تحديد الحل الأمثل البديل القائم على المخاطر (على سبيل المثال ما إذا كان سيتم التطوير أو الاستحواذ)؛
- تحديد الإطار الزمني لتنفيذ الحل؛
- تحديد التكلفة التقريبية للتطوير / الاستحواذ؛ و
- تحديد ما إذا كان الحل يناسب استراتيجية العمل.

يجب أن تكون نتيجة الدراسة تقريرًا مقارنًا يوضح نتائج المعايير التي تم تحليلها (على سبيل المثال، التكاليف والفوائد والمخاطر والموارد المطلوبة والأثر التنظيمي) ويوصي بأحد البدائل / الحلول ومسار العمل (على سبيل المثال، ما إذا كان تطوير أو الحصول على نظام).

ب. تطوير وإدارة المتطلبات

عند الحصول على برامج جديدة أو تطويرها أو تعديل أنظمة المعلومات الحالية، يجب على فرق المشروع والمطورين تحديد المتطلبات ويجب أيضًا إدارة التغييرات على تلك المتطلبات. تحدد المتطلبات ما يجب على النظام القيام به، ومدى جودة القيام بذلك، وكيف يتفاعل مع الأنظمة الأخرى. المتطلبات المحددة والمدارة جيدًا هي الأساس لتطوير النظام الفاعل وجهود الاستحواذ. يحدد *CMMI للتطوير* التابع لمعهد هندسة البرمجيات، الإصدار 1.3، الممارسات الرائدة في أربعة مجالات تتعلق بتطوير وإدارة المتطلبات:

- **تطوير متطلبات العملاء.** جمع احتياجات أصحاب المصلحة والتوقعات والقيود والواجهات وجميع متطلبات الأتمتة (الرقمنة) التي تدار مركزياً بواسطة قسم تقنية المعلومات أو بمشاركة كبيرة من قسم تقنية المعلومات وترجمتها إلى متطلبات العملاء؛

[46] لمزيد من المعلومات بخصوص نموذج Agile، راجع مكتب محاسبة الحكومة الأمريكية، *دليل التقييم السريع: أفضل الممارسات للتبني السريع والتنفيذ*، GAO-20-590g، (28 سبتمبر 2020)، https://www.gao.gov/products/gao-20-590g.

- **تطوير متطلبات المنتج.** صقل وتفصيل متطلبات العملاء لتطوير متطلبات المنتج ومكونات المنتج؛
- **تحليل والتحقق من صحة المتطلبات.** التحقق من قابلية استخدام أصول تقنية المعلومات الحالية (بما في ذلك البرامج التطبيقية) إن وجدت؛ تحليل المتطلبات والتحقق منها فيما يتعلق بالبيئة التي يقصدها المستخدم النهائي؛ و
- **إدارة المتطلبات.** إدارة المتطلبات وتحديد التناقضات مع خطط المشروع ومنتجات العمل.

وفقًا لمعهد هندسة البرمجيات، يجب على المؤسسات أيضًا أن تضع وتحافظ على الخطط التي تحدد عمليات أداء وتحقيق هذه الممارسات الرائدة للمتطلبات والتي تحدد وتعزز التوقعات لأصحاب المصلحة المعنيين. يوصي معهد هندسة البرمجيات بإجراء عملية موثقة ومنضبطة لتطوير وإدارة المتطلبات لتقليل مخاطر تطوير نظام لا يلبي احتياجات المستخدم، ولا يمكن اختباره بشكل كافٍ، ولا يؤدي أو يعمل على النحو المنشود.

ج. إدارة المخاطر

يتطلب التطوير والاكتساب الفاعل أي مؤسسة لتحديد المخاطر وتحديد أولوياتها وإدارتها في كل مرحلة من مراحل SDLC. عندما يتم تحديد المشكلات، يمكن التخطيط لأنشطة معالجة المخاطر والاستناد إليها حسب الحاجة طوال عمر المشروع بهدف التخفيف من الآثار السلبية على الأهداف. تتضمن الإدارة الفاعلة للمخاطر تحديد المخاطر بشكل مبكر وشديد من خلال التعاون وإشراك أصحاب المصلحة المعنيين. استنادًا إلى CMMI في معهد هندسة البرمجيات، يمكن تقسيم أنشطة إدارة المخاطر إلى أربعة مجالات رئيسية:

- **التحضير لإدارة المخاطر.** يتم الإعداد من خلال إنشاء والحفاظ على استراتيجية لتحديد وتحليل وتخفيف المخاطر. تتناول استراتيجية إدارة المخاطر الإجراءات المحددة ونهج الإدارة المستخدم لتطبيق ومراقبة برنامج إدارة المخاطر. كما يتضمن تحديد وإشراك أصحاب المصلحة المعنيين في عملية إدارة المخاطر. تشمل الأنشطة المرتبطة بالتحضير لإدارة المخاطر، على سبيل المثال، تطوير متطلبات إدارة المخاطر واستراتيجية إدارة المخاطر.
- **تحديد وتحليل المخاطر.** تحديد المخاطر من المصادر الداخلية والخارجية ثم تقييم كل خطر تم تحديده لتحديد احتمالية وعواقبه. يشمل تحليل المخاطر تقييم المخاطر، وتصنيفها، وتحديد الأولويات، ويستخدم في تحديد متى يلزم اهتمام الإدارة المناسب. تشمل الأنشطة المرتبطة بتحديد وتحليل المخاطر، على سبيل المثال، وضع قائمة بالمخاطر المحددة وتحديد فئة وأولوية ومصدر لكل خطر.
- **التخفيف من المخاطر.** يتضمن التخفيف من حدة المخاطر تطوير التقنيات والأساليب المستخدمة لتجنب وتقليل والسيطرة على احتمالية حدوث المخاطر المحددة. يجب وضع خطط لتخفيف المخاطر لأهم المخاطر التي يتعرض لها المشروع. يجب مراقبة حالة كل خطر بشكل دوري لتحديد ما إذا تم تجاوز الحدود المحددة أم لا، وينبغي تنفيذ خطط التخفيف من المخاطر عند الاقتضاء. تشمل الأنشطة المرتبطة بتخفيف المخاطر، على سبيل المثال، تطوير خطط التخفيف من المخاطر وخطط الطوارئ.
- **الرقابة التنفيذية.** الأنشطة الأساسية المرتبطة بالإشراف التنفيذي هي مراجعات لحالة مخاطر المشروع التي يتم إجراؤها على أسس دورية وقائمة على الأحداث مع مستويات مناسبة من الإدارة لتوفير رؤية بخصوص إمكانية التعرض لمخاطر المشروع والإجراءات التصحيحية المناسبة. لُطفًا راجع الفصل 2 لمزيد من المعلومات بخصوص دور الرقابة التنفيذية في توجيه أنشطة تقنية المعلومات داخل المنظمات.

د. إدارة المشروع والتحكم فيه

تتضمن إدارة المشروع تحديد خطة المشروع وأنشطة المراقبة. تتضمن إدارة المشروع أيضًا تحديد خطوط الأساس للتكلفة والجدول الزمني، وتحديد الجداول الزمنية للمشروع، وإشراك أصحاب المصلحة في الأنشطة الرئيسة. تتضمن مراقبة المشروع الإشراف وإعداد التقارير الدورية لاتخاذ الإجراءات التصحيحية عندما لا يتوافق أداء المشروع مع الخطة. على سبيل المثال، إذا ارتفعت تكلفة المشروع بشكل كبير، فقد تختار المنظمة قطع وظائف معينة بعد التشاور مع أصحاب المصلحة لاحتواء التكلفة.

يجب وصف هيكل إدارة المشروع في نهج SDLC الخاص بالمؤسسة أو استراتيجية الاستحواذ عند الاقتضاء. بشكل عام، يتكون هيكل إدارة المشروع من مدير المشروع، وموظف المخاطر، وموظفي دعم إدارة ضمان الجودة والتكوين، وموظفين من مجموعة الاختبار إن لم يكن جزءًا من ضمان الجودة. تعمل خطة المشروع كأساس لتوجيه جميع الأنشطة. الإحاطة الدورية للإدارة العليا تبقيهم على دراية بحالة المشروع وكيفية إدارة المخاطر. بالإضافة إلى ذلك، يتيح لهم التفكير في المفاضلات التي تتضمن التكلفة والجدول الزمني والأداء نظرًا لأنه من النادر أن يلبي المشروع جميع أهدافه المقصودة في هذه المجالات.

هـ. تطوير التصميم

بناءً على المتطلبات المحددة، يجب أن ينشئ التصميم أساسًا لمواصفات النظام والنظام الفرعي التي تصف أجزاء النظام، بما في ذلك كيفية تفاعلها وكيفية تنفيذ النظام باستخدام الأجهزة والبرامج ومرافق الشبكة المختارة. بشكل عام، يتضمن التصميم أيضًا مواصفات البرنامج وقاعدة البيانات وسيعالج أي اعتبارات أمنية. بعد ذلك، أثناء التطوير، يتم استخدام مواصفات التصميم لبدء البرمجة وإضفاء الطابع الرسمي على العمليات التشغيلية الداعمة للنظام.

على مر السنين، حدث تطوير تطبيقات الأعمال إلى حد كبير باستخدام مراحل SDLC التقليدية. نظرًا لأن الحزم المشتراة أصبحت أكثر شيوعًا، يتم استبدال مراحل التصميم / التطوير لدورة الحياة التقليدية **بالطلب**[47] مرحلة.

نتيجة لذلك، عند الحصول على حلول تقنية المعلومات، غالبًا ما تستخدم المؤسسات حزمة التماس (طلب عرض). طلب تقديم العروض هو عملية توثيق متطلبات العمل وجمع المواد المرجعية الأخرى التي ستساعد البائع في توفير حل تقنية المعلومات. ويتضمن إنشاء حزمة العطاءات وطرحها للمناقصة والحصول على العروض والاختيار من بين البائعين المختلفين. يجب أن تكون عملية الاختيار شفافة وموضوعية وتستند إلى معايير مناسبة للنظام أو الخدمات التي يتم الحصول عليها. من الأهمية بمكان أن يُشرك فريق المشروع قسمه القانوني في هذه العملية. الفريق القانوني على دراية بالقوانين واللوائح، ويمكنه المساعدة في ضمان أن تكون معايير اختيار البائع عادلة وسيتم دعمها في محكمة قانونية إذا طعن بائعون خاسرون في الجائزة.

و. ضمان الجودة والاختبار

يوفر ضمان الجودة لموظفي المشروع والإدارة نظرة ثاقبة لجودة ووظائف منتجات العمل المؤقتة والنهائية. للقيام بذلك، يجب على الموظفين المشاركين في ضمان الجودة إنشاء إطار عمل لضمان الجودة، ودليل مستخدم نظام جيد التوثيق، وتقييم منتجات العمل بشكل دوري للتأكد من أنها تلبي معايير الجودة الموثقة للمنظمة وما إذا كان الموظفون قد اتبعوا العمليات المطلوبة بغية تطوير المنتجات. تحتاج المنظمات إلى التحقق من أن المنتج المطور أو المكتسب يلبي المتطلبات، ويفي بمعايير القبول (على سبيل المثال، أقل من عدد معين من الأخطاء غير الفادحة) وخضع للاختبار (وظيفي، تكامل النظام وقبول المستخدم) بمشاركة المستخدم وأصحاب المصلحة.

كما ينبغي لموظفي ضمان الجودة التأكد من اتباع منهجية التطوير المعتمدة والمتفق عليها، وإجراء الرقابة المطلوبة. على سبيل المثال، يجب عليهم التأكد من إجراء المراجعات (الرسمية أو غير الرسمية) وإرسال تقارير الحالة الضرورية إلى أصحاب المصلحة والإدارة المناسبين. علاوة على ذلك في عملية ضمان الجودة، يجب على موظفي ضمان الجودة والإدارة العليا تقييم ما إذا كان فريق المشروع يتبع السياسات والإجراءات الموضوعة داخليًا للاكتساب أو جهود التطوير. يجب أن يكون إشراف كبار الموظفين واضحًا في المراحل الرئيسة من دورة الاستحواذ أو التطوير.

ز. إدارة التكوين

تُستخدم إدارة التكوين لضمان الحفاظ على سلامة المستندات والبرامج والمواد الوصفية أو الداعمة الأخرى التي تشكل جزءًا من النظام الذي يتم تطويره أو الحصول عليه. تتم إدارة التغييرات على هذه المواد (تسمى أيضًا منتجات العمل) ويتم إنشاء خطوط الأساس (أو الإصدارات) بحيث تكون المؤسسة قادرة على العودة إلى الإصدارات المعروفة والمختبرة حسب الحاجة.

قد تستخدم المنظمات لوحة التحكم في التكوين للمساعدة في أنشطة إدارة التكوين. لوحة التحكم في التكوين عبارة عن مجموعة من موظفي إدارة التكوين المؤهلين الذين يشاركون في الموافقة على البرامج أو ترخيصها للتثبيت في بيئة الإنتاج. عادةً ما يتم ذلك بعد اختبار المستخدم وأي اختبار إضافي مطلوب لضمان استمرار الأنظمة الأخرى في العمل كما كان من قبل بمجرد تثبيت النظام أو البرنامج الجديد (على سبيل المثال، اختبار التكامل[48] أو اختبار الانحدار).[49] من المهم تضمين التكامل مع الأنظمة الحالية واختبار الانحدار ذي الصلة في اتفاقية الاستعانة بمصادر خارجية مع المطور. من المهم أيضًا ضمان إدارة التكوين ليس فقط في بيئة الإنتاج، ولكن أيضًا في بيئة الاختبار أثناء التطوير.

ثالثا. المخاطر على الهيئة الخاضعة للرقابة

عندما تقوم منظمة ما بتطوير برامج داخلية، فإنها تواجه عددًا من المخاطر أو التحديات في ضمان نجاح المشروع. تتعلق بعض هذه المخاطر بالمهارات في مجال البرمجيات، والخبرة في الاختبار وإدارة المشروع، وتقديرات التكلفة والفوائد المعقولة، والقدرة على مراقبة حالة المشروع وتتبعها. على سبيل المثال، يمكن أن تنشأ المشاكل بسبب سوء تطبيق عمليات وأساليب تطوير البرمجيات الرشيقة. يمكن أن تشمل هذه المشكلات عدم تحديد الأدوار الرئيسة السريعة، أو تحديد أولويات متطلبات النظام، أو تنفيذ القدرات الآلية.

---

[47] يشار إليه أيضًا بالاختيار والاستحواذ.

[48] اختبار التكامل هو المرحلة في اختبار البرامج التي يتم فيها دمج وحدات البرامج الفردية واختبارها كمجموعة. يحدث هذا عادةً بعد اختبار الوحدة وقبل التحقق من الصحة أو اختبار القبول.

[49] اختبار الانحدار هو نوع من اختبار البرامج الذي يتحقق من أن البرنامج الذي تم تطويره واختباره مسبقًا لا يزال يعمل بشكل صحيح بعد تغييره أو التفاعل مع برامج أخرى. قد تتضمن هذه التغييرات تحسينات البرامج والتصحيحات وتغييرات التكوين. أثناء اختبار الانحدار، قد يتم اكتشاف أخطاء برمجية جديدة أو انحدارات.

بالإضافة إلى ذلك، يجب أن تتضمن متطلبات البرنامج أو النظام التي تجمع، واختبار، والموافقة عليها جميع المستخدمين النهائيين (على سبيل المثال، المستخدمين الداخليين والخارجيين)، ويجب على المدققين النظر فيما إذا كان قد تمت استشارة المستخدمين في تعريف المتطلبات. يجب أن ينظر المدققون أيضًا في ما إذا كان الموظفون المشاركون في مجال ضمان الجودة مستقلين وموضوعيين في تقييمهم لجودة النظام أثناء تطويره. كما هو الحال في الاستحواذ، يجب إطلاع الإدارة بشكل دوري على حالة المشروع ويجب أن تتخذ الإجراءات التصحيحية عند الاقتضاء.

ينصب التركيز الأساسي للمدققين عند مواجهة منظمة قامت بشراء نظام (أو منتج) على تحديد ما إذا كانوا يديرون البائع ويحصلون على تقارير دورية عن الحالة واتخاذ الإجراءات التصحيحية. بغية القيام بذلك، يحتاج العقد إلى تحديد المعالم الرئيسة أثناء التطوير والتنفيذ حيث توجد مراجعة رسمية وتقارير حالة تزود الوكالة بمعلومات التكلفة والجدول الزمني والأداء. سيحتاج المدقق إلى التأكد من أن إدارة الوكالة أو الموظفين المعينين يتلقون ويراجعون ويتخذون إجراءات تصحيحية بشأن تقارير الحالة وأنشطة العقود عند الاقتضاء.

يجب على مدقق تقنية المعلومات أيضًا مراجعة ما إذا كان

- يتم تنفيذ التخطيط المناسب للمشروع، بما في ذلك التقديرات الفاعلة للموارد والميزانية والوقت؛
- كان قرار التطوير / الاستحواذ مناسبًا؛
- تم تحقيق أهداف ومتطلبات النظام؛
- يتم قياس التكلفة والفوائد المحددة في دراسة الجدوى وتحليلها وإبلاغ الإدارة بها بدقة؛
- تم التحكم في زحف النطاق، و
- تم إجراء مراجعة دورية وتحليل المخاطر في كل مرحلة من مراحل المشروع.

رابعا. المراجع وقراءات إضافية

مجلس مسؤولي المعلومات. *مكتبة الموارد: المنشورات وكتيبات التشغيل والإرشادات والمزيد.* https://www.cio.gov/resources/.

وكالة تدقيق عقود الدفاع. *دليل تدقيق عقود DCAA.* https://www.dcaa.mil/Guidance/CAM-Contract-Audit-Manual/.

إيساكا. *BAI01-BAI10 إدارة — برنامج ضمان المراجعة*. 2014.

أنا ساكا. *دليل مراجعة CISA، الطبعة 27*. 2019.

إيساكا. *إطار عمل COBIT 2019: أهداف الحوكمة والإدارة*. 2019.

إيساكا. *برنامج تدقيق تطوير النظام وإدارة المشاريع*. 2009.

المعهد الوطني للمعايير والتقنية. *المنشور الخاص 800-39: إدارة مخاطر أمن المعلومات: عرض المنظمة والرسالة ونظام المعلومات*. مارس 2011. https://csrc.nist.gov/publications/detail/sp/800-39/final.

معهد هندسة البرمجيات. *CMMI for Acquisition* الإصدار 1.3. 2010 http://www.sei.cmu.edu/library/abstracts/reports/10tr032.cfm.

معهد هندسة البرمجيات. *CMMI للتطوير*، الإصدار 1.3. 2010 http://www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm.

تسوي وفرانك واورلاندو كرم. *أساسيات هندسة البرمجيات*، الطبعة الثانية. 2011.

مكتب محاسبة الحكومة الأمريكية. *دليل التقييم السريع: أفضل الممارسات لاعتماد وتنفيذ Agile*. GAO-20-590G. https://www.gao.org/products/gao-20-590g. 28 سبتمبر 2020.

مكتب محاسبة الحكومة الأمريكية. *يحتاج مكتب التعداد إلى تنفيذ ممارسات الإدارة الرئيسة*. GAO-12-915. https://www.gao.gov/products/gao-12-915. 18 سبتمبر 2012.

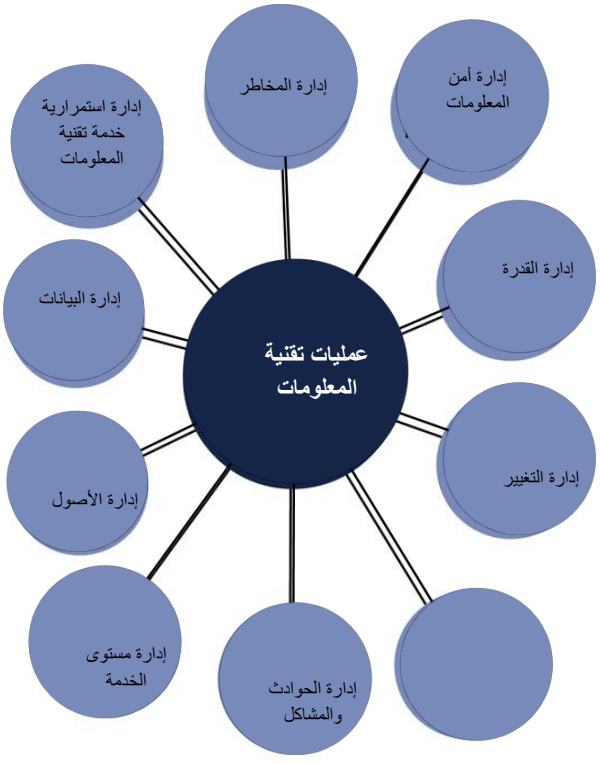
الفصل 4: عمليات تقنية المعلومات

1. ما هي عمليات تقنية المعلومات؟

على الرغم من وجود العديد من التفسيرات أو التعريفات المختلفة لعمليات تقنية المعلومات، إلا أنه يُعتقد عمومًا أنها المهام اليومية المتضمنة في تشغيل ودعم البنية التحتية لتقنية المعلومات لمؤسسة ما (على سبيل المثال، تشغيل الخوادم وإجراء الصيانة ومراقبة الأمن وتوفير ما يلزم التخزين، وتشغيل مكتب المساعدة). يتم قياس العمليات وإدارتها باستخدام **مؤشرات الأداء الرئيسة** (KPI) لعمليات تقنية المعلومات التي تحدد المعايير التي يمكن قياس الفاعلية التشغيلية على أساسها. يجب مراقبة هذه التدابير أو ما يعادلها بشكل مستمر ومراجعتها بشكل دوري. توثق معظم المؤسسات ذلك في اتفاقية بين مستخدمي الأعمال ومنظمة تقنية المعلومات. **اتفاقية مستوى الخدمة** (SLA) هي اتفاقية رسمية واحدة، حيث يتم توثيق هذه المعايير والترتيبات الأخرى. تمت مناقشة هذا بمزيد من التفصيل خلال هذا الفصل.

ثانيًا. العناصر الرئيسة لعمليات تقنية المعلومات

شكل8: مجالات عمليات تقنية المعلومات



المصدر: مجهول.

تتضمن عناصر عمليات تقنية المعلومات التي يجب على المدقق مراجعتها لتحديد ما إذا كانت المؤسسة تدير عمليات تقنية المعلومات بشكل فعال، على سبيل المثال، إدارة استمرارية خدمات تقنية المعلومات، وإدارة أمن المعلومات، وإدارة القدرات، وإدارة القوى العاملة، وإجراءات التعامل مع إدارة الحوادث والمشكلات لضمان استمرارية العمليات، وتغيير ممارسات الإدارة، وإدارة المخاطر (لُطفًا راجع الشكل 8). يتم تحديد هذه المجالات وغيرها في إطار مكتبة البنية التحتية لتقنية المعلومات ((ITIL،[50] أحد الأطر المعتمدة على نطاق واسع لتحديد خدمات تقنية المعلومات وتخطيطها وتقديمها ودعمها لأعمال المؤسسة.

لتحديد ما إذا كانت المنظمة الخاضعة للرقابة تقدم خدمات موثقة بشكل فعال، يجب على المدقق تقييم ما إذا كانت اتفاقية مستوى الخدمة تتضمن المعايير المحددة للخدمات المختلفة. قد تكون ثمة حالات في المؤسسات الأصغر حيث يمكن توثيق الاتفاقية بين المنظمة ومجموعة تقنية المعلومات في مخطط تنظيمي أو مستند آخر، بدلاً من اتفاقية مستوى الخدمة (SLA). بغض النظر عما يسمى المستند، يجب توثيق معلمات تقديم خدمات تقنية المعلومات والموافقة عليها من قبل مجموعات المستخدمين ومنظمة تقنية المعلومات.

أ. إدارة استمرارية خدمة تقنية المعلومات

يتمثل الغرض من إدارة الاستمرارية في الحفاظ على متطلبات استمرارية الأعمال المستمرة المناسبة، بالإضافة إلى تقليل تكاليف وقت التوقف عن العمل وتأثيرات الأعمال أثناء الحوادث على مستوى الكوارث. تنجز مؤسسة تقنية المعلومات ذلك من خلال تحديد وقت الاسترداد (المدة التي يستغرقها التعافي) وأهداف نقطة الاسترداد (من أي نقطة قبل الكارثة) لمكونات تقنية المعلومات المختلفة التي تدعم عمليات الأعمال بهدف الحفاظ على توافر الخدمة والأداء في أعلى المستويات الممكنة. بالإضافة إلى ذلك، تتضمن إدارة الاستمرارية مراجعة وتحديث أوقات ونقاط الاسترداد بشكل دوري للتأكد من أنها تتماشى مع خطط استمرارية الأعمال وأولويات العمل. يتم التطرق لهذا المجال بمزيد من التفصيل لاحقًا في الفصل 6.

[50] "ما هو ITIL؟" https://www.axelos.com/best-practice-solutions/itil/what-is-itil.

ب. إدارة المخاطر

إدارة المخاطر هي الممارسة التي تضمن أن المؤسسة تتفهم تمامًا وتعالج أي مخاطر تتعرض لها المنظمة، بما في ذلك تلك المتعلقة بعمليات تقنية المعلومات. يتم تعريف المخاطر على أنها المشاكل التي يجب التقليل منها أو التخفيف من حدتها لتجنب التأثير على قدرة المنظمة على تقديم قيمة لأصحاب المصلحة. تشمل المخاطر التي تتعرض لها عمليات تقنية المعلومات نشاط أو سلوك النظام غير المصرح به، والكشف غير المصرح به عن معلومات التعريف الشخصية، والتغييرات غير المصرح بها، من بين أمور أخرى. ممارسات وإجراءات إدارة المخاطر التي تنفذها المنظمة ستوجه قرارات المنظمة المتعلقة بالمخاطر. وفق ما تمت مناقشته سابقًا، يمكن تقسيم ممارسات وإجراءات إدارة المخاطر إلى أربعة مجالات رئيسية: (1) الاستعداد لإدارة المخاطر، (2) تحديد وتحليل المخاطر، (3) التخفيف من المخاطر، (4) الإشراف التنفيذي. لُطفًا راجع الفصل 3 للحصول على معلومات إضافية بخصوص كل مجال من المجالات الرئيسة الأربعة.

ج. إدارة أمن المعلومات

تتعلق إدارة أمن المعلومات بإدارة المخاطر المتعلقة بالأمن، وضمان تنفيذ ضوابط أمن المعلومات، واتخاذ الإجراءات المناسبة، والتأكد من أن المعلومات متاحة وقابلة للاستخدام وكاملة وغير منقوصة عند الحاجة. ويتعلق الأمر أيضًا بضمان وصول المستخدمين المصرح لهم فقط إلى المعلومات وحمايتها عند نقلها بين الوجهات والموثوقية عند وصولها. يتم التطرق لهذا المجال بمزيد من التفصيل لاحقًا في الفصل 7.

د. إدارة القدرات

تشمل إدارة القدرات إدارة الخدمات المختلفة التي تدعم المنظمة بطريقة تواكب متطلبات المنظمة أو المستخدمين. يعد تحسين سعة إنتاجية الشبكة وتوافر الموارد وتحسين التخزين والتنبؤ بالطلب جزءًا من إدارة السعة. بغية إدارة القدرات، تحتاج مؤسسة تقنية المعلومات إلى قياس الظروف الحالية وتحتاج إلى اتخاذ إجراءات تسهل تزويد المستخدمين بقدرات إضافية؛ على سبيل المثال، يمكن تحقيق ذلك من خلال الحصول على قوة معالجة إضافية عند تجاوز معلمات معينة (أي عندما يكون استخدام الكمبيوتر بنسبة 75 في المائة أو أكثر لـ 60 في المائة من يوم العمل).

هـ. إدارة التغيير

في مؤسسات تقنية المعلومات، تُستخدم عملية إدارة التغيير عادةً لإدارة التغييرات التي تطرأ على أنظمة تقنية المعلومات ومكوناتها والتحكم فيها، مثل البرامج والأجهزة والوثائق ذات الصلة. ثمة حاجة إلى ضوابط التغيير للتأكد من أن جميع التغييرات التي تطرأ على تكوينات النظام مرخصة واختبارها وتوثيقها والتحكم فيها بحيث تستمر الأنظمة في دعم عمليات الأعمال بالطريقة المخطط لها، وأن ثمة أثرًا وسجلًا مناسبًا للتغييرات.[51]

وبمجرد تنفيذ التغييرات، من المهم أن يكون ثمة فصل بين بيئات التطوير والاختبار والإنتاج وأن مطوري التغيير لا يُسمح لهم بالوصول إلى بيئة الإنتاج. وهذا يقلل من مخاطر إجراء تغييرات غير مختبرة أو غير معتمدة مباشرة في بيئة الإنتاج.

قد يؤدي التغيير غير المعتمد أو العرضي إلى مخاطر جسيمة على استمرارية الأعمال وعواقب مالية للمؤسسة. يجب أن تتبع المنظمات إجراءً محددًا لإدارة التغيير يتطلب موافقة مجلس الإدارة قبل تنفيذه في بيئة التشغيل. يقتضي أن تضمن عملية إدارة التغيير أن التغييرات يتم تسجيلها وتقييمها وترخيصها وتحديد أولوياتها وتخطيطها واختبارها وتنفيذها وتوثيقها ومراجعتها وفقًا لإجراءات إدارة التغيير الموثقة والمعتمدة.

يمكن تحديد التغييرات والبدء فيها، على سبيل المثال، عن طريق تغيير في بيئة الأعمال، أو تعديل نموذج العمل، أو الاحتياجات المشتركة بين العمليات، أو من خلال نتيجة الحادث أو تحليل المشكلة. يتحتم أن تتضمن إجراءات ضبط التغيير إجراءات بغية:

- إذن الإدارة (على سبيل المثال، توثيق عملية لتسجيل طلب التغيير)،
- اختبار شامل وترخيص من قبل إدارة العمليات قبل الاستخدام في البيئة الحية،
- مراجعة الإدارة لآثار أي تغييرات،
- الاحتفاظ بسجلات كافية،

---

[51] قد لا تتطلب تغييرات معينة في نظام تقنية المعلومات جميع الإجراءات المنصوص عليها في هذا القسم. على سبيل المثال، عادةً ما تكون **التغييرات القياسية** طفيفة جدًا ومنخفضة المخاطر على أنظمة تقنية المعلومات، وبالتالي قد يكون لها إشراف أقل بشكل مناسب (على سبيل المثال، لا حاجة لموافقة مجلس التغيير، ولكن لا تزال تتطلب الاختبار والتوقيع التشغيلي).

- إعداد الخطط الاحتياطية (في حالة حدوث أي خطأ)، و
- وضع إجراءات للتغييرات الطارئة.

برجاء مراجعة الشكل 9 لمعرفة الخطوات في عملية إدارة التغيير.

شكل9 : خطوات إدارة التغيير

المصدر: مجهول.

تعتبر تكلفة التغيير، والتأثير على نظام تقنية المعلومات وأهداف العمل، وتأثير عدم التنفيذ، ومتطلبات الموارد المستقبلية من المحددات المهمة في الإذن بالتغيير وتحديد أولوياته.

التغييرات الطارئة هي تغييرات لا يمكن أن تنتظر لتنفيذ إجراءات التحكم في التغيير العادية ويجب تنفيذها بأقل تأخير. ثمة وقت أقل لإجراء واختبار مثل هذه التغييرات، مما يزيد من مخاطر الأخطاء وأخطاء البرمجة.

في حالة وجود إجراءات تغيير طارئة، يجب على المدقق التحقق من أنها معقولة وتتضمن شكلاً من أشكال الرقابة. قد يشمل ذلك الموافقة على التغيير الطارئ من قبل أحد الموظفين مع السلطة المناسبة، مع وجود تسمية مناسبة للإصدار والتحكم جنبًا إلى جنب مع مسار المراجعة (أي استخدام تطبيقات التحكم في التغيير الآلي)، والموافقة بأثر رجعي من لوحة التغيير أو مالك النظام، والاختبار بأثر رجعي، وتحديث الوثائق.

و. إدارة القوى العاملة

تهدف إدارة القوى العاملة إلى التأكد من أن المنظمة لديها الأشخاص المناسبون الذين لديهم المهارات والمعرفة المناسبة في الأدوار الصحيحة لدعم المنظمة. بالنسبة لمؤسسة تقنية المعلومات التي تقدم خدمات للأعمال، تكون إدارة القوى العاملة فعالة عند نشر موظفي مؤسسة تقنية المعلومات المؤهلين والمدربين بشكل مناسب، واستخدام الموارد الكافية والأدوات المناسبة للتعامل مع مراقبة الشبكة ووظائف مكتب المساعدة، ويشارك الموظفون المشاركون بشكل استباقي في معالجة الاختناقات مع الاستمرار في الاستجابة لاحتياجات العمل. وبحب ما نوقش في الفصل 2، يجب على المنظمات تقييم احتياجات القوى العاملة بانتظام (على سبيل المثال، الكفاءة ومتطلبات التوظيف)، وتقييم الثغرات، ووضع استراتيجيات وخطط لمعالجة هذه الفجوات، من بين الأنشطة الرئيسة الأخرى.

ز. إدارة الحوادث والمشكلات

إدارة الحوادث هي الأنظمة والممارسات المستخدمة لتحديد ما إذا كان يتم تسجيل الحوادث أو الأخطاء وتحليلها وحلها في الوقت المناسب. تهدف إدارة المشكلات إلى حل المشكلات من خلال التحقيق والتحليل المتعمق لحادث كبير أو متكرر بغية تحديد السبب الجذري. بمجرد تحديد المشكلة وإجراء تحليل للسبب الجذري لها، تصبح خطأ أو عدم كفاءة معروفين، ويمكن تطوير حل لمعالجتها ومنع حدوث الحوادث ذات الصلة في المستقبل.

يجب وضع عملية رسمية لتوثيق الظروف التي يمكن أن تؤدي إلى الكشف عن حادثة والتعرف عليها. يتحتم أن يحتوي قسم تشغيل تقنية المعلومات باتفاقية مستوى الخدمة على إجراءات موثقة للكشف عن الحالات غير الطبيعية وتسجيلها. لتسهيل تحليل هذه الظروف غير الطبيعية، غالبًا ما تحتفظ المنظمات بسجلات لجميع الحوادث. يمكن

استخدام سجل يدوي أو آلي لبرنامج تقنية المعلومات المخصص لتسجيل هذه الشروط. يمكن أن تشمل الأمثلة على الحوادث وصول المستخدم غير المصرح به أو التطفل (الأمان)، أو فشل الشبكة (التشغيل)، أو ضعف وظائف البرامج (تقديم الخدمة)، أو الافتقار إلى مهارات المستخدم النهائي (التدريب).

عند تدقيق إدارة الحوادث والمشكلات، يجب على المدقق فحص تقارير وسجلات الحوادث / المشكلات للتأكد من حلها في الوقت المناسب وتخصيصها للأفراد أو المجموعات الأكثر قدرة على حل الحادث / المشكلة. في بعض الحالات، قد يتم استدعاء خطط التعافي من الكوارث لحل إحدى الحوادث. لُطفًا راجع الفصل 6 لمزيد من المعلومات بخصوص خطط التعافي من الكوارث والفصل 7 لإدارة حوادث أمن المعلومات.

ح. إدارة مستوى الخدمة

كما ذكرنا سابقًا، توثق اتفاقية مستوى الخدمة (SLA) المعلمات المختلفة التي تستخدمها مؤسسة تقنية المعلومات لتقديم الخدمة للأعمال. يتم الاتفاق بشكل عام على المعلمات الواردة في اتفاقية مستوى الخدمة من قبل أصحاب الأعمال ومنظمة تقنية المعلومات. سيستخدم المدقق المعلمات في اتفاقية مستوى الخدمة لمعرفة ما إذا كانت مؤسسة تقنية المعلومات تلبي مستويات الخدمة وما إذا كان أصحاب الأعمال راضين ويتخذون الإجراء المناسب إذا كانت ثمة انحرافات عن معايير مستوى الخدمة المتفق عليها. تتضمن هذه المعلمات مقاييس قابلة للقياس الكمي مثل التوافر أو الاستخدام أو عدد الأخطاء. بشكل عام، ثمة أيضًا اتفاقية مستوى الخدمة (SLA) أو اتفاقية رسمية أخرى بين مؤسسة تقنية المعلومات والبائعين التابعين لها. على سبيل المثال، قد يكون لمؤسسة تقنية المعلومات عدة اتفاقيات مستوى الخدمة مع مختلف البائعين الذين يقدمون خدمات الاستعانة بمصادر خارجية أو خدمات الحوسبة السحابية.

قد يكون لدى بعض المنظمات أيضًا اتفاقية بين مؤسسة تقنية المعلومات والعملاء التجاريين داخل المؤسسة، والتي يشار إليها باسم اتفاقية المستوى التشغيلي (OLA). تتشابه OLAs في المحتوى مع اتفاقيات مستوى الخدمة الموضحة أعلاه ولكنها اتفاقيات داخلية قد يحددها مزود الخدمة لوصف كيفية استيفائها لاتفاقيات مستوى الخدمة. يمكن أن يحتوي OLA على معلومات مثل وقت الاستجابة لمعالجة الحوادث أو توفر الخوادم. بشكل عام، يتم استخدام OLAs لتمثيل العلاقات الداخلية بين مزود خدمة تقنية المعلومات وجزء آخر من المؤسسة.

يحتوي SLA و OLA، من بين عناصر أخرى، على مؤشرات الأداء الرئيسة لخدمات تقنية المعلومات. ستساعد مراجعة مؤشرات الأداء الرئيسة المدقق في طرح الأسئلة المتعلقة به

- ما إذا كانت الأنظمة تعمل وفقًا للاتفاقيات الموثقة؛
- ما إذا كانت الآليات موجودة لتحديد الثغرات في الأداء أو الأمن، ومعالجة الثغرات التي تم تحديدها، ومتابعة تنفيذ الإجراءات التصحيحية المتخذة كنتيجة لتقييم أداء المنظمة؛ و
- تحديد قضايا الرقابة في كيان المنظمة الذي يتم تدقيقه وبالتالي المساعدة في تحديد طبيعة وتوقيت ومدى الاختبار.

على سبيل المثال، ترد أدناه مقاييس KPI والتعريفات والأهداف المقابلة لإدارة التغيير:

معالجة	هدف (عامل النجاح الحاسم)	مؤشر الأداء الرئيسي	هندسة القياس
إدارة التغيير	تقليل الحوادث الناتجة عن التغييرات غير المقصودة	النسبة المئوية للانخفاض في عدد الحوادث الناتجة عن الوصول غير المصرح به	يتم تتبعها من خلال إدارة الحوادث وإدارة التغيير والإبلاغ عنها شهريًا

في الحالات التي قد لا توفر فيها مؤشرات الأداء الرئيسة وسيلة للمؤسسة لتقييم التقدم وتحقيق الأهداف بشكل فعال، قد يرغب المدقق في إجراء مزيد من التقييم لمؤشرات الأداء الرئيسة. عند تقييم مؤشرات الأداء الرئيسة، يجب على المدقق تحديد ما إذا كانت تحتوي على سمات مهمة ستساعد في جعلها فعالة في مراقبة التقدم وتحديد مدى نجاح المؤسسة أو البائع في تحقيق أهدافه. تتضمن بعض الأمثلة على هذه السمات ما يلي:

- **الوضوح**. المقياس واضح، والاسم والتعريف يتفقان مع المنهجية المستخدمة لحسابه.
- **هدف قابل للقياس**. المقياس له هدف عددي؛ المقياس قابل للقياس الكمي أو له أهداف قابلة للقياس الكمي أو مقاييس أخرى تسمح بمقارنة الأداء المتوقع بالنتائج الفعلية.
- **الموضوعية**. المقياس خالي بشكل معقول من التحيز أو التلاعب الكبير الذي من شأنه أن يشوه التقييم الدقيق للأداء.
- **الموثوقية**. المقياس ينتج نفس النتيجة في ظل ظروف مماثلة.

- **بيانات خط الأساس والاتجاه**. يحتوي المقياس على بيانات أساسية واتجاه مقترنة به لتحديد التغييرات في الأداء ومراقبتها والإبلاغ عنها وللمساعدة في ضمان عرض الأداء في السياق.
- **الارتباط**. يتماشى التدبير مع أهداف ومهام القسم والمؤسسة ويتم توصيله بوضوح في جميع أنحاء المنظمة.[52]

قد تكون ثمة حالات قامت فيها مؤسسة تقنية المعلومات بالاستعانة بمصادر خارجية لمعظم وظائفها إلى بائع. في مثل هذه الحالة، فإن مؤسسة تقنية المعلومات هي حلقة الوصل بين البائع والمستخدمين وهي مسؤولة عن إدارة البائع لضمان تلبية احتياجات العمل. لُطفًا راجع الفصل 5 لمزيد من المعلومات بخصوص الاستعانة بمصادر خارجية.

i. إدارة الأصول

إدارة الأصول هي عملية تحديد وإنشاء جرد للأصول ذات القيمة الملموسة أو غير الملموسة التي تستحق الحماية وتشمل الأشخاص والمعلومات والبنية التحتية والمالية والسمعة. لا يمكن حماية الأصل أو إدارته بشكل فعال إذا لم يتم تحديده على سبيل المثال. بالإضافة إلى ذلك، تسمح إدارة الأصول للمؤسسات بضمان صيانة أصولها وترقيتها والتخلص منها بشكل صحيح. في الماضي، كان من الأسهل التحكم في الأصول حيث كانت تدار في كثير من الأحيان ضمن نطاق المنظمة، لكن المؤسسات الآن تستعين بمصادر خارجية للخدمات والأصول. تتضمن بعض فوائد إدارة الأصول تحسين الاستخدام، والقضاء على الهدر، وتمكين الإنتاجية، ودعم إدارة استمرارية الأعمال.

ي. إدارة البيانات

إدارة البيانات هي ممارسة إدارة وتأمين البيانات كمورد قيم للمؤسسة. تتطلب إدارة البيانات أن تقوم المؤسسة بجمع البيانات وتخزينها وتأمينها بالإضافة إلى الوصول إلى البيانات ودمجها وتنظيفها لتحليلها. تقوم المنظمات بجمع البيانات من العديد من الموارد، مثل أنظمة المعاملات والماسحات الضوئية وأجهزة الاستشعار والوسائط الاجتماعية والأجهزة الذكية وغيرها. يمكن للمؤسسة استخدام البيانات التي تم جمعها للمساعدة في اتخاذ القرارات وخلق القيمة. تشمل إدارة البيانات أنشطة مثل:

- إنشاء البيانات والوصول إليها وتحديثها
- تخزين البيانات عبر مرافق وسحب متعددة
- ضمان التوافر العالي والتعافي من الكوارث
- استخدام البيانات لدعم التطبيقات والتحليلات والخوارزميات
- ضمان خصوصية البيانات وأمنها
- التخلص من البيانات وفقًا للقوانين واللوائح المعمول بها

تستخدم المنظمات أنظمة إدارة البيانات لإدارة البيانات اللازمة لدعم تحليلات وخوارزميات المنظمة. بينما يتحتم أن يكون لدى المؤسسات أدوات آلية تساعد في إدارة هذه الأنظمة، سيظل مسؤولو قواعد البيانات بحاجة إلى التواجد للتدخل اليدوي.

لإدارة بيانات المنظمة بشكل أفضل، قد تطبق المنظمة ممارسات إدارة البيانات. حوكمة البيانات هي إطار عمل لإدارة بيانات المنظمة. تحتاج المؤسسات إلى تحديد السياسات والإجراءات الخاصة بكيفية إدارة البيانات طوال دورة حياة البيانات بالكامل. ستساعد إدارة البيانات المؤسسات على حماية بياناتها من خلال توثيق أصول البيانات وضوابط الوصول، وتحديد ملكية البيانات والمسؤوليات، وتحديد سياسات التوزيع داخليًا وخارجيًا. تشمل الوظائف الأخرى لإدارة البيانات

- **إدارة هندسة البيانات**، والتي تحدد احتياجات البيانات الخاصة بالمنظمة.
- **تطوير البيانات**، التي تصمم الحلول وتنفذها وتحافظ عليها لتلبية احتياجات البيانات الخاصة بالمنظمة.
- **إدارة عمليات البيانات**، التي تخطط وتحكم وتوفر الدعم للبيانات المنظمة طوال دورة حياة البيانات بالكامل.
- **إدارة أمن البيانات**، والتي تقوم بتنفيذ السياسات والإجراءات الأمنية لضمان سرية البيانات وسلامتها وتوافرها.
- **مستودع البيانات وإدارة ذكاء الأعمال**، والتي توفر عمليات لاتخاذ القرارات لدعم تقارير البيانات والاستعلام والتحليل.

ثالثا. المخاطر على الهيئة الخاضعة للرقابة

[52] لمزيد من المعلومات بخصوص السمات الرئيسة لمؤشرات الأداء الرئيسة، راجع مكتب محاسبة الحكومة الأمريكية، *لوجيستيات الدفاع: مقاييس الأداء المحسنة* والمعلومات *اللازمة لتقييم مبادرات رؤية الأصول*، GAO-17-183، (16 مارس 2017)، https://www.gao.gov/products/gao-17-183.

الأدوات الرئيسة للمدقق، كما لوحظ سابقًا، هي SLA و OLA. تحدد هذه الاتفاقيات المعلمات ومؤشرات الأداء والمتطلبات التي يجب قياس مؤسسة تقنية المعلومات على أساسها. إذا كانت هذه المستندات غير متوفرة أو لم تتم مراجعتها والموافقة عليها رسميًا من قبل مالكي الأعمال (العملية)، فقد تكون موارد تقنية المعلومات الخاصة بالمنظمة معرضة لخطر عدم استخدامها بشكل فعال أو فعال. بعد الحصول على SLA و OLA، سيحتاج المدقق إلى الحصول على تقارير دورية من مؤسسة تقنية المعلومات تقيس حالة المؤشرات وتقريرها بالإضافة إلى مراجعة الإدارة لنفسها وأي عناصر إجراءات أو توجهات إلى منظمة تقنية المعلومات عندما يكون ثمة انحرافات كبيرة عن المعايير المتفق عليها.

في مجال إدارة التغيير، يجب على المدقق التحقق لمعرفة ما إذا كانت ثمة إجراءات للتحكم في التغيير مطبقة تضمن سلامة النظام وتضمن تقديم التطبيقات المعتمدة والمختبرة فقط في بيئة التشغيل.

لابد أن يهتم المدقق أيضًا بكيفية إدارة الوكالة للقدرة (على سبيل المثال، التخزين ووحدة المعالجة المركزية وموارد الشبكة) بطريقة استباقية للاستجابة للمستخدمين وإدارة الحوادث وقضايا الأمان الأخرى بحيث لا يتم المساس بوظائف العمل.

رابعا. المراجع ومزيد من القراءة

أتلاسيان. *ما هي إدارة أصول تقنية المعلومات (ITAM)؟*. https://www.atlassian.com/itsm/it-asset-management. 2022.

أكسلوس. *ما هو ITIL؟*. https://www.axelos.com/best-practice-solutions/itil/what-is-itil.

أكسلوس. *مؤسسة ITIL: ITIL 4 Edition (ITIL 4 Foundation)*. نورويتش: TSO، 2019.

سيشونسكي وبول وتوماس ميلار وتيم جرانس وكارين سكاروني. *منشور NIST الخاص 800-61، مراجعة 2: دليل التعامل مع حوادث أمن الكمبيوتر*. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final. 2012.

CISA. *دليل تطوير العنصر*. https://www.isaca.org/-/media/files/isacadp/project/isaca/certification/cisa/cisa-item-development-guide_bro_eng_0219.pdf. أكتوبر 2018.

سيسكو. *إدارة مستوى الخدمة: المستند التعريفي التمهيدي بأفضل الممارسات*. https://www.cisco.com/c/en/us/support/docs/availability/high-availability/15117-sla.html. 4 أكتوبر 2005.

داما انترناشيونال. *هيئة إدارة البيانات المعرفية*، الطبعة الأولى. https://www.dama.org/cpages/body-of-knowledge. 2010.

إيساكا. *برنامج تدقيق إدارة التغيير*.

إيساكا. *دليل مراجعة CISA*. الطبعة 27. ISACA. https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KokCEAS، 2011.

إيساكا. *إطار عمل COBIT 2019: أهداف الحوكمة والإدارة*. 2019.

نايت، ميشيل. *ما هي إدارة البيانات؟*. https://www.dataversity.net/what-is-data-governance/. 18 ديسمبر 2017.

وحي. *ما هي إدارة البيانات؟*. https://www.oracle.com/database/what-is-data-management/.

محترف. *إدارة البيانات - ماذا ولماذا وكيف ومن وأفضل 15 ممارسة*. https://profisee.com/data-governance-what-why-how-who/.

ساس. *إدارة البيانات: ما هو ولماذا هو مهم*. https://www.sas.com/en_us/insights/data-management/data-management.html.

مكتب محاسبة الحكومة الأمريكية. *تقنية المعلومات: تحتاج الوكالات إلى التنفيذ الكامل لأنشطة تخطيط القوى العاملة الرئيسة*. GAO-20-129. https://www.gao.gov/products/gao-20-129. 30 أكتوبر 2019.

مكتب محاسبة الحكومة الأمريكية. *لوجستيات الدفاع: مقاييس الأداء المحسنة والمعلومات اللازمة لتقييم مبادرات رؤية الأصول*. GAO-17-183. https://www.gao.gov/products/gao-17-183 16 مارس 2017.

الفصل 5: الاستعانة بمصادر خارجية

ماذا يقصد بالاستعانة بمصادر خارجية؟

الاستعانة بمصادر خارجية هي عملية التعاقد مع وظيفة أو خدمة عمل حالية كانت منظمة تؤديها سابقًا داخليًا أو تتعاقد مع وظيفة أو خدمة عمل جديدة مع كيان خارجي. الكيان المتعاقد هو المسؤول عن تقديم الخدمات المطلوبة تعاقديا مقابل رسوم متفق عليها. قد تختار المنظمة الاستعانة بمصادر خارجية لأجزاء محددة (أو كل) من البنية التحتية لتقنية المعلومات أو الخدمات أو العمليات. لابد أن يكون لدى المنظمة سياسة أو رؤية بخصوص وظائف العمل (عادةً ما تكون تقنية المعلومات غير أنه يمكن أن تكون أخرى) فهي تستعين بمصادر خارجية والوظائف التي ستحتفظ بها داخل الشركة.

أ. مزايا الاستعانة بمصادر خارجية

يوفر الاستعانة بمصادر خارجية مزايا معينة، والتي تشمل:

1. مرونة التوظيف

إذا كان المشروع يتطلب مهارات لا تمتلكها المنظمة حاليًا، فقد تقرر المنظمة الاستعانة بمصادر خارجية للمشروع بدلاً من تدريب الموظفين الداخليين - لتوفير الوقت وتكلفة التدريب. بالإضافة إلى ذلك، ستسمح الاستعانة بمصادر خارجية للعمليات التي لها مطالب موسمية أو دورية بجلب موارد إضافية عندما تحتاجها المنظمة، والإفراج عنها عند انتهاء العمليات الموسمية. يمكن أن يكون هذا مفيدًا بشكل خاص في الأسواق المتقلبة حيث يمكن أن تؤدي مرونة التوظيف وإمكانية التوسع إلى تقليل المخاطر.

2. تقليل التكاليف

ينتج عن الاستعانة بمصادر خارجية عادةً خفض التكلفة عن طريق تحويل العمالة والتكاليف الأخرى إلى بائع لديه تكاليف عمالة أقل. تتطلع مؤسسات تقنية المعلومات إلى الاستعانة بمصادر خارجية للمهام التي سيكون إكمالها داخليًا أكثر تكلفة. مثال على هذا النوع من المهام سيكون مهمة متعلقة بالبرمجيات تتطلب مهارات متخصصة. يمكن للمنظمات التي ليس لديها موظفين مؤهلين لإكمال هذه المهمة أن تستفيد مالياً من خلال الاستعانة بمصادر خارجية لهذه المهمة. كما يساعد الاستعانة بمصادر خارجية للعمليات غير الأساسية المنظمة على التركيز على أعمالها الأساسية وتحقيق النتائج بكفاءة.

3. خبراء تحت الطلب

الاستعانة بمصادر خارجية تمكن المنظمة من الحصول على خبراء تحت الطلب ينتظرون المساعدة في القضايا الحالية أو الناشئة. المنظمة قادرة على الاستجابة بسرعة لاحتياجات العمل المتغيرة (على سبيل المثال، مهام جديدة أو القيام بوظائف إضافية) بمساعدة الخبير. بالإضافة إلى ذلك، يمكن للخبراء مساعدة الموظفين الداخليين الذين يعملون جنبًا إلى جنب مع البائع من خلال توفير التدريب العملي ونقل المعرفة.

4. تخفيف المخاطر

خاصة في الأسواق المتقلبة، قد تتطلع المؤسسات إلى التخفيف من المخاطر من خلال زيادة مستويات الاستعانة بمصادر خارجية. على سبيل المثال، يمكن للمؤسسات تقليل موارد تقنية المعلومات والموظفين الذين تحتفظ بهم المنظمة، وبالتالي، الاستعانة بمصادر خارجية لهذه القدرات للسماح بقدر أكبر من المرونة وقابلية التوسع في البيئات المتغيرة باستمرار. قد تقرر مؤسسات تقنية المعلومات الاستعانة بمصادر خارجية لجميع عملياتها أو بعضها، واعتمادًا على مدى أهمية الخدمة الخارجية، يمكن للمؤسسة أن تقرر اتباع ضوابط رسمية أكبر أو أقل على الخدمة الخارجية. من الأهمية بمكان أن نتذكر أن المنظمة تحتفظ بالمسؤولية النهائية عن توفير تلك الوظائف أو الخدمات، لأنها نقلت الوظيفة، وليس المسؤولية.

ب. أمثلة على الاستعانة بمصادر خارجية

وفقًا لـ ISACA،[53] يمكن للمنظمات الاستعانة بمصادر خارجية في مجالات مختلفة من الأعمال والبنية التحتية لتقنية المعلومات. علي سبيل المثال:

- البنية التحتية للتشغيل التي قد تشمل مركز البيانات والعمليات ذات الصلة
- معالجة الطلبات الداخلية من قبل مزود الخدمة
- تطوير الأنظمة أو صيانة التطبيقات
- تثبيت وصيانة وإدارة الحوسبة المكتبية والشبكات المرتبطة بها

تعد **الحوسبة السحابية** واحدة من أكثر خدمات تقنية المعلومات التي يتم الاستعانة بمصادر خارجية لها شيوعًا اليوم. تعد الحوسبة السحابية نموذجًا لتمكين الوصول إلى الشبكة عند الطلب لمجموعة من موارد الحوسبة القابلة للتكوين (مثل التطبيقات والشبكات والخوادم والتخزين والخدمات الأخرى). من بين المزايا الأخرى، يمكن للحوسبة السحابية تمكين المؤسسات من الوصول إلى موارد الحوسبة على أساس الدفع لكل استخدام وتوفير المرونة في القدرة على توسيع نطاق حل تقنية المعلومات بسرعة.

كمثال، يمكن للمؤسسة الاستعانة بمصادر خارجية لمعالجة البيانات أو خدمة أخرى لموارد الحوسبة التي يمتلكها البائع. عادةً ما يستضيف البائع المعدات، بينما لا تزال المنظمة تتحكم في التطبيق والبيانات. قد تتضمن الحوسبة السحابية أيضًا استخدام أجهزة كمبيوتر البائع لتخزين بيانات المؤسسة ونسخها احتياطيًا وتوفير الوصول عبر الإنترنت إلى بيانات المؤسسة. ستحتاج المنظمة إلى وصول قوي إلى الإنترنت إذا أرادت لموظفيها أو مستخدميها الوصول بسهولة إلى البيانات أو حتى التطبيق الذي يعالج البيانات. في البيئة الحالية، تتوفر البيانات أو التطبيقات أيضًا من الأنظمة الأساسية للجوّال (على سبيل المثال، أجهزة الكمبيوتر المحمولة المزودة باتصالات الإنترنت اللاسلكية أو البطاقات الخلوية / المحمولة والهواتف الذكية والأجهزة اللوحية).

غالبًا ما يتم تصنيف الحوسبة السحابية إلى ثلاثة نماذج خدمة منفصلة:

- **البرامج كخدمة** - تستخدم المنظمة تطبيقًا وبنية أساسية يوفرها البائع.
- **النظام الأساسي كخدمة** - تستخدم المؤسسة البنية التحتية السحابية التي يوفرها البائع لتشغيل التطبيقات التي يمتلكها البائع.
- **البنية التحتية كخدمة** - تقوم المؤسسة بتعهيد موارد الحوسبة المتنوعة إلى بائع مثل المعالجة والتخزين والشبكات من البائع. لا تدير المنظمة البنية التحتية، ولكنها تتحكم في التطبيق ونظام التشغيل المستخدم.

بالإضافة إلى نماذج الخدمة المختلفة، ثمة أربعة نماذج نشر منفصلة:

- **السحابة الخاصة** - يتم توفير البنية التحتية للاستخدام الحصري من قبل مؤسسة واحدة.
- **سحابة المجتمع** - يتم توفير البنية التحتية السحابية لمجتمع المستهلكين الذين غالبًا ما يكون لديهم اعتبارات مشتركة، مثل اعتبارات المهمة والأمان والامتثال.
- **السحابة العامة** - يتم توفير البنية التحتية للاستخدام المفتوح من قبل عامة الناس ويتم تشغيلها عادةً بواسطة مؤسسة تجارية أو أكاديمية أو حكومية.
- **السحابة المختلطة** - البنية التحتية عبارة عن تكوين من اثنين أو أكثر من البنى التحتية المذكورة سابقًا والتي يمكن تشغيلها بشكل متبادل لتمكين إمكانية نقل البيانات والتطبيقات.

يمكن أن يقلل التكوين السحابي المناسب من مخاطر المخاوف الأمنية ويمكن أن يؤدي تطبيق ضوابط أمنية إضافية إلى إنشاء بيئة سحابية يمكن الدفاع عنها. بالإضافة إلى ذلك، يستلزم أن تتضمن عقود الحوسبة السحابية بندًا يتعلق بعدم الكشف عن البيانات الحساسة وتحتاج إلى تحديد ما يشكل خرقًا للأمن ووصف كيفية قيام البائع بإخطار المنظمة بالخرق.

بإيجاز، يمكن للحوسبة السحابية أن تقدم فوائد للمؤسسة، مثل احتواء التكلفة والتزويد الفوري والمرونة الديناميكية وقابلية التوسع وحلول النسخ الاحتياطي للحد من وقت التوقف عن العمل. ومع ذلك، مثل كل التعهيد الخارجي، فإن الحوسبة السحابية تنطوي على مخاطر وتحديات عند تنفيذها. على سبيل المثال، يمكن أن تقدم الحوسبة السحابية مخاطر إضافية، مثل التهيئة الخاطئة وسوء فهم المسؤوليات المشتركة وضوابط الوصول الضعيفة والموارد السحابية المشتركة مع المستأجرين الآخرين لمزود الخدمة السحابية ونقاط الضعف في سلسلة التوريد. يمكن أن يصبح نموذج التكلفة المرن للحوسبة السحابية مكلفًا للغاية إذا لم تراقب المنظمة وتتحكم في استخدامها.

ثانيًا. عناصر الاستعانة بمصادر خارجية

[53] برنامج تدقيق / ضمان بيئات تقنية المعلومات الخارجية (2009).

أ. سياسة الاستعانة بمصادر خارجية

تحتاج المنظمات إلى سياسة تحدد الوظائف التي يمكن الاستعانة بمصادر خارجية والوظائف التي يستلزم أن تظل داخلية.[54] عادةً ما تقوم المؤسسات بالاستعانة بمصادر خارجية لعمليات تقنية المعلومات الروتينية والصيانة ومنصات أجهزة سطح المكتب. تعد سجلات الموارد البشرية والموظفين بشكل عام وظائف داخلية لأنها تتطلب مراقبة دقيقة وتخضع للعديد من متطلبات الخصوصية والأمان التي قد لا تجعلها فعالة من حيث التكلفة للاستعانة بمصادر خارجية.

يستلزم أن يبدأ المدقق بمراجعة سياسة التعهيد وإجراءات المنظمة. من الضروري أن يكون لدى المؤسسات الكبرى، التي غالبًا ما يكون لديها حصة كبيرة من عملياتها التجارية التي يتم الاستعانة بمصادر خارجية لها، سياسة تعهيد معتمدة تتضمن تحديدًا واضحًا لعمليات الاستعانة بمصادر خارجية. قد لا يكون للمنظمات الصغيرة سياسة رسمية غير أنه يقتضي أن تتبع إجراءات التماس تتسم بالكفاءة والشفافية. بغض النظر عن الحجم، يقتضي أن يكون لدى المنظمات استراتيجية حوكمة واضحة بغية تحديد الاتجاه والأهداف للاستعانة بمصادر خارجية.

ب. الإغراء

طلب تقديم العروض هو عملية توثيق متطلبات النظام وجمع المواد المرجعية الأخرى التي ستساعد البائع في بناء النظام. يتضمن إنشاء حزمة الالتماس وطرحها للمناقصة / العطاء، والحصول على العروض، والاختيار بين مختلف البائعين. يقتضي أن تكون عملية الاختيار شفافة وموضوعية وتستند إلى معايير مناسبة للنظام أو الخدمات التي يتم الحصول عليها. قبل اتخاذ القرار النهائي، يجب على المنظمة مراجعة البائع المحتمل بدقة بحثًا عن أي مشكلات أو عوائق محتملة أمام تقديم الخدمة.

ج. إدارة البائعين

تعد إدارة البائعين عنصرًا أساسيًا في الاستعانة بمصادر خارجية لضمان تقديم الخدمات وفقًا لتوقعات المنظمة. يقتضي أن يكون لدى المنظمة عمليات لضمان المتابعة الدورية فيما يتعلق بحالة المشروع، وجودة الخدمة، واختبار المنتجات المبنية قبل إدخالها في بيئة التشغيل. بالإضافة إلى ذلك، كجزء من عملية مراقبة البائعين، قد تقوم المنظمة أيضًا بمراجعة عملية ضمان الجودة الداخلية للمورد للتأكد من أن موظفي البائع يتبعون السياسات والخطط المعتمدة تعاقديًا لجميع أعمالهم.

عنصر مهم في إدارة البائعين هو جيش تحرير السودان. كما ذكرنا سابقًا، اتفاقية مستوى الخدمة (SLA) هي اتفاقية موثقة بين المؤسسة والمورد وهي أداة رئيسية لإدارة البائعين. يجب أن تحدد اتفاقية مستوى الخدمة (SLA) الخدمات التي من المتوقع أن يؤديها البائع بالإضافة إلى المعلمات الفنية لتلك الخدمات نظرًا لأنها اتفاقية ملزمة قانونًا بين البائع والمؤسسة.

من منظور إدارة البائعين، تشمل المجالات النموذجية التي تغطيها اتفاقية مستوى الخدمة

- أنواع الخدمات التي سيقدمها البائع؛
- توزيع المسؤوليات بين المنظمة والبائع؛
- الخدمات التي سيتم قياسها، وفترة القياس، والمدة، والموقع، والجداول الزمنية لإعداد التقارير (على سبيل المثال، معدلات العيوب، ووقت الاستجابة، وساعات التوظيف في مكتب الدعم)؛
- الوقت لتنفيذ وظائف جديدة ومستويات إعادة العمل؛
- مستوى حقوق الوصول الممنوحة للبائع لأداء خدماتهم؛
- نوع الوثائق المطلوبة للتطبيقات التي وضعها البائع؛
- الموقع الذي ستؤدى فيه الخدمات؛
- تواتر معاملات النسخ الاحتياطي واستعادة البيانات؛
- طرق وصيغ الإنهاء وإيصال البيانات؛
- عملية الإبلاغ المنتظمة ومشاركة معلومات الحوادث / المشاكل؛ و

---

[54] المنظمة الدولية للتوحيد القياسي / اللجنة الكهروتقنية الدولية، *تقنية المعلومات - الحوسبة السحابية - إرشادات لتطوير السياسات* (جنيف، سويسرا: المنظمة الدولية للتوحيد القياسي، يناير 2019).

- شروط الحوافز والجزاءات.

بالنسبة لاتفاقيات مستوى الخدمة الخاصة بالحوسبة السحابية، يمكن للمؤسسة دمج عدد من الممارسات في العقود للمساعدة في ضمان أداء خدمات الحوسبة السحابية بفعالية وكفاءة وأمان.[55] وتشمل هذه

- تحديد مقاييس الأداء مثل مستوى الخدمة (على سبيل المثال، المدة)، ومستوى السعة (على سبيل المثال، الحد الأقصى لعدد المستخدمين)، ووقت الاستجابة (على سبيل المثال، مدى سرعة معالجة المعاملة)؛
- تحديد كيف ومتى يمكن للمؤسسة الوصول إلى البيانات والشبكات الخاصة بها التي يستضيفها البائع، خاصة عند إنهاء العقد؛
- تحديد كيفية قيام موفر السحابة بمراقبة الأداء ومتى ستقوم المؤسسة بمراجعة الأداء؛
- تحديد مقاييس الأمان، مثل من يمكنه الوصول إلى البيانات ووسائل الحماية بخصوص البيانات؛ و
- تحديد الإخطار الذي سيحدث أثناء خرق الاتفاقية.

بإيجاز، يجب وضع معظم العناصر التي تعتبر بالغة الأهمية بالنسبة للمنظمة في اتفاقية مستوى الخدمة (SLA). يحتاج مدقق تقنية المعلومات إلى طلب اتفاقية مستوى الخدمة أو أي مستند آخر (عقد أو اتفاقية رسمية) حيث يتم توثيق هذه المعلمات. سيحتاج المدقق إلى النظر في ما إذا كانت المنظمة قد حددت متطلباتها للوظيفة التي يتم الاستعانة بمصادر خارجية لها قبل اختيار البائع (على سبيل المثال، المتطلبات المحددة والمعايير التشغيلية موجودة في العقد واتفاقية مستوى الخدمة)، ما إذا كانت المنظمة تراقب هذا البائع في بالمتطلبات المنصوص عليها في اتفاقية مستوى الخدمة (عبر تقارير الحالة الدورية)، وإذا كانت المنظمة قد اتخذت إجراءً عندما لا يفي البائع بمعايير اتفاقية مستوى الخدمة المنصوص عليها (أي الإجراءات التصحيحية أو غرامات الدفع).

د. تحليل التكاليف والفوائد

يمكن للمنظمات الاستعانة بمصادر خارجية لتحقيق وفورات في التكاليف. يتم تحقيق ذلك عندما تكون تكلفة تقديم هذه الخدمات أرخص من البائع من استخدام العمالة الداخلية أو البنية التحتية. ثمة فوائد أخرى لا يمكن قياسها بشكل مباشر، مثل الاستفادة من البنية التحتية للبائع لتوسيع مستوى الخدمة بسرعة أو استخدام خبرته في حالات خاصة. كلما كان ذلك ممكنًا، يجب أن تحاول المنظمة تحديد ما إذا كانت الوفورات المتوقعة تتحقق على أساس دوري. هذا التحديد كأحد نقاط البيانات لتقرير ما إذا كان سيتم الاستمرار أو التوقف مع القدرة الاستعانة بمصادر خارجية.

هـ. حماية

أثناء الاستعانة بمصادر خارجية، يجب على مؤسسات تقنية المعلومات تقييم ما إذا كان لدى البائعين ممارسات أمنية قوية بما فيه الكفاية وما إذا كان بإمكان البائعين تلبية متطلبات الأمن الداخلي. في حين أن معظم مؤسسات تقنية المعلومات تجد ممارسات أمان البائع مثيرة للإعجاب (غالبًا ما تتجاوز الممارسات الداخلية)، إلا أن مخاطر الانتهاكات الأمنية أو حماية الملكية الفكرية تزداد بطبيعتها من خلال حقيقة أن البيانات قد تم الاستعانة بمصادر خارجية لها. يجب أيضًا معالجة مخاوف الخصوصية. تشمل المخاوف الأمنية الأخرى احتمال إساءة التعامل أو الكشف عن البيانات الحساسة، والوصول غير المصرح به إلى البيانات والتطبيقات وخطة التعافي من الكوارث. على الرغم من أن هذه القضايا نادرًا ما تشكل عوائق كبيرة أمام الاستعانة بمصادر خارجية، يجب توثيق المتطلبات.

يزيد استخدام الحوسبة السحابية أيضًا من الحاجة إلى ممارسات أمان قوية نظرًا لطبيعة ميزاتها. تتضمن بعض المخاوف الأمنية الاعتماد على أطراف ثالثة، وزيادة تعقيد الامتثال للقوانين واللوائح (في بعض الحالات عبر بلدان متعددة)، والاعتماد على الإنترنت كقناة أساسية للبيانات، والطبيعة الديناميكية للحوسبة السحابية (على سبيل المثال، متعددة مواقع المعالجة). تم تضمين مزيد من المعلومات بخصوص هذه المخاوف والمخاطر ذات الصلة لاحقًا في هذا الفصل.

يتم تدقيق بعض البائعين أو المؤسسات الخدمية بشكل مستقل نظرًا لحجمهم وعدد المنظمات المتعاقد عليها وسيكون لها تقرير مراقبة منظمة الخدمة، والذي سيدرج ضوابط أمن المعلومات وفعاليتها. تتضمن هذه التقارير تقييمًا مستقلاً للمورد أو ضوابط مؤسسات الخدمة التي يمكن أن تشمل الضوابط الداخلية والضوابط المتعلقة بالأمان والتوافر والنزاهة والسرية. يمكن للمراجع أن يطلب هذا التقرير من خلال المنظمة.

---

[55] المنظمة الدولية للتوحيد القياسي / اللجنة الكهرتقنية الدولية *ISO / IEC 19086-1، تقنية المعلومات - الحوسبة السحابية - إطار اتفاقية مستوى الخدمة (SLA) - الجزء 1: نظرة عامة ومفاهيم* (15 سبتمبر 2016)، https://www.iso.org/standard/67545.html ومكتب محاسبة الحكومة الأمريكية، *الحوسبة السحابية: تحتاج الوكالات إلى دمج الممارسات الأساسية لضمان الأداء الفاعل*، GAO-16-325، (7 أبريل 2016)، https://www.gao.gov/products/GAO-16-325.

ثالثا. المخاطر على الهيئة الخاضعة للرقابة

أ. الاحتفاظ بالمعرفة التجارية وامتلاك عملية الأعمال

ثمة مخاطر متأصلة تتمثل في فقدان المعرفة التجارية، والتي تقع داخل مطوري التطبيقات. إذا كان البائع غير قادر على تقديم هذه الخدمة، فيجب أن تكون مؤسسات تقنية المعلومات مستعدة لتولي هذا الواجب مرة أخرى. أيضًا، نظرًا لأن تطوير التطبيق يحدث خارج المنظمة، فإن المنظمة أيضًا تخاطر بالتنازل عن ملكية العملية التجارية أو فقدانها، والتي قد يطالب بها مزود الخدمة باعتبارها ملكيتها الفكرية. تحتاج المؤسسات إلى معالجة هذه المشكلة في وقت إبرام العقد، والتأكد من أن لديها وثائق كاملة لعملية تطوير النظام بالإضافة إلى تصميمات النظام. من الضروري أن تكون حزمة الالتماس المرسلة إلى البائع متوافقة مع التخطيط الاستراتيجي للمؤسسة، وأن تكون محددة بوضوح ومفصلة حتى لا تكون ثمة شكوك أو عدم دقة أو عدم وضوح بشأن المتطلبات. سيساعد هذا أيضًا المنظمة على التبديل بين مقدمي الخدمة، إذا لزم الأمر.

ب. فشل البائع في التسليم

قد يفشل البائع في تسليم المنتج في الوقت المحدد أو يجب التخلي عن المنتج بسبب نقص الوظائف الصحيحة. إذا لم يتم تنفيذ عملية الاستعانة بمصادر خارجية بشكل صحيح، فثمة احتمال كبير بأن النظام أو الخدمات التي يتم الحصول عليها قد لا تلبي احتياجات المستخدم، أو أن تكون دون المستوى المطلوب، أو تكلف أكثر، أو تتطلب موارد كبيرة للصيانة والتشغيل، أو قد تكون ذات جودة رديئة أنه سيتعين استبداله في المستقبل القريب. يعد العقد السيئ، ونظام اختيار البائع المعيب، والمعالم غير الواضحة، وظروف السوق غير المواتية من الأسباب الشائعة لفشل البائع.

تحتاج مؤسسات تقنية المعلومات إلى خطط طوارئ لمثل هذا الحدث. عند التفكير في الاستعانة بمصادر خارجية، يجب على مؤسسات تقنية المعلومات تقييم الآثار المترتبة على فشل البائع (على سبيل المثال، هل الفشل له آثار مهمة على أداء الأعمال؟). إن توافر الوثائق التفصيلية بخصوص تصميم النظام وتطوير النظام سيساعد المنظمة في ضمان استمرارية الأعمال من خلال مزود خدمة آخر أو من تلقاء نفسها.

ج. عدم وجود موظفين منظمين على استعداد لإدارة عقود الاستعانة بمصادر خارجية

يجب أن تعد المنظمة وتحافظ على موظفين مؤهلين قادرين على تنفيذ الإدارة الصحيحة لعقود الاستعانة بمصادر خارجية. إذا لم يكن لديها عدد كافٍ من الموظفين المؤهلين، أثناء تنفيذ العقد بالكامل، يجوز للمنظمة الخاضعة للتدقيق دفع مبالغ زائدة للبائع أو عدم الحصول على النتائج المتوقعة أو فشل الاستعانة بمصادر خارجية تمامًا. بالإضافة إلى ذلك، من مصلحة المؤسسات أن تخلق بيئة تنافسية للعقود التي يتم فيها تقييم الموردين وتعظيمهم باستمرار. بدون مؤسسات الرقابة المناسبة لن تكون قادرة على زيادة المرونة والسيطرة على خدمات تقنية المعلومات الخاصة بهم.

د. تقديرات التكلفة والجدول غير دقيقة

تحتوي جميع عقود الاستعانة بمصادر خارجية على أسس وافتراضات. إذا اختلف العمل الفعلي عن التقديرات، سيدفع العميل الفرق. لقد أصبح هذا عقبة رئيسية لمؤسسات تقنية المعلومات التي تفاجأ بأن السعر لم يكن "ثابتًا" (على سبيل المثال، لموارد الحوسبة السحابية) أو أن البائع يتوقع أن يتم الدفع له مقابل تغييرات النطاق الإضافية. بالإضافة إلى ذلك، غالبًا ما تخلق المؤسسات حالات عمل مفرطة في التفاؤل أو غير واقعية يمكن أن تسبب زحفًا كبيرًا في النطاق خلال تكامل الخدمات التي يتم الاستعانة بمصادر خارجية لها.

هـ. دوران الموظفين الرئيسيين

أدى النمو السريع بين البائعين الخارجيين إلى خلق سوق عمل ديناميكي. عادة ما يكون الموظفون الرئيسيون مطلوبين لمشاريع جديدة رفيعة المستوى، أو حتى معرضين لخطر التوظيف من قبل بائعين آخرين في الخارج. في حين أن البائعين في الخارج غالبًا ما يستشهدون بإحصائيات دوران إجمالي تبدو منخفضة نسبيًا، إلا أن الإحصاء الأكثر أهمية الذي يجب إدارته هو معدل دوران الموظفين الرئيسيين في الحساب. تتراوح مستويات الدوران الشائعة بين 15 و 20 بالمائة، ويعد إنشاء شروط تعاقدية بخصوص هذه المستويات طلبًا معقولاً.

و. المخاطر الخارجية

يعد توظيف موفري الخدمات في الخارج شكلاً شائعًا من أشكال الاستعانة بمصادر خارجية، خاصة في بيئة الحوسبة السحابية. في هذا السيناريو، قد تنطوي المخاطر التي يتعرض لها مثل هذا الاستعانة بمصادر خارجية على لوائح أجنبية بشأن تخزين المعلومات ونقلها قد تحد مما يمكن تخزينه وكيف يمكن معالجته، ويمكن استخدام البيانات من قبل تطبيق القانون في بلد أجنبي دون معرفة المنظمة والخصوصية ومعايير الأمن قد لا تكون متناسبة دائمًا، ولا يمكن تجنب النزاعات بسبب الاختصاصات القانونية المختلفة تمامًا.

ز. أمن المعلومات

يمكن أن تجلب الاستعانة بمصادر خارجية مجموعة متنوعة من مخاطر أمن المعلومات، مثل سوء التعامل أو الكشف عن البيانات الحساسة أو الوصول غير المصرح به إلى البيانات، كما ذكرنا سابقًا. علاوة على ذلك، فإن تأثير الأعمال والمخاطر المرتبطة باستخدام خدمات الحوسبة السحابية تشمل المجالات والعمليات التالية:

- زيادة الاعتماد على الأطراف الثالثة، مما قد يؤدي إلى زيادة المخاطر بسبب
  - نقاط الضعف في الواجهات الخارجية،
  - مراكز البيانات المجمعة،
  - الاعتماد على عمليات التأكيد المستقلة، و
  - المؤسسات التي لم تعد تمتلك البيانات أو تشرف على الضوابط المستخدمة من قبل أطراف ثالثة؛
- التعقيد المتزايد للامتثال للقوانين واللوائح، مع آثار على
  - قدرًا أكبر من مخاطر الخصوصية،
  - التدفق عبر الحدود لمعلومات التعريف الشخصية، و
  - الامتثال التعاقدي
- الاعتماد على الإنترنت باعتباره القناة الأساسية لبيانات المؤسسة، والذي يقدم
  - القضايا الأمنية المرتبطة بالبيئة العامة و
  - مشاكل الاتصال بالإنترنت وتوافرها؛
- الطبيعة الديناميكية للحوسبة السحابية، بما في ذلك احتمالية ذلك
  - قد يتغير موقع مرافق المعالجة وفقًا لموازنة الحمل،
  - قد تقع مرافق المعالجة عبر الحدود الدولية،
  - يمكن مشاركة مرافق التشغيل مع المنافسين، و
  - القضايا القانونية (المسؤولية، الملكية، إلخ) المتعلقة بالقوانين المختلفة في البلدان المضيفة قد تعرض البيانات للخطر؛
- مخاطر حوكمة تقنية المعلومات مثل
  - فقدان إدارة تقنية المعلومات والتحكم فيها من قبل المؤسسة عند استخدام الخدمات السحابية،
  - أقل تفاعل لأمر العميل مقارنة بالتزويد الداخلي للخدمة، و
  - نقص الدعم الداخلي بسبب الثقافة التنظيمية وتصور العملاء للمخاطر الأكبر المرتبطة بالخدمات السحابية؛ و
- المخاطر المتعلقة بالمراجعة مثل
  - عدم القدرة على الوصول إلى سجلات النظام والأمان من أطراف ثالثة،
  - الخسارة أو عدم اكتمال توفير المعلومات من المزود للعميل فيما يتعلق بالحوادث الأمنية وتوفير مسارات المراجعة، و
  - عدم وجود عزل لبيانات السجل بين العملاء المختلفين أو تسريب بيانات السجل الأخرى.

ح. قفل البائع

قفل البائع هو مشكلة تحدث في الاستعانة بمصادر خارجية عندما يصبح العثور على بائع جديد أو نقل العمليات داخل الشركة مكلفًا للغاية. يمكن أن يحدث هذا بسبب قيام المؤسسات بتقديم مساهمات كبيرة لمنتج أو خدمة فريدة مقدمة من قبل البائع، ولكن فقط كونها قادرة على استخدام المنتج أو الخدمة مع البائع الحالي. يمكن أن يكون هذا مزعجًا بشكل خاص في بيئة السحابة، حيث قد يتطلب نقل البيانات إلى نوع مختلف من البيئة إعادة تنسيق البيانات. بالإضافة إلى ذلك، قد تصبح المؤسسات معتمدة على البرنامج الذي تستخدمه مع موفر خدمة سحابي معين ولن تتمكن بسهولة من تغيير البائعين. يمكن للمؤسسات تقليل مخاطر قفل البائع من خلال تقييم الخدمات السحابية بعناية، والتأكد من إمكانية نقل البيانات بسهولة، وإجراء نسخ احتياطية وظيفية للبيانات، واستخدام خدمات سحابية مختلفة عبر مزودين متعددين.

رابعا. المراجع والقراءات الإضافية

المحكمة الفيدرالية للحسابات، TCU (SAI Brazil). *تقرير النقاط البارزة: الحوسبة السحابية*. https://portal.tcu.gov.br/en_us/biblioteca-digital/report-highlights-cloud-computing.htm . 15 يوليو 2015.

المنظمة الدولية للتوحيد القياسي / اللجنة الكهروتقنية الدولية. *ISO / IEC، 2016 :1-19086، تقنية المعلومات - الحوسبة السحابية - إطار اتفاقية مستوى الخدمة (SLA) - الجزء 1: نظرة عامة ومفاهيم*. https://www.iso.org/standard/67545.html . 15 سبتمبر 2016.

المنظمة الدولية للتوحيد القياسي / اللجنة الكهروتقنية الدولية. ISO / IEC، *19086-2: 2018، الحوسبة السحابية - إطار اتفاقية مستوى الخدمة (SLA) - الجزء 2: نموذج متري*. جنيف، سويسرا: المنظمة الدولية للتوحيد القياسي، ديسمبر 2018.

المنظمة الدولية للتوحيد القياسي / اللجنة الكهروتقنية الدولية. ISO / IEC، *TR 22678: 2019، تقنية المعلومات - الحوسبة السحابية - إرشادات لتطوير السياسات*. جنيف، سويسرا: المنظمة الدولية للتوحيد القياسي، يناير 2019.

المنظمة الدولية للتوحيد القياسي / اللجنة الكهروتقنية الدولية. ISO / IEC، *27036-1: 2014، تقنية المعلومات - تقنيات الأمان - أمن المعلومات للعلاقات مع الموردين - الجزء 1: نظرة عامة ومفاهيم*. جنيف، سويسرا: المنظمة الدولية للتوحيد القياسي، 1 أبريل 2014.

المنظمة الدولية للمقاييس. *ISO 37500: 2014، إرشادات بخصوص الاستعانة بمصادر خارجية*. جنيف، سويسرا: المنظمة الدولية للتوحيد القياسي 11 نوفمبر 2014.

المعهد الوطني للمعايير والتقنية. *المنشور الخاص 500-292: العمارة المرجعية للحوسبة السحابية*. http://www.nist.gov/customcf/get_pdf.cfm?pub/. 5Fid=909505 سبتمبر 2011.

المعهد الوطني للمعايير والتقنية. *المنشور الخاص 800-144: إرشادات بخصوص الأمان والخصوصية في الحوسبة السحابية العامة*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf. ديسمبر 2011.

المعهد الوطني للمعايير والتقنية. *المنشور الخاص 800-145: تعريف NIST للحوسبة السحابية*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. سبتمبر 2011.

وكالة الأمن القومي. *التخفيف من ثغرات السحابة*. https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/csi-mitigating-cloud-vulnerabilities_20200121.pdf. 22 يناير 2020.

مجلس الخزانة من أمانة كندا. *دليل اتفاقيات الخدمة: العناصر الأساسية*. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25761§ion=html. 4 يوليو 2012.

مكتب محاسبة الحكومة الأمريكية. *حوسبة سحابية: تحتاج الوكالات إلى دمج الممارسات الرئيسة لضمان الأداء الفاعل*. GAO-16-325. https://www.gao.gov/products/GAO-16-325. 7 أبريل 2016.

الفصل 6: إدارة استمرارية العمل

ما هي إدارة استمرارية الأعمال؟

يعد توافر أنظمة تقنية المعلومات وعملياتها الصحيحة أمرًا بالغ الأهمية لقدرة المؤسسات الحكومية على الوفاء بالتزاماتها القانونية. تلعب هذه الأنظمة دورًا مهمًا في أنشطة متنوعة مثل تقييم وتحصيل الضرائب والإيرادات الجمركية؛ دفع معاشات الدولة ومزايا الضمان الاجتماعي؛ وفي معالجة الإحصاءات الوطنية (مثل المواليد والوفيات والجريمة والأمراض). في الواقع، لا يمكن تنفيذ العديد من الأنشطة بفعالية - إن وجدت - بدون دعم نظم المعلومات. بغية الحد من تعطيل وتعطل هذه الأنظمة، يجب على المنظمات تطوير استراتيجية التخطيط المستمر والإجراءات المرتبطة بها.

غالبًا ما تكون الكوارث والأزمات الأخرى بطبيعتها أحداثًا غير متوقعة. في حين أنه لا يمكن تجنب كل هذه الأحداث، إلا أن التخطيط المستمر يمكن أن يحد في كثير من الأحيان من تأثير هذه الأحداث غير المتوقعة. يمكن أن يكون لفقدان الطاقة، والإجراءات الصناعية، والحرائق، والأضرار الكيدية آثار كارثية على أنظمة المعلومات. قد يستغرق الأمر عدة أسابيع حتى تستأنف المنظمة عملياتها التجارية الفاعلة إذا لم يكن لديها خطة استمرارية عملية مطبقة. بالإضافة إلى ذلك، غالبًا ما يتم الاستعانة بمصادر خارجية للعديد من عمليات تقنية المعلومات لمقدمي الخدمات الخارجيين. إذا تعطلت العمليات في مزود خدمة خارجي بسبب كارثة، فقد يكون لها أيضًا تأثير كارثي على المنظمة.

بغية منع الانقطاعات المحتملة للخدمة من المخاطر المعروفة، يجب على المؤسسات إجراء العديد من أنشطة إدارة استمرارية الأعمال للمساعدة في منع انقطاع الخدمة، بما في ذلك **التخطيط لاستمرارية الأعمال، وتخطيط التعافي من الكوارث، والتخطيط للطوارئ لنظام المعلومات**، من بين أمور أخرى. يُستخدم المصطلحان "تخطيط استمرارية الأعمال" و "التخطيط لاستعادة القدرة على العمل بعد الكوارث" في بعض الأحيان بشكل مترادف، لكنهما في الحقيقة مصطلحان مختلفان ولكنهما متكاملان. كلاهما مهم لمدقق تقنية المعلومات، لأنهما يضمنان معًا أن المنظمة قادرة على العمل بقدرة محددة بعد حدوث خلل طبيعي أو من صنع الإنسان. تخطيط طوارئ نظام المعلومات مشابه لتخطيط التعافي من الكوارث، لكنه يركز على استعادة النظام بغض النظر عن موقع النظام. يتم شرح الشروط بمزيد من التفصيل أدناه:

- **تخطيط استمرارية الأعمال** هو العملية التي تستخدمها المنظمة لتخطيط واختبار استعادة عملياتها التجارية بعد حدوث اضطراب. كما يصف أيضًا كيف ستستمر المنظمة في العمل في ظل الظروف المعاكسة التي قد تنشأ (على سبيل المثال، الكوارث الطبيعية أو غيرها من الكوارث، أو حتى في غياب الموظفين الرئيسيين). الهدف النهائي لتخطيط استمرارية الأعمال هو أن تنشئ المنظمة أكثر المنظمات مرونة. وهذا يشمل المهام الحيوية المستمرة للمهمة في جميع الأوقات خلال أي نوع من الكوارث أو الاضطراب.
- **تخطيط التعافي من الكوارث** هو عملية التخطيط والاختبار لاستعادة البنية التحتية لتقنية المعلومات بعد وقوع كارثة طبيعية أو كارثة أخرى. إنه مكمل لتخطيط استمرارية الأعمال. ينطبق تخطيط استمرارية الأعمال على وظائف الأعمال التنظيمية بينما ينطبق تخطيط التعافي من الكوارث على البنية التحتية لتقنية المعلومات التي تدعم وظائف الأعمال.
- **التخطيط للطوارئ لنظام المعلومات** هو عملية التخطيط والاختبار لاستعادة أنظمة المعلومات الفردية. هذا أيضًا مكمل لتخطيط استمرارية الأعمال ويعالج استعادة نظام واحد. من المفترض أن يكون التخطيط للطوارئ لنظام المعلومات بمثابة دليل لاستعادة النظام ويمكن تنشيطه لهذا النظام بغض النظر عن الموقع.

في جوهرها، تتناول **خطة استمرارية الأعمال (BCP)** قدرة المنظمة على مواصلة العمل عندما تتعطل العمليات العادية. تتضمن هذه الخطة السياسات والإجراءات والممارسات التي تسمح للمؤسسة باستعادة واستئناف العمليات اليدوية والآلية ذات المهام الحرجة بعد وقوع كارثة أو أزمة. إلى جانب ذكر الممارسات التي يجب اتباعها في حالة الانقطاع، تتضمن بعض خطط استمرارية العمل مكونات أخرى، مثل التعافي من الكوارث والاستجابة للطوارئ واستعادة المستخدم والطوارئ وطوارئ نظام المعلومات وأنشطة إدارة الأزمات. على هذا النحو، في هذه المنظمات، يُنظر إلى تخطيط استمرارية الأعمال على أنه عملية شاملة تغطي كلاً من التعافي من الكوارث واستئناف أنشطة الأعمال.

بيد أنه، سواء كجزء من خطة العمل الأساسية أو وثيقة منفصلة، يجب أن تحدد **خطط التعافي من الكوارث (DRP)** الموارد والإجراءات والمهام والبيانات المطلوبة لإدارة عملية استرداد المؤسسة في حالة انقطاع الأعمال. يجب أن تساعد هذه الخطة أيضًا المنظمة عند استعادة العمليات التجارية المتأثرة، من خلال تحديد الخطوات المحددة التي يجب على المنظمة اتخاذها في طريقها نحو التعافي. على وجه التحديد، يتم استخدام DRP للإعداد والتخطيط المتقدم اللازمين لتقليل أضرار الكوارث ولضمان توافر أنظمة المعلومات الهامة للمنظمة. فيما يتعلق بتقنية المعلومات، يعالج DRPs استرداد أصول التقنية الهامة، بما في ذلك الأنظمة والتطبيقات وقواعد البيانات وأجهزة التخزين وموارد الشبكة الأخرى.[56]

---

[56] Iia.org. *دور مدقق تقنية المعلومات في إدارة استمرارية الأعمال*، منشورات معهد المدققين الداخليين (IIA). http://www.theiia.org/intAuditor/itaudit/archives/2008/january/the-it-auditors-role-in-business-continuity-management

بالإضافة إلى تطوير DRPs، تعد **خطط طوارئ نظام المعلومات (ISCP)** خطوة حاسمة في تنفيذ برنامج التخطيط الشامل لاستمرارية الأعمال. قد تقوم المنظمات بتطوير ISCPs لكل نظام بناءً على مدى أهمية هذا النظام. بشكل عام، يصف ISCP خطوات وإجراءات مماثلة لـ BCP، ولكن تم تطوير ISCPs بشكل مستقل عن مواقع ومواقع محددة. من بين أشياء أخرى، يوفر ISCP معلومات أساسية محددة للنظام، مثل الأدوار والمسؤوليات، ومعلومات المخزون، وإجراءات التقييم، وإجراءات الاسترداد التفصيلية لهذا النظام.

ثانيًا. العناصر الرئيسة لإدارة استمرارية الأعمال

مطلوب مدقق تقنية المعلومات لتقييم برامج إدارة استمرارية الأعمال في المنظمة، والتي تتضمن تقييم BCPs و DRPs و ISCPs، من بين أمور أخرى. للقيام بذلك، يحتاج المدققون إلى فهم ما ينطوي عليه تطوير برنامج إدارة استمرارية الأعمال والخطوات التي يجب عليهم اتخاذها لتقييم فعالية البرامج الحالية.

تخطيط الاستمرارية الفاعلة له عدة مراحل مشتركة في جميع أنظمة المعلومات. المراحل العامة في العملية هي:[57]

- سياسة وخطة وتنظيم استمرارية الأعمال؛
- إنشاء فريق إدارة استمرارية الأعمال؛
- تقييم تأثير الأعمال وتقييم المخاطر؛
- الضوابط الوقائية والبيئية؛
- وثائق الخطة
- اختبار الخطة والتدريب؛
- تنفيذ الأمن و
- النسخ الاحتياطي والتعافي من الكوارث لخدمات الاستعانة بمصادر خارجية.

تمثل هذه المراحل العناصر الأساسية في القدرة الشاملة على التخطيط لاستمرارية الأعمال. يتم شرح العناصر بمزيد من التفصيل أدناه.

أ. سياسة وخطة وتنظيم استمرارية الأعمال

تبدأ الإدارة الفاعلة لاستمرارية الأعمال بوضع سياسة لإدارة استمرارية الأعمال. يجب أن يحدد بيان سياسة إدارة استمرارية الأعمال أهداف الاستمرارية العامة للمؤسسة، وأن يحدد الإطار التنظيمي والمسؤوليات لتخطيط الاستمرارية. يلعب فريق إدارة استمرارية الأعمال (الذي تمت مناقشته لاحقًا) الذي يمثل جميع وظائف العمل المناسبة أيضًا دورًا مهمًا في نجاح خطة استمرارية الأعمال الخاصة بالمنظمة. يمكن أن يمثل معدل دوران الموظفين الرئيسيين تحديًا لاستمرارية العمل لأي منظمة ويجب اتخاذ خطوات لضمان توفر الموارد المناسبة.

1. منع وتقليل الأضرار المحتملة والمقاطعة

يجب أن تتخذ المنظمة عددًا من الخطوات لمنع أو تقليل الضرر الذي قد يلحق بالعمليات الآلية نتيجة الأحداث غير المتوقعة. يمكن تصنيف هذه الخطوات على أنها

- النسخ الاحتياطي لملفات البيانات وبرامج الكمبيوتر والمستندات الهامة بشكل روتيني أو نسخها احتياطيًا باستخدام التخزين خارج الموقع؛ و / أو الترتيب لمنشآت النسخ الاحتياطي / التعافي من الكوارث عن بُعد التي يمكن استخدامها في حالة تلف المرافق المعتادة للمنظمة بشكل غير قابل للاستخدام؛
- إنشاء قدرة على استعادة نظام المعلومات وإعادة تكوينه بحيث يمكن استرداد نظام المعلومات وإعادة تشكيله إلى حالته الأصلية بعد الانقطاع أو الفشل؛
- تركيب ضوابط بيئية، مثل أنظمة إخماد الحرائق أو إمدادات الطاقة الاحتياطية؛
- التأكد من أن الموظفين ومستخدمي النظام الآخرين يفهمون مسؤولياتهم أثناء حالات الطوارئ؛ و
- الصيانة الفاعلة للأجهزة وإدارة المشكلات وإدارة التغيير.

بالإضافة إلى ذلك، عند الاستعانة بمصادر خارجية، يجب على المنظمة أن تثبت أن البائع لديه آليات مماثلة وأن الآليات فعالة.

---

[57] لمعلوماتٍ حول الإرشادات بخصوص عمليات التخطيط للطوارئ، انظر المعهد القومي للمعايير والتكنولوجيا، *إصدار خاص، 34-800 دليل التخطيط للطوارئ لأنظمة المعلومات الفيدرالية*.

2. تنفيذ إجراءات النسخ الاحتياطي للبيانات والبرامج

عادةً ما يكون نسخ ملفات البيانات والبرامج بشكل روتيني وتخزين هذه الملفات في مكان آمن بعيد أكثر الإجراءات فعالية من حيث التكلفة التي يمكن للمؤسسة اتخاذها للتخفيف من انقطاعات الخدمة. على الرغم من أنه يمكن غالبًا استبدال المعدات بسهولة، إلا أن التكلفة قد تكون كبيرة وقد تكون إعادة بناء ملفات البيانات واستبدال البرامج مكلفة للغاية وتستغرق وقتًا طويلاً. في الواقع، لا يمكن دائمًا إعادة بناء ملفات البيانات. بالإضافة إلى التكاليف المباشرة لإعادة بناء الملفات والحصول على البرامج، يمكن أن يؤدي انقطاع الخدمة ذات الصلة إلى خسائر مالية كبيرة.

3. تمرين

يجب تدريب الموظفين وإدراكهم لمسؤولياتهم في منع حالات الطوارئ والتخفيف من حدتها والاستجابة لها. على سبيل المثال، يجب أن يتلقى موظفو دعم أمن المعلومات تدريبًا دوريًا على إجراءات حرائق الطوارئ والمياه والإنذار، بالإضافة إلى مسؤولياتهم في بدء وتشغيل موقع بديل لمعالجة البيانات. أيضًا، إذا كان المستخدمون الخارجيون مهمين لعمليات المنظمة، فيجب إبلاغهم بالخطوات التي قد يتعين عليهم اتخاذها نتيجة لحالة الطوارئ.

4. خطط لصيانة الأجهزة وإدارة المشكلات وإدارة التغيير

يمكن أن تحدث انقطاعات غير متوقعة في الخدمة نتيجة فشل الأجهزة أو من تغيير المعدات دون إخطار مسبق كافٍ لمستخدمي النظام. لمنع مثل هذه الحوادث يتطلب برنامجًا فعالًا للصيانة وإدارة المشكلات وإدارة التغيير لمعدات الأجهزة.

ب. تأسيس فريق إدارة استمرارية الأعمال

لكي تكون ناجحًا، يجب تنظيم فريق إدارة استمرارية الأعمال من حيث تمثيل جميع وظائف العمل المناسبة. يجب أن تدعم الإدارة العليا والمسؤولون الآخرون ذوو الصلة برنامج استمرارية الأعمال وأن يكونوا مرتبطين بعملية تطوير السياسة. يجب تحديد الأدوار والمسؤوليات في الفريق وتحديدها بوضوح.

ج. تقييم اثر الاعمال وتقييم المخاطر

5. تقييم مدى أهمية وحساسية عمليات النظام وتحديد الموارد الداعمة

في أي منظمة، تعتبر استمرارية عمليات معينة أكثر أهمية من العمليات الأخرى، كما أنها ليست فعالة من حيث التكلفة لتوفير نفس المستوى من الاستمرارية لجميع العمليات. لهذا السبب، من المهم أن تحدد المنظمة العمليات الأكثر أهمية والموارد اللازمة لاستردادها ودعمها. يتم إجراء هذا التحديد من خلال إجراء تقييم للمخاطر وتقييم تأثير الأعمال،[58] التي تهدف إلى تحديد التهديدات المحتملة وتأثيراتها على معلومات المنظمة والموارد ذات الصلة، بما في ذلك برامج البيانات والتطبيقات والعمليات. يتم استخدام تقييم تأثير الأعمال لتحديد مكونات النظام وترتيب أولوياتها من خلال ربطها بعملية أعمال المؤسسة التي يدعمها النظام. يجب أن يغطي تقييم المخاطر وتأثير الأعمال جميع المجالات الوظيفية. يجب اتخاذ قرار بشأن المخاطر المتبقية وفقًا لذلك عندما يكون تأثير التهديد المحتمل ضئيلًا أو تكون أنظمة التحكم كافية للتخفيف من مثل هذه الحالات في الوقت المناسب.

6. تحديد البيانات والعمليات الهامة وترتيبها حسب الأولوية

يجب تحديد مدى أهمية وحساسية البيانات والعمليات المختلفة وترتيبها حسب الأولوية بناءً على التصنيفات الأمنية ومتطلبات التوفر وتقييم شامل للمخاطر لعمليات المنظمة.[59] يجب أن يكون تقييم المخاطر هذا بمثابة الأساس لخطة أمن المنظمة. تشمل العوامل التي يجب مراعاتها أهمية وحساسية البيانات والأصول التنظيمية الأخرى، وتكلفة عدم استعادة البيانات أو العمليات على الفور. على سبيل المثال، قد يؤدي الانقطاع لمدة يوم واحد عن نظام رئيسي لتحصيل الضرائب أو الرسوم أو فقدان البيانات ذات الصلة إلى إبطاء أو إيقاف تلقي الإيرادات بشكل كبير، وتقليل الضوابط المفروضة على الإيصالات بملايين الدولارات، وتقليل ثقة الجمهور. على العكس من ذلك، قد يكون النظام الذي يراقب تدريب الموظفين خارج الخدمة ربما لعدة أشهر دون عواقب وخيمة.

---

[58] للحصول على مثال على نموذج تقييم تأثير الأعمال، راجع https://csrc.nist.gov/CSRC/media/Publications/sp/800-34/rev-1/final/documents/sp800-34-rev1_bia_template.docx.

[59] لمزيد من المعلومات بخصوص تصنيفات الأمان، راجع https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

بشكل عام، يجب تحديد البيانات والعمليات الهامة وتصنيفها من قبل هؤلاء الأفراد المشاركين في أعمال المنظمة أو عمليات البرنامج. من المهم أيضًا الحصول على موافقة الإدارة العليا على مثل هذه القرارات، وكذلك موافقة المجموعات المتأثرة.

يجب مراجعة القائمة ذات الأولوية لمصادر المعلومات الهامة والعمليات بشكل دوري لتحديد ما إذا كانت الظروف الحالية تنعكس فيها. يجب أن تحدث مثل هذه المراجعات عندما يكون ثمة تغيير كبير في مهمة المنظمة وعملياتها أو في موقع أو تصميم الأنظمة التي تدعم هذه العمليات.

7. تحديد الموارد التي تدعم العمليات الحيوية

بمجرد تحديد البيانات والعمليات الهامة، يجب تحديد الحد الأدنى من الموارد اللازمة لدعمها وتحليل أدوارها. الموارد التي يجب النظر فيها تشمل

- موارد تقنية المعلومات، مثل الأجهزة والبرامج وملفات البيانات؛
- الشبكات، بما في ذلك المكونات مثل أجهزة التوجيه وجدران الحماية؛
- الإمدادات، بما في ذلك مخزون الورق والنماذج المطبوعة مسبقًا؛
- خدمات الاتصالات؛ و
- أي موارد أخرى ضرورية للعملية، مثل الأشخاص والمرافق المكتبية والإمدادات والسجلات الورقية.

نظرًا لأنه من المحتمل أن يتم الاحتفاظ بالموارد الأساسية أو إدارتها من قبل مجموعة متنوعة من المجموعات داخل المنظمة، فمن المهم أن يعمل فريق دعم أمن المعلومات والبرنامج معًا لتحديد الموارد اللازمة للعمليات الحيوية.

8. تحديد أولويات معالجة الطوارئ

بالتزامن مع تحديد الوظائف الحرجة وترتيبها، يجب على المنظمة وضع خطة لاستعادة العمليات الحرجة. يجب أن تحدد الخطة بوضوح الترتيب الذي يجب أن تتم فيه استعادة الجوانب المختلفة للمعالجة، ومن المسؤول، وما هي المعدات الداعمة أو الموارد الأخرى المطلوبة. يمكن لخطة استعادة المعالجة التي تم تطويرها بعناية أن تساعد المؤسسات على بدء عملية الاستعادة على الفور، وتحقيق أقصى استفادة من موارد الكمبيوتر المحدودة أثناء الطوارئ. يجب أن يشارك كل من مستخدمي النظام وموظفي دعم أمن المعلومات في تحديد أولويات معالجة الطوارئ.

د. الضوابط الوقائية والبيئية

تمنع الضوابط البيئية أو تخفف الضرر المحتمل للمرافق وانقطاعات الخدمة. تتضمن أمثلة الضوابط البيئية

- طفايات الحريق وأنظمة إخماد الحرائق،
- الحريق،
- كاشفات الدخان،
- أجهزة كشف المياه،
- إضاءة الطوارئ،
- التكرار في أنظمة تبريد الهواء،
- إمدادات الطاقة الاحتياطية،
- وجود صمامات إغلاق وإجراءات لأي خطوط سباكة للمباني قد تعرض مرافق المعالجة للخطر،
- مرافق المعالجة المبنية بمواد مقاومة للحريق ومصممة للحد من انتشار الحريق،
- سياسات تحظر الأكل والشرب والتدخين داخل مرافق تقنية المعلومات،
- تخزين النسخ الاحتياطي خارج الموقع، و
- ضوابط الأمان التقنية، مثل إدارة مفتاح التشفير.

يمكن أن تقلل الضوابط البيئية من الخسائر الناجمة عن بعض الانقطاعات، مثل الحرائق، أو تمنع الحوادث من خلال اكتشاف المشكلات المحتملة مبكرًا، مثل تسرب المياه أو الدخان، بحيث يمكن معالجتها. أيضًا، يمكن لمصادر الطاقة غير المنقطعة أو الاحتياطية أن تحمل مرفقًا من خلال انقطاع التيار الكهربائي لفترة قصيرة أو توفر وقتًا لنسخ البيانات احتياطيًا وتنفيذ إجراءات إيقاف التشغيل بشكل منظم أثناء انقطاع التيار الكهربائي الممتد.

هـ. وثائق الخطة

يجب توثيق خطط الاستمرارية، مثل BCPs و DRPs و ISCP، بشكل واضح، وإبلاغ الموظفين المتأثرين بها، وتحديثها لتعكس العمليات الحالية. بالإضافة إلى ذلك، يجب الحفاظ على الخطط في حالة جاهزة تعكس البيئة الحالية. يجب مواءمة DRPs و ISCPs بوضوح مع BCP وتقديم إرشادات خطوة بخطوة لتقليل تأثير الكارثة. مع تغير التقنية، قد يتم تعديل استراتيجيات وخطط الاسترداد. تتطلب التغييرات في هذه الخطط تغييرًا في تقييم تأثير الأعمال بحيث يتم توثيق المتطلبات والأولويات الجديدة للطوارئ بشكل واضح.

1. *BCP*

يركز BCP على الحفاظ على مهمة المنظمة / العمليات التجارية في حالة حدوث كارثة أو اضطراب. تعتبر خطط استمرارية العمل ضرورية لتوفير الإجراءات الخاصة بكيفية استمرار المؤسسة في عملياتها أثناء وبعد وقوع كارثة أو اضطراب. يمكن كتابة BCP لوحدة عمل واحدة أو عبر المنظمة بأكملها. بالإضافة إلى ذلك، يمكن تحديد نطاق خطة استمرارية العمل لمعالجة الوظائف التي تم تحديدها على أنها الأكثر أهمية. يجب تنسيق خطة استمرارية العمل مع خطط الاسترداد الأخرى لضمان توافق الإجراءات والتوقعات.

يجب أن تتضمن خطة استمرارية الأعمال عناصر، مثل تقييم تأثير الأعمال، للمساعدة في توجيه أولويات الاسترداد لخطة استمرارية العمل. يجب أيضًا توثيق استراتيجيات الاسترداد، مثل متطلبات الموارد للاسترداد وموافقة الإدارة على استراتيجيات الاسترداد. يجب على BCP توثيق المعلومات مثل فرق الاستعادة ومتطلبات جمع البيانات. علاوة على ذلك، يجب أن تتضمن خطة استمرارية الأعمال متطلبات التمرين والصيانة لضمان أن استراتيجيات الاسترداد محدثة ودقيقة. ستساعد هذه العناصر في إنشاء BCP شامل يمكنه توجيه الخطط الأخرى، مثل DRP.

2. *DRP*

يجب تطوير DRP لاستعادة التطبيقات الحرجة؛ وهذا يشمل الترتيبات الخاصة بمرافق المعالجة البديلة في حالة تضرر المرافق المعتادة بشكل كبير أو تعذر الوصول إليها. تحدد السياسات والإجراءات على مستوى المؤسسة عملية تخطيط الاسترداد ومتطلبات التوثيق. علاوة على ذلك، يجب أن تحدد الخطة على مستوى المنظمة الأنظمة والتطبيقات الهامة وأي خطط ثانوية أو ذات صلة.

يجب أن يتم الاتفاق على DRPs من قبل كل من إدارات الأعمال وأمن المعلومات، وإبلاغ الموظفين المناسبين. يجب أن تعكس الخطة المخاطر والأولويات التشغيلية التي حددتها المنظمة. يجب تصميمها بحيث لا تتجاوز تكاليف تخطيط الاسترداد التكاليف المرتبطة بالمخاطر التي تهدف الخطة إلى تقليلها. كما يجب أن تكون الخطة مفصلة وموثقة بشكل كافٍ بحيث لا يعتمد نجاحها على معرفة أو خبرة فرد أو شخصين. يجب أن تتوفر نسخ متعددة من DRP، مع تخزين بعضها في مواقع خارج الموقع لضمان عدم إتلافها من خلال نفس الأحداث التي جعلت مرافق معالجة البيانات الأساسية غير متاحة.

اعتمادًا على درجة استمرارية الخدمة المطلوبة، ستتراوح خيارات المواقع أو المرافق البديلة من موقع مجهز جاهز لخدمة النسخ الاحتياطي الفورية، ويشار إليه **بالموقع الساخن**، إلى موقع غير مجهز سيستغرق بعض الوقت للتحضير للعمليات، يشار إليه على أنه **موقع بارد**. بالإضافة إلى ذلك، يمكن ترتيب أنواع مختلفة من الخدمات مسبقًا مع البائعين. وتشمل هذه الترتيبات مع موردي أجهزة تقنية المعلومات وخدمات الاتصالات، وكذلك مع موردي نماذج الأعمال واللوازم المكتبية الأخرى.

ثالثا. *ISCP*

يجب على المنظمات وضع خطط طوارئ لكل نظام معلومات يمكن أن يتأثر في حالة وقوع كارثة.[60] يجب كتابة ISCP بالتنسيق مع الخطط الأخرى، مثل DRP. يمكن أن تكون أنظمة المعلومات معقدة للغاية وتدعم وظائف عمل مختلفة ومتعددة. ولهذه الغاية، تحتاج المنظمات إلى العمل مع الإدارة عند تطوير ISCPs لضمان تحديد الأهمية المناسبة وفهم تأثير انقطاع النظام أو تعطله.

[60] للحصول على إرشادات بشأن عمليات التخطيط للطوارئ، برجاء مراجعة المعهد الوطني للمعايير والتقنية، *المنشور الخاص 800-34: دليل التخطيط للطوارئ لأنظمة المعلومات الفيدرالية*.

سيحتوي ISCP عادةً على خمسة مكونات رئيسية: المعلومات الداعمة، التنشيط والإخطار، الاسترداد، إعادة التكوين، والملاحق. يقدم ما يلي وصفًا موجزًا لكل من هذه المكونات الخمسة:

- **المعلومات الداعمة** - يتضمن ذلك توفير معلومات أساسية أو معلومات سياقية تسهل فهم الخطة وتنفيذها وصيانتها.
- **التنشيط والإخطار**- يتضمن ذلك إخطار موظفي الاسترداد وإجراء تقييم الانقطاع وتفعيل الخطة.
- **الاسترداد** - يتضمن ذلك تنفيذ استراتيجيات الاسترداد لاستعادة قدرات النظام وإصلاح التلف واستئناف العمليات.
- **إعادة التأسيس** - يتضمن ذلك التحقق من صحة الاسترداد الناجح وإلغاء تنشيط الخطة. يمكن أن يشتمل هذا المكون على اختبار الوظائف للتأكد من عودة جميع وظائف النظام إلى التشغيل العادي.
- **الملاحق** - تتضمن معلومات قيمة لم تكن موجودة في متن الخطة.

سيساعد تضمين هذه المكونات في ضمان أن تكون المنظمة في وضع أفضل للتعامل مع الكوارث المتعلقة بالنظام.

و. اختبار الخطة والتدريب

1. الاختبار الدوري لخطط الاستمرارية

يعد اختبار خطط الاستمرارية أمرًا ضروريًا لتحديد ما إذا كانت ستعمل على النحو المنشود في حالة الطوارئ. يجب أن يكشف الاختبار عن نقاط ضعف مهمة في الخطط، مثل مرافق الدعم التي لا يمكنها تكرار العمليات الحرجة بشكل كافٍ كما هو متوقع. من خلال عملية الاختبار، تحتاج هذه الخطط إلى تحسين كبير.

سيختلف تواتر اختبار خطة الاستمرارية اعتمادًا على مدى أهمية عمليات المنظمة. بشكل عام، يجب اختبار خطط الاستمرارية للأنظمة والوظائف بالغة الأهمية بشكل كامل مرة واحدة كل عام أو عامين، عندما يتم إجراء تغييرات كبيرة على الخطة، أو عند حدوث دوران كبير للموظفين الرئيسيين. من المهم للإدارة العليا تقييم مخاطر المشاكل المحتملة في تنفيذ خطة الاستمرارية، وتطوير وتوثيق سياسة بشأن وتيرة ومدى هذا الاختبار.

2. تحديث خطة الاستمرارية بناءً على نتائج الاختبار

توفر نتائج اختبار الاستمرارية مقياسًا مهمًا لجدوى خطط الاستمرارية. على هذا النحو، يجب إبلاغ الإدارة العليا بها حتى يمكن تحديد الحاجة إلى التعديل والاختبار الإضافي، وحتى تكون الإدارة العليا على دراية بمخاطر استمرار العمليات مع خطط استمرارية غير كافية.

3. تمرين

تدريب الموظفين الذين لديهم مسؤوليات خطة الاستمرارية أمر بالغ الأهمية لضمان أن هؤلاء الموظفين على دراية بأدوارهم وامتلاكهم المهارات اللازمة لإنجاز تلك الأدوار. وهذا يضمن أن الموظفين على استعداد للمشاركة في أحداث الاختبار وانقطاع التيار الكهربائي الفعلي. بالإضافة إلى ذلك، ينبغي تدريب الموظفين بالقدر اللازم لأداء أدوارهم دون الحاجة إلى الرجوع إلى توثيق أدوارهم. يمكن أيضًا أن تكون الإرشادات الإرشادية الموثقة لمحاكاة الحالة الطارئة مع وجود جميع الأشخاص الرئيسيين أداة مفيدة.

ز. تنفيذ الأمن

يجب أن يتم تضمين أمن الموارد والعمليات في خطة العمل الأساسية حيث أن البيانات الهامة وبرامج التطبيقات والعمليات والموارد معرضة للخطر بسهولة أثناء أي حالة كارثة أو نشاط إدارة استمرارية الأعمال. على سبيل المثال، أثناء النسخ الاحتياطي للبيانات، يمكن أن يؤدي الافتقار إلى الأمان إلى إنشاء نسخ مكررة وتسرب البيانات المهمة. في الوقت نفسه، قد يكون من الممكن أن يتم اختراق البيانات التي يتم نسخها احتياطيًا أثناء عملية النسخ الاحتياطي (يتم نسخ البيانات من خادم المعاملات إلى البيانات التي يتم حفظها على خادم النسخ الاحتياطي).

ح. النسخ الاحتياطي والتعافي من الكوارث لخدمات الاستعانة بمصادر خارجية

تقوم العديد من المؤسسات بتعهيد كل أو جزء من عمليات تقنية المعلومات الخاصة بهم إلى مزود خدمة. نظرًا لأن العمليات والضوابط اليومية سيتم تنفيذها من قبل مزود الخدمة، فسيكون من الضروري أن تضمن المنظمة أن يتم تضمين BCP و DRP في العقد. ستحتاج المنظمة أيضًا إلى مراقبة ضمان استمرارية الأعمال والتأهب لاستعادة القدرة على العمل بعد الكوارث من قبل مزود الخدمة. وسيشمل ذلك الاستعداد الأمني لمزود الخدمة أيضًا. قد تحتاج المنظمة أيضًا إلى التأكد من أن مزود الخدمة يحافظ على سرية البيانات. يجب أن تحتفظ المنظمة بملكية العملية التجارية والمخاطر ذات الصلة. يجب أن يكون لدى المنظمة أيضًا BCP لضمان الاستمرارية إذا توقف مقدم الخدمة عن عمله. كما ذكرنا سابقًا، غالبًا ما تتوفر تقارير مراقبة مؤسسة الخدمة لتقديم هذا التأكيد كجزء من العقد المبرم مع البائع.

ثالثا. المخاطر على الهيئة الخاضعة للرقابة

الخدمات أو المنتجات الحاسمة هي تلك التي يجب تقديمها لضمان البقاء وتجنب التسبب في الخسارة والوفاء بالالتزامات القانونية أو غيرها من الالتزامات الخاصة بالمؤسسة. التخطيط المستمر هو عملية تخطيط استباقية تضمن أن العمليات التجارية والبنية التحتية لتقنية المعلومات في مؤسسة ما قادرة على دعم احتياجات المهمة بعد وقوع كارثة أو اضطراب آخر. تخدم المؤسسات الحكومية العديد من الاحتياجات المهمة (تقديم مدفوعات للمواطنين، فضلاً عن الرعاية الصحية والتعليم والدفاع وغيرها من الخدمات التي يعتمد عليها المواطنون). إذا تعطلت هذه الخدمات لفترات طويلة من الزمن، فسيؤدي ذلك إلى خسائر مالية وخسائر أخرى. يجب على المدققين التأكد من أن جميع المؤسسات الحكومية لديها عمليات التخطيط المستمر التي تضمن أن المنظمات قادرة على الاستمرار في خدمة المواطنين.

عند تقييم ما إذا كانت عمليات تخطيط استمرارية المنظمة قادرة على تحسين موثوقية واستمرارية البنية التحتية لتقنية المعلومات والعمليات التجارية، يمكن للمدققين التركيز على بعض مخاطر المراجعة لتحديد فعالية التخطيط. تتضمن مخاطر المراجعة هذه تحديد ما إذا كانت المنظمة قد طورت وثائق مهمة، بما في ذلك BCPs و DRPs و ISCPs، التي تغطي جميع المجالات الوظيفية الهامة. علاوة على ذلك، إذا كانت الأدوار والمسؤوليات غير واضحة ومفهومة من قبل الموظفين المعنيين، فقد يصبح BCP الجيد غير فعال.

تطوير تقييم تأثير الأعمال والضوابط الوقائية والبيئية والتوثيق؛ اختبار خطة طوارئ الاستمرارية؛ ويدعم تدريب الموظفين التنفيذ الفاعل لبرنامج إدارة استمرارية الأعمال. يشكل الأمان الناقص في تنفيذ BCP و DRP خطر تعرض المنظمة لفقدان البيانات وضياع الوقت الثمين والتكاليف الأخرى بسبب التعافي غير الفاعل في حالة وقوع كارثة.

تمثل خدمات الاستعانة بمصادر خارجية منطقة مخاطر متميزة حيث لا يكون التخطيط المستمر تحت سيطرة المنظمة بالكامل. يجب معالجة المخاطر المتعلقة بأمن البيانات وفقدان البيانات والتعامل غير المصرح به وتسرب البيانات. بالإضافة إلى ذلك، تواجه المؤسسات مخاطر الاستمرارية المتعلقة بفقدان المعرفة التجارية أو ملكية العملية، فضلاً عن عدم القدرة على تغيير مزود الخدمة في حالة ضعف الأداء أو الإغلاق.

رابعا. المراجع وقراءات إضافية

" .IIa دور مدقق تقنية المعلومات في إدارة استمرارية الأعمال،" *المدقق الداخلي*. https://elearn.iia.org.au/mod/resource/view.php?id=10550 يناير 2008.

المنظمة الدولية للتوحيد القياسي / اللجنة الكهروتقنية الدولية. *ISO / IEC 22301: 2019 - الأمن والمرونة - أنظمة إدارة استمرارية الأعمال - المتطلبات* . https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en. 2019

المنظمة الدولية للتوحيد القياسي / اللجنة الكهروتقنية الدولية. *ISO / IEC 22300: 2021* - الأمن والمرونة - المفردات. https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en. 2021

المنظمة الدولية للتوحيد القياسي / اللجنة الكهروتقنية الدولية. *ISO / IEC 22313: 2020 - الأمان والمرونة - أنظمة إدارة استمرارية الأعمال - إرشادات بشأن استخدام ISO 22301*. https://www.iso.org/standard/75107.html. 2020

إيساكا. *إطار عمل COBIT 2019: أهداف الحوكمة والإدارة*. 2019.

المعهد الوطني للمعايير والتقنية. *المنشور الخاص 800-34: دليل التخطيط للطوارئ لأنظمة المعلومات الفيدرالية*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.

المعهد الوطني للمعايير والتقنية. *المنشور الخاص 800-53: ضوابط الأمن والخصوصية لأنظمة المعلومات والمنظمات*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. سبتمبر 2020.

المعهد الوطني للمعايير والتقنية. *معايير التصنيف الأمني لأنظمة المعلومات والمعلومات الفيدرالية ، FIPS 199*. https://csrc.nist.gov/publications/detail/fips/199/final February 2004.

مكتب محاسبة الحكومة الأمريكية. *دليل تدقيق نظم المعلومات الفيدرالية (FISCAM)*. https://www.gao.gov/products/gao-09-232g. 2 فبراير 2009.

الفصل 7: أمن المعلومات

ما هو أمن المعلومات؟

كما هو مذكور في الفصل 1، يمكن تعريف أمن المعلومات على أنه حماية المعلومات وأنظمة المعلومات من الوصول غير المصرح به أو الاستخدام أو الكشف أو التعطيل أو التعديل أو التدمير بغية توفير السرية والنزاهة والتوافر.[61] يشمل أمن المعلومات تلك التدابير اللازمة للتحكم في هذه التهديدات ومنعها واكتشافها وتوثيقها ومواجهتها، كما يسمح للمؤسسة بحماية البنية التحتية لنظام المعلومات الخاص بها من المستخدمين غير المصرح لهم.

يرتبط أمن المعلومات ارتباطًا وثيقًا بالأمن السيبراني ولكنه يختلف عنه، وهو عملية حماية المعلومات عن طريق منع الهجمات الإلكترونية واكتشافها والاستجابة لها، غالبًا من مصادر خارجية.[62] يتضمن الأمن السيبراني الاستراتيجية والسياسة والمعايير المتعلقة بأمن الفضاء السيبراني والعمليات فيه، ويشمل، من بين أمور أخرى، الحد من التهديد ونقاط الضعف؛ الاستجابة للحوادث والمرونة والتعافي؛ وتأمين المعلومات.[63] على الرغم من أن العديد من العناصر الرئيسة لأمن المعلومات التي تمت مناقشتها لاحقًا في هذا الفصل قابلة للتطبيق على الأمن السيبراني، فإن التركيز الأساسي لهذا الفصل ينصب على سياسات وإجراءات وممارسات أمن المعلومات التي يجب على المنظمات تنفيذها. يجري إعداد وثيقة توجيه تدقيق منفصلة بشأن الأمن السيبراني وحماية البيانات كجزء من مشروع INTOSAI WGITA آخر.

كما ذكرنا سابقًا، يتمثل أحد الجوانب الأساسية لأمن المعلومات في القدرة على ضمان **سرية المعلومات وسلامتها وتو افرها** - والتي يعتمد عليها كل شيء آخر.

- تحافظ **السرية** على القيود المصرح بها على الوصول إلى المعلومات والإفصاح عنها، بما في ذلك وسائل حماية الخصوصية الشخصية ومعلومات الملكية. فقدان السرية هو الكشف غير المصرح به عن المعلومات.
- **النزاهة** هي الحماية من تعديل المعلومات أو إتلافها بشكل غير لائق، والذي يتضمن ضمان عدم التنصل من المعلومات[64] والأصالة.[65] فقدان السلامة هو التعديل غير المصرح به أو إتلاف المعلومات.
- **التو افر** هو التأكد من أن جميع أنظمة المعلومات بما في ذلك الأجهزة وشبكات الاتصال وتطبيقات البرامج والبيانات التي تحتفظ بها متاحة للمستخدمين في الأوقات اللازمة لتنفيذ الأنشطة التجارية. كما ينبغي أن تضمن الوصول الموثوق به في الوقت المناسب إلى المعلومات واستخدامها. فقدان التوافر هو تعطيل الوصول إلى المعلومات أو نظام المعلومات أو استخدامها.

يحتاج أمن المعلومات إلى أشياء كثيرة للمؤسسة، ويجب أن يكون في النهاية أداة تمكن المنظمة وتدعم أهدافها بدلاً من أن تصبح ذاتية الخدمة. إحدى الطرق التي يمكن أن يدعم بها أمن المعلومات أهداف العمل هي أن تكون حارس البوابة لأصول معلومات المؤسسة. هذا يستدعي برنامج أمن معلومات المنظمة لحماية البيانات التنظيمية مع تمكين المؤسسة أيضًا من متابعة أهداف أعمالها - والتسامح مع مستوى مقبول من المخاطر في القيام بذلك.

بالإضافة إلى ذلك، يدعو هذا المنظمة إلى توفير المقدار المناسب من المعلومات للمستخدمين المناسبين. سيتطلب تطبيق مبادئ أمن المعلومات على استخدام الأجهزة وشبكات الاتصال وتطبيقات البرامج والوصول إلى البيانات سياسة للتحكم في الوصول. الهدف من **التحكم في الوصول** هو ضمان وصول المستخدمين إلى الموارد والخدمات التي يحق لهم الوصول إليها فقط، وعدم حرمان المستخدمين المؤهلين من الوصول إلى الخدمات التي يتوقعون الحصول عليها بشكل شرعي. إن توفير المعلومات لمن ينبغي أن يكون بحوزتها لا يقل أهمية عن حمايتها من أولئك الذين لا ينبغي لهم الحصول عليها.

في جوهره، يتعلق أمن المعلومات بتقليل التعرض، بناءً على إدارة المخاطر، في جميع مجالات نموذج حوكمة تقنية المعلومات. قد يؤدي الفشل في تنفيذ عمليات تخفيف المخاطر

---

[61] المعهد الوطني للمعايير والتقنية، *المسرد* (2021)، https://csrc.nist.gov/glossary.

[62] المعهد الوطني للمعايير والتقنية، *إطار عمل تحسين الأمن السيبراني للبنية التحتية الحرجة*، الإصدار 1.1، 2018.

[63] المبادرة الوطنية لشغل وظائف ودراسات *الأمن السيبراني*، *مسرد مصطلحات الأمن السيبراني*، https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.

[64] **عدم التنصل** هو تأكيد على تزويد مرسل المعلومات بإثبات التسليم ويتم تزويد المستلم بإثبات هوية المرسل، لذلك لا يمكن لأي منهما أن ينكر لاحقًا معالجة المعلومات. قد لا يكون عدم التنصل ضروريًا لتقييم النزاهة لتحقيق هدف المراجعة.

[65] **الأصالة** هي خاصية أن تكون أصليًا وأن تكون قادرًا على التحقق من صحتها والوثوق بها؛ الثقة في صحة الإرسال أو الرسالة أو منشئ الرسالة. قد لا تكون المصداقية ضرورية لتقييم النزاهة لتحقيق هدف المراجعة.

ومراقبتها في منطقة واحدة إلى إلحاق الضرر بالمنظمة بأكملها. حتى لو كان معروفًا على نطاق واسع أن إدارة مخاطر أمن المعلومات بشكل فعال أمر ضروري لسلامة المنظمة، فغالبًا ما يتم التغاضي عن هذه المخاطر أو لا يتم تحديث احتياطات السلامة استجابة للظروف المتغيرة.

أ. ضرورة أمن المعلومات

تزداد أهمية أمن المعلومات بالنسبة للمنظمات الحكومية. نظرًا لأن الترابط بين الشبكات العامة والخاصة ومشاركة موارد المعلومات يزيدان من تعقيد التحكم في الوصول والحفاظ على سرية البيانات وسلامتها وتوافرها، فثمة حاجة متزايدة للمنظمات لإنشاء برامج أمن المعلومات.

أنظمة المعلومات عبارة عن تجمعات معقدة بشكل لا يصدق من التقنية والعمليات والأشخاص الذين يعملون بشكل تعاوني لاستيعاب معالجة المعلومات وتخزينها ونقلها لدعم مهمة المنظمة ووظائف الأعمال. لذلك، من الضروري أن تقوم كل منظمة ببناء برنامج لأمن المعلومات.

الهدف من برنامج أمن نظام المعلومات هو حماية معلومات المنظمة عن طريق الحد من مخاطر فقدان السرية، والسلامة، وتوافر تلك المعلومات إلى مستوى مقبول. إذا لم تقم المنظمة بإنشاء برنامج لأمن المعلومات، فستكون لديها مخاطر متزايدة لمواجهة التهديدات المحتملة لعمليات المنظمة، وتحقيق الأهداف العامة، والتأثير في نهاية المطاف على مصداقية المنظمة.

مع نمو إمكانات تقنية المعلومات وتعقيدها ودورها، يصبح أمن المعلومات موضوعًا مهمًا بشكل متزايد لعمليات تدقيق تقنية المعلومات. إنه عامل حاسم في أنشطة المنظمات، لأن نقاط الضعف في أمن المعلومات قد تؤدي إلى أضرار جسيمة. تشمل الآثار المحتملة لنقاط الضعف في أمن المعلومات ما يلي :

- مخالفات المتطلبات القانونية والتنظيمية؛
- الغرامات والتعويضات والمبيعات المخفضة أو تكاليف الإصلاح أو الاستعادة؛
- الحد من الفاعلية و / أو الكفاءة في مشروع أو برنامج أو خدمة كاملة تقدمها المنظمة؛
- فقدان أو سرقة موارد الكمبيوتر والأصول والأموال؛
- الوصول غير الملائم إلى المعلومات الحساسة والكشف عنها أو تعديلها أو إتلافها، مثل معلومات الأمن القومي، ومعلومات التعريف الشخصية، والمعلومات التجارية المسجلة الملكية؛
- مطالب القرصنة والفدية المحتملة؛
- تعطيل العمليات الأساسية الداعمة للبنية التحتية الحيوية أو الدفاع الوطني أو خدمات الطوارئ؛
- تقويض المهام التنظيمية بسبب الحوادث التي تضر بسمعة المنظمة و / أو المالية؛
- استخدام موارد الكمبيوتر لأغراض غير مصرح بها أو لشن هجمات على أنظمة أخرى؛ و
- الأضرار التي لحقت بالشبكات والمعدات.

قد يكون سبب هذا الضرر:

- **الخروقات الأمنية** - المكتشفة وغير المكتشفة؛
- **اتصالات خارجية غير مصرح بها** - بالمواقع البعيدة؛
- الكشف **عن المعلومات** - الكشف عن أصول الشركة والمعلومات الحساسة لأطراف غير مصرح لها. يُعرف أحد الأمثلة على كيفية حدوث ذلك بالهندسة الاجتماعية، وهي تقنية تلاعب يستخدمها المجرمون تعتمد على غريزة الثقة الإنسانية الأساسية لخداع الأشخاص للتخلي عن معلومات سرية؛
- **التهديدات الداخلية** - المستخدمون الذين يستغلون مواقعهم داخل المنظمات للوصول غير المقيد والتسبب في الضرر؛ و
- **ثغرات النظام** - الأنظمة والبيانات التي يتم الوصول إليها بطريقة غير مصرح بها معرضة لمجموعة واسعة من الهجمات الضارة ويمكن فتحها لمزيد من عمليات التطفل.

يمكن أن يصبح الاستخدام المتزايد لوسائل التواصل الاجتماعي من قبل المنظمات الحكومية أيضًا مجالًا لعمليات تدقيق تقنية المعلومات المحتملة. يوفر استخدام خدمات الوسائط الاجتماعية هذه - بما في ذلك الخدمات الشائعة مثل Facebook و Twitter و YouTube - فرصًا للوكالات لمشاركة المعلومات بسهولة أكبر مع الجمهور والتماس التعليقات من الجمهور. بيد أنه، يمكن أن يشكل استخدام هذه الخدمات تحديات في حماية المعلومات الشخصية وضمان أمن المعلومات والأنظمة، من بين مجالات أخرى. على سبيل المثال، قد يستخدم المهاجمون وسائل التواصل الاجتماعي لجمع المعلومات وشن هجمات ضد أنظمة معلومات المنظمة. بالإضافة إلى ذلك، يمكن المساس بالخصوصية إذا لم يتم وضع حدود واضحة على كيفية استخدام المنظمة للمعلومات الشخصية التي يمكنها الوصول إليها في بيئات الشبكات الاجتماعية. للمساعدة في مواجهة هذه التحديات،

يجب أن يكون لدى المؤسسات سياسات وإجراءات مطبقة لإدارة المخاطر الأمنية وحماية الخصوصية التي تتناول استخدام وسائل التواصل الاجتماعي.[66]

ب. تشكيل ثقافة أمن المعلومات

أحد العوامل المحددة لنجاح برامج أمن المعلومات في المنظمة هو خلق ثقافات تنظيمية تعالج قضايا الأمن. لمعالجة هذه القضايا وغيرها بشكل موحد في مؤسسة كبيرة، يجب اتباع نموذج عمل لأمن المعلومات.[67] تتضمن العناصر الأساسية لثقافة أمن المعلومات الناجحة ما يلي:

- **خلق الوعي الأمني.** يتكون هذا من أنشطة توعية عامة بأمن المعلومات وجلسات تثقيفية للموظفين. هذه الجلسات هي فرص جيدة للبدء في تقديم مسؤوليات أمن المعلومات. قد تكون وظيفة الموارد البشرية مسؤولة عن تدريب الوعي الأولي للموظفين الجدد. يجب أن يستمر التدريب أثناء التوظيف وحتى إنهاء الخدمة لتعزيز الوعي الأمني دائمًا.
- **السعي للحصول على التزام الإدارة.** التزام الإدارة هو سمة فريدة من نوعها في تشكيل ثقافة أمن المعلومات. يظهر الالتزام من قبل الإدارة ليس فقط في إعداد التوثيق الرسمي للمعلومات بشأن السياسات الأمنية، غير أنه أيضًا من خلال المشاركة الفاعلة. إذا كانت الإدارة لا تدعم برنامج أمن المعلومات بشكل حقيقي، فقد يؤدي ذلك إلى تثبيط شعور الموظفين بالالتزام أو المسؤولية تجاه البرنامج. لذلك من الأهمية بمكان للإدارة قبول الملكية لأمن المعلومات وتقديم الدعم الكامل للبرنامج.
- **بناء تنسيق قوي من خلال إنشاء فرق متعددة الوظائف.** نظرًا لأن أمن المعلومات يتضمن العديد من جوانب المنظمة التي تتطلب التنسيق، فيجب النظر في تشكيل فرق متعددة الوظائف (على سبيل المثال، فرق بها أعضاء من أقسام متعددة، بما في ذلك تقنية المعلومات). يشجع استخدام فرق متعددة الوظائف على التواصل والتعاون ويقلل من العزلة الإدارية والجهود المكررة.

يعتبر ترسيخ ثقافة أمن المعلومات جزءًا لا يتجزأ من تطبيق الحوكمة داخل المنظمة، وتتميز بما يلي:

- **محاذاة أمن المعلومات وأهداف العمل.** من الضروري مواءمة أمن المعلومات وأهداف العمل لأن الأهداف الأمنية تمكن وتدعم أهداف العمل. يحتاج برنامج أمن المعلومات إلى التوافق مع المنظمة وتوفير ضوابط لأمن المعلومات تكون عملية وتوفر تقليلًا حقيقيًا وقابل للقياس للمخاطر.
- **التوازن بين المنظمة والأفراد والعملية والتقنية.** يتطلب أمن المعلومات الفاعل الدعم التنظيمي، والموظفين الأكفاء، والعمليات الفاعلة، واختيار التقنية المناسبة. يتفاعل كل عنصر مع المجالات الأخرى - مما يؤثر على العناصر الأخرى ويدعمها، غالبًا بطرق معقدة - لذلك، من الضروري تحقيق التوازن فيما بينها. في حالة نقص أي عنصر، يتضاءل أمن المعلومات.
- **إدارة المخاطر.** يجب أن يكون تطبيق أمن المعلومات مدفوعًا بإدارة المخاطر. يصف المعهد الوطني لمعايير التقنية الجوانب الأربعة التالية لعملية إدارة المخاطر في منشوره الخاص بشأن إدارة مخاطر أمن المعلومات:[68]
  - إسناد مسؤوليات إدارة المخاطر الأمنية إلى كبار القادة / المديرين التنفيذيين؛
  - الاعتراف المستمر والفهم من قبل كبار القادة / المديرين التنفيذيين لمخاطر أمن المعلومات على العمليات والأصول التنظيمية، والأفراد، والمنظمات الأخرى، الناشئة عن تشغيل واستخدام نظم المعلومات؛
  - إنشاء التسامح التنظيمي للمخاطر والإبلاغ عن تحمل المخاطر في جميع أنحاء المنظمة، بما في ذلك التوجيه بشأن كيفية تأثير تحمل المخاطر على أنشطة صنع القرار المستمرة؛ و
  - المساءلة من قبل كبار القادة / المديرين التنفيذيين عن قراراتهم المتعلقة بإدارة المخاطر ولتنفيذ برامج إدارة مخاطر فعالة على مستوى المنظمة.

ثانيًا. عناصر أمن المعلومات

تغطي مناقشة أمن المعلومات في مؤسسة ما 12 مجالًا:

---

[66] لمزيد من المعلومات بشأن مراجعة سياسات المنظمة وإجراءاتها لاستخدام وسائل التواصل الاجتماعي، راجع مكتب محاسبة الحكومة الأمريكية، *وسائل التواصل الاجتماعي: تحتاج الوكالات الفيدرالية إلى سياسات وإجراءات لإدارة وحماية المعلومات* التي تصل إليها وتنشرها، GAO-11-605، (28 يونيو 2011)، https://www.gao.gov/products/GAO-11-605.

[67] ISACA، *نموذج عمل لأمن المعلومات*، 2010.

[68] المعهد الوطني للمعايير والتقنية، *المنشور الخاص 800-39: إدارة مخاطر أمن المعلومات: عرض التنظيم والرسالة ونظام المعلومات*، 2011.

- تقييم المخاطر
- سياسة الأمن
- تنظيم أمن تقنية المعلومات
- إدارة العمليات والسجلات
- إدارة الأصول
- أمن الموارد البشرية
- الأمن المادي والبيئي
- صلاحية التحكم صلاحية الدخول
- تطوير أنظمة تقنية المعلومات واقتنائها وصيانتها
- إدارة حوادث أمن تقنية المعلومات
- إدارة استمرارية العمل
- الالتزام

أ. تقييم المخاطر

تقييم المخاطر هو عملية تحديد وتحليل وتقييم المخاطر في البنية التحتية لأمن تقنية المعلومات. إنها أيضًا عملية تقييم المخاطر المتعلقة بالأمن من التهديدات الداخلية والخارجية للكيان وأصوله وموظفيه. تتضمن عملية تقييم المخاطر تحديد وتحليل

- جميع الأصول والعمليات المتعلقة بالنظام؛
- بيئات الاستعانة بمصادر خارجية المتعلقة بالنظام؛
- التهديدات المحتملة التي يمكن أن تؤثر على سرية أو سلامة أو توفر النظام؛
- نقاط ضعف النظام والتهديدات المرتبطة بها؛
- الآثار والمخاطر المحتملة من نشاط التهديد؛
- متطلبات الحماية للتخفيف من المخاطر؛ و
- اختيار التدابير الأمنية المناسبة وتحليل علاقات المخاطر.

قد يؤدي تقييم المخاطر الذي يتم إجراؤه بشكل غير صحيح إلى عدم حماية البنية التحتية والمعلومات الحساسة، أو في بعض الحالات إهدار الحماية المفرطة. يحدد المعهد الوطني لمعايير التقنية أربع خطوات لعملية تقييم المخاطر في *دليل نشره الخاص لإجراء تقييمات المخاطر*:[69]

- **الاستعداد** للتقييم من خلال تطوير إطار المخاطر التنظيمية.
- **إجراء** التقييم من قبل
  - تحديد مصادر التهديد والأحداث،
  - تحديد نقاط الضعف والظروف المؤهبة،
  - تحديد احتمالية الحدوث،
  - تحديد حجم التأثير في حالة حدوث خرق أمني، و
  - باستخدام المعلومات الواردة أعلاه لتحديد المخاطر الشاملة.
- **توصيل** نتائج التقييم
- **حافظ** على التقييم.

[69] المعهد الوطني للمعايير والتقنية، مبادرة التبشأن لفريق العمل المشترك، منشور خاص 800-30، *دليل لإجراء تقييمات المخاطر*، 2012.

تقييمات المخاطر ليست أنشطة لمرة واحدة توفر معلومات دائمة ونهائية لصانعي القرار لتوجيه وتوجيه الاستجابات لمخاطر أمن المعلومات. بدلاً من ذلك، يجب على المنظمات استخدام تقييمات المخاطر على أساس مستمر، مع تكرار تقييمات المخاطر والموارد المستخدمة أثناء التقييمات بما يتناسب مع الغرض المحدد ونطاق التقييمات.

سيساعد تطبيق تقييم المخاطر الإدارة على اختيار الضوابط المناسبة للتخفيف من المخاطر بشكل فعال. لتحديد ضوابط الأمان المناسبة، يحدد منشور معايير معالجة المعلومات الفيدرالية 199 ثلاثة مستويات من التأثير المحتمل - منخفض ومتوسط وعالي - على المؤسسات أو الأفراد في حالة حدوث خرق للأمن (أي فقدان السرية أو النزاهة أو التوفر).[70] يجب أن يتم تطبيق هذه التعريفات في سياق كل منظمة والمصلحة الوطنية العامة.

- يكون التأثير المحتمل **منخفضًا** إذا كان من المتوقع أن يكون لفقدان السرية أو النزاهة أو التوافر تأثير سلبي **محدود** على العمليات التنظيمية أو الأصول التنظيمية أو الأفراد.
- التأثير المحتمل **معتدلة** إذا كان من المتوقع أن يكون لفقدان السرية أو النزاهة أو التوافر تأثير سلبي **خطير** على العمليات التنظيمية أو الأصول التنظيمية أو الأفراد.
- يكون التأثير المحتمل **مرتفعًا** إذا كان من المتوقع أن يكون لفقدان السرية أو النزاهة أو التوافر تأثير سلبي **شديد أو كارثي** على العمليات التنظيمية أو الأصول التنظيمية أو الأفراد.

يؤثر تصنيف التأثير هذا على صرامة الاختبار في العديد من مجالات أمن المعلومات. على سبيل المثال، فيما يتعلق بضوابط الوصول، تعتبر تقييمات المخاطر التنظيمية (وتحمل المخاطر) من العوامل المهمة في تحديد سياسات وإجراءات التحكم في الوصول. يجب أن تكون سياسات وإجراءات التحكم في الوصول لمورد معين مناسبة لمستوى التأثير (أي فقدان السرية أو النزاهة أو التوافر) الذي قد يكون لخرق أمني لذلك المورد على المنظمة.

ب. نهج الأمان

السياسة الأمنية للمؤسسة هي مجموعة القوانين والقواعد والممارسات التي تنظم كيفية إدارتها وحماية وتوزيع الموارد لتحقيق أهداف أمنية محددة. يجب أن تحدد هذه القوانين والقواعد والممارسات معايير سلطة الأفراد، وقد تحدد الشروط التي يُسمح بموجبها للأفراد بممارسة سلطتهم. لكي تكون ذات مغزى، يجب أن توفر هذه القوانين والقواعد والممارسات للأفراد قدرة معقولة على تحديد ما إذا كانت أفعالهم تنتهك السياسة أو تمتثل لها.

راجع الجدول للتعرف على العناصر الموصى بها لسياسة أمان تقنية المعلومات.

عناصر من أمن تقنية المعلومات سياسات	تعريف أمن المعلومات - الأهداف والنطاق (بما في ذلك سرية البيانات)
	مبادئ ومعايير الأمان التفصيلية ومتطلبات الامتثال (على سبيل المثال، لا ينبغي أن يكون لموظفي قسم تقنية المعلومات مسؤوليات تشغيلية أو محاسبية)
	تحديد المسؤوليات العامة والمحددة لجميع جوانب أمن المعلومات
	استخدام أصول المعلومات والوصول إلى البريد الإلكتروني والإنترنت
	وضع وطريقة الوصول (لتشمل التحكم في الوصول وسياسات المصادقة)
	إجراءات النسخ الاحتياطي
	إجراءات التعامل مع البرامج والبرامج الضارة (على سبيل المثال، المراقبة المستمرة، وكشف التسلل، وأنظمة منع التطفل)
	عناصر التوعية والتدريب الأمني
	عملية الإبلاغ عن الحوادث الأمنية المشتبه بها والاستجابة لها
	خطط استمرارية العمل
	إدارة التصحيح
	الأمن المادي
	طرق إبلاغ الموظفين بالسياسة والإجراءات المعتمدة لأمن المعلومات

[70] معايير معالجة المعلومات الفيدرالية 199، *معايير التصنيف الأمني لأنظمة المعلومات والمعلومات الفيدرالية*، 2004.

ج. تنظيم أمن تقنية المعلومات

غالبًا ما يتطلب تنظيم أمن تقنية المعلومات تنفيذ سياسة أمنية لكيان ما. يمكن إعطاء مسؤولية تنفيذ السياسة الأمنية إلى وحدة أو فرد يعمل لاحقًا مع المنظمة لاكتساب الأدوات والعمليات المناسبة لتنفيذ السياسة بشكل فعال. بمجرد تنفيذ السياسة، ستكون المنظمة مسؤولة بالإضافة إلى ذلك عن توفير التدريب للموظفين والاستجابة للحوادث الأمنية. تحتاج المنظمة أيضًا إلى التأكد من أن بياناتها التي تم الوصول إليها من قبل المنظمات الخارجية أو المنقولة إليها محمية بشكل مناسب. سيحتاج المدقق إلى التأكد من أن المنظمات الخارجية يمكنها تنفيذ متطلبات الأمان.

د. إدارة العمليات والسجلات

تحتاج المنظمة إلى تتبع العملية والإجراءات التي تستخدمها لعملياتها التجارية. يتضمن ذلك مجموعة الإجراءات والعمليات التنظيمية التي تضمن معالجة البيانات الصحيحة وإجراءات التوثيق لوسائل الإعلام ومعالجة البيانات، وإجراءات الطوارئ، وتسجيل أمان الشبكة، وإجراءات النسخ الاحتياطي.

هـ. إدارة الأصول

تشير إدارة الأصول، على نطاق واسع، إلى أي نظام يتم بموجبه مراقبة الأشياء ذات القيمة للمؤسسة والمحافظة عليها. إدارة الأصول هي عملية منهجية لتشغيل الأصول وصيانتها وترقيتها والتخلص منها بطريقة فعالة من حيث التكلفة.

بالنسبة لتقنية المعلومات، تتضمن إدارة الأصول الاحتفاظ بجرد دقيق للمعدات والبيانات ومعرفة التراخيص الخاصة بالمعدات المرتبطة وصيانة المعدات وحمايتها (مثل غرفة الإغلاق والتحكم). تتضمن إدارة أصول تقنية المعلومات أيضًا إدارة البرامج ووثائق العملية التي تعتبر ذات قيمة للمؤسسة.

تعتبر إدارة أصول تقنية المعلومات مهمة للغاية، حيث قد تكون المنظمة معرضة للخطر إذا لم يكن لديها جرد كامل لأصولها. بدون جرد كامل لأصول تقنية المعلومات، من المستحيل على المؤسسات معرفة ما إذا كانت تطبق ضوابط أمنية مناسبة على إجمالي أصولها. يمكن أن يؤدي عدم وجود مخزون كامل لأصول تقنية المعلومات أيضًا إلى حدوث مضاعفات عندما تحتاج المؤسسات إلى ترقية البرامج لتلبية احتياجات العمل المستقبلية.

و. أمن الموارد البشرية

يحتاج الموظفون الذين يتعاملون مع البيانات الشخصية في مؤسسة ما إلى تلقي تدريب توعوي مناسب وتحديثات منتظمة في محاولة لحماية البيانات الموكلة إليهم. يجب تحديد الأدوار والمسؤوليات المناسبة المخصصة لكل وصف وظيفي وتوثيقها بما يتماشى مع السياسة الأمنية للمؤسسة. يجب حماية بيانات المنظمة من الوصول غير المصرح به أو الكشف أو التعديل أو الإتلاف أو التدخل. تعد إدارة مخاطر أمن وخصوصية الموارد البشرية ضرورية خلال جميع مراحل ارتباط التوظيف بالمنظمة.

المجالات الثلاثة لأمن الموارد البشرية هي:

- **ما قبل التوظيف:** يتضمن ذلك تحديد الأدوار والمسؤوليات الخاصة بالوظيفة، وتحديد الوصول المناسب إلى المعلومات الحساسة للوظيفة، وتحديد عمق مستويات فحص المرشح - كل ذلك وفقًا لسياسة أمن تقنية المعلومات الخاصة بالمنظمة. خلال هذه المرحلة، يجب أيضًا تحديد شروط العقد.
- **أثناء العمل:** يجب أن يتلقى الموظفون الذين يتمتعون بإمكانية الوصول إلى المعلومات الحساسة في مؤسسة ما تذكيرات دورية بمسؤولياتهم وأن يتلقوا تدريبًا مستمرًا ومحدثًا للتوعية الأمنية لضمان فهمهم للتهديدات الحالية والممارسات الأمنية المقابلة للتخفيف من هذه التهديدات.
- **الفصل من العمل:** لمنع الوصول غير المصرح به إلى المعلومات الحساسة، يجب إلغاء الوصول فور إنهاء الموظف الذي لديه حق الوصول إلى هذه المعلومات. يتضمن هذا أيضًا إعادة أي أصول للمنظمة كان يحتفظ بها الموظف. خلال هذه المرحلة، يمكن إعداد نموذج خاص لتوثيق جميع الأعمال التي قام بها الموظف وللتأكد من إلغاء الوصول بالكامل وإعادة جميع الأصول.

يجب وضع برنامج للوعي الأمني، يذكر جميع الموظفين بالمخاطر المحتملة والتعرض، بالإضافة إلى مسؤولياتهم كأوصياء على معلومات المنظمة.

ز. الأمن المادي والبيئي

يصف الأمان المادي الإجراءات التي تم تصميمها لمنع الوصول إلى الأفراد غير المصرح لهم (بما في ذلك المهاجمين أو حتى الدخلاء العرضيين) من الوصول المادي إلى مبنى أو منشأة أو مورد أو معلومات مخزنة. بالإضافة إلى ذلك، فهو يتضمن إرشادات بشأن كيفية تصميم الهياكل لمقاومة الأعمال العدائية المحتملة. يمكن أن يكون الأمن المادي بسيطًا مثل الباب المغلق أو معقدًا مثل طبقات متعددة من الحواجز، وحراس الأمن المسلحين، ووضع حراسة.

يهتم الأمن المادي في المقام الأول بتقييد الوصول المادي من قبل الأشخاص غير المصرح لهم (يتم تفسيرهم عادة على أنهم دخلاء) إلى المرافق الخاضعة للرقابة، على الرغم من وجود اعتبارات وحالات أخرى تكون فيها تدابير الأمن المادي ذات قيمة (على سبيل المثال، تقييد الوصول داخل منشأة أو إلى أصول محددة، و الضوابط البيئية للحد من الحوادث المادية، مثل الحرائق والفيضانات).

لا مفر من أن يؤدي الأمن إلى تكاليف ولا يمكن أن يكون كاملاً؛ يمكن أن يقلل الأمن من المخاطر ولكن لا يمكنه القضاء عليها تمامًا. نظرًا لأن الضوابط غير كاملة، فإن الأمان المادي القوي يطبق مبدأ الدفاع في العمق باستخدام مجموعات مناسبة من الضوابط المتداخلة والتكميلية. على سبيل المثال، تهدف ضوابط الوصول المادي للمرافق المحمية عمومًا إلى:

- ردع الدخلاء المحتملين (على سبيل المثال، علامات التحذير وعلامات المحيط)؛
- التمييز بين الأشخاص المصرح لهم وغير المصرح لهم (على سبيل المثال، استخدام بطاقات المرور والمفاتيح)؛
- تأخير وإحباط ومنع محاولات التسلل بشكل مثالي (على سبيل المثال، الجدران القوية وأقفال الأبواب والخزائن)؛
- كشف الاختراقات ومراقبة / تسجيل المتسللين (على سبيل المثال، أجهزة إنذار الدخلاء وأنظمة الدائرة التلفزيونية المغلقة)؛ و
- إطلاق استجابات مناسبة للحوادث (على سبيل المثال، من قبل حراس الأمن والشرطة).

تنطبق الضوابط البيئية بشكل أساسي على المرافق التنظيمية التي تحتوي على تركيزات لموارد النظام (على سبيل المثال، مراكز البيانات وغرف الكمبيوتر المركزية وغرف الخادم وغرف الاتصالات). الضوابط البيئية غير الكافية، خاصة في البيئات القاسية للغاية، يمكن أن يكون لها تأثير سلبي كبير على توافر الأنظمة ومكونات النظام اللازمة لدعم المهمة التنظيمية ووظائف الأعمال.

ح. صلاحية التحكم صلاحية الدخول

يشير التحكم في الوصول إلى ممارسة التحكم في من يمكنه التفاعل مع مورد. في كثير من الأحيان ولكن ليس دائمًا، هذا ينطوي على سلطة تقوم بالسيطرة. يمكن أن يكون المورد عبارة عن مبنى معين أو مجموعة من المباني أو أنظمة تقنية المعلومات. التحكم في الوصول - سواء كان ماديًا أو منطقيًا - هو في الواقع ظاهرة يومية. يعد قفل باب السيارة في الأساس شكلاً بسيطًا من أشكال التحكم في الوصول. يعد رقم التعريف الشخصي على نظام الصراف الآلي في البنك وكذلك الأجهزة البيومترية وسائل أخرى للتحكم في الوصول. يعد امتلاك التحكم في الوصول أمرًا ذا أهمية قصوى عندما يسعى الأشخاص إلى تأمين معلومات ومعدات مهمة أو سرية أو حساسة. يضمن التحكم في الوصول ذلك[71]

- يتم إصدار الهويات وبيانات الاعتماد وإدارتها والتحقق منها وإبطالها وتدقيقها للأجهزة والمستخدمين والعمليات المصرح لها؛
- إدارة وحماية الوصول المادي إلى الأصول؛
- تتم إدارة الوصول عن بُعد - إذا تم استخدامه من قبل المنظمة؛
- تدار أذونات وتصاريح الوصول، بما في ذلك مبادئ الامتياز الأقل وفصل الواجبات؛[72]
- تكامل الشبكة محمي (على سبيل المثال، الفصل بين الشبكات وتجزئة الشبكة)؛
- يتم إثبات الهويات وربطها بأوراق الاعتماد والتأكيد عليها في التفاعلات؛ و
- المصادقة على المستخدمين والأجهزة والأصول الأخرى (على سبيل المثال، عامل واحد، متعدد العوامل) بما يتناسب مع مخاطر المعاملة (على سبيل المثال، مخاطر الأمان والخصوصية للأفراد والمخاطر التنظيمية الأخرى).

تعتبر تقييمات المخاطر التنظيمية وتحمل المخاطر من العوامل المهمة في تحديد سياسات وإجراءات التحكم في الوصول. يجب أن تكون سياسات وإجراءات التحكم في الوصول لمورد معين مناسبة لمستوى التأثير (أي فقدان السرية و / أو النزاهة و / أو التوافر) لخرق أمني لذلك المورد على المنظمة.

---

[71] مكتب محاسبة الحكومة الأمريكية، *دليل تدقيق ضوابط نظام المعلومات الفيدرالي*، 2009.

[72] يتطلب مبدأ الامتياز الأقل منح كل موضوع مجموعة الامتيازات الأكثر تقييدًا اللازمة لأداء المهام المصرح بها. يحد تطبيق هذا المبدأ من الضرر الذي يمكن أن ينتج عن حادث أو خطأ أو استخدام غير مصرح به لنظام المعلومات. يعتبر الفصل بين الواجبات من الضوابط الأساسية التي تمنع أو تكتشف الأخطاء والمخالفات من خلال إسناد المسؤولية عن بدء المعاملات وتسجيل المعاملات وتسجيل عهدة الأصول للأفراد المنفصلين. يستخدم هذا المبدأ بشكل شائع في مؤسسات تقنية المعلومات الكبيرة بحيث لا يوجد شخص واحد في وضع يسمح له بإدخال تعليمات برمجية احتيالية أو ضارة دون اكتشافها.

في البيئة الحكومية، يعد التحكم في الوصول أمرًا مهمًا لأن العديد من الهيئات الحكومية تعالج البيانات الحساسة ومخاوف الخصوصية تحد من يجب أن يشاهد أجزاء مختلفة من المعلومات. يضمن التحكم في الوصول أن المستخدمين الذين لديهم بيانات اعتماد مناسبة هم فقط من يمكنهم الوصول إلى البيانات الحساسة.

أنا. تطوير أنظمة تقنية المعلومات والاستحواذ عليها وصيانتها

من المهم للمؤسسات تحديد وإدارة مخاطر سلسلة التوريد عند تطوير منتجات وخدمات تقنية المعلومات والحصول عليها. تبدأ سلاسل التوريد بمصادر المنتجات والخدمات وتمتد من تصميم وتطوير وتصنيع ومعالجة وتسليم المنتجات والخدمات إلى المستخدم النهائي. بالنظر إلى هذه العلاقات المعقدة والمترابطة، تعد **إدارة مخاطر سلسلة التوريد** وظيفة تنظيمية مهمة. يتمثل الهدف الأساسي لإدارة مخاطر سلسلة التوريد السيبراني في تحديد وتقييم وتخفيف المنتجات والخدمات التي قد تحتوي على وظائف ضارة محتملة أو مزيفة أو معرضة للخطر بسبب سوء ممارسات التصنيع والتطوير في سلسلة التوريد السيبراني. قد تشمل أنشطة إدارة مخاطر سلسلة التوريد السيبراني ما يلي:[73]

- تحديد متطلبات الأمن السيبراني للموردين؛
- سن متطلبات الأمن السيبراني من خلال اتفاق رسمي (مثل العقود)؛
- إبلاغ الموردين بكيفية التحقق من متطلبات الأمن السيبراني والتحقق من صحتها؛
- التحقق من تلبية متطلبات الأمن السيبراني من خلال مجموعة متنوعة من منهجيات التقييم، بما في ذلك تقارير مركز العمليات الأمنية، إن وجدت؛ و
- تنظيم وإدارة الأنشطة المذكورة أعلاه.

الصيانة المستمرة مطلوبة بعد التطوير الناجح أو الحصول على منتج أو خدمة تقنية المعلومات. تتضمن صيانة نظام تقنية المعلومات خلال دورة حياته التغييرات والتحديثات على النظام (على سبيل المثال، تثبيت التصحيحات) نتيجة للمتطلبات الجديدة وإصلاح أخطاء النظام والتحسينات التي تم إجراؤها كنتيجة للواجهات الجديدة.

لتثبيت التصحيحات، يجب على المؤسسات استخدام **إدارة التصحيح**. إدارة التصحيح هي عملية تحديد واكتساب وتثبيت والتحقق من تصحيحات المنتجات والأنظمة. تصحح مشاكل الأمان والوظائف في البرامج والبرامج الثابتة. من منظور أمني، غالبًا ما تكون التصحيحات ذات أهمية لأنها تخفف من ثغرات البرمجيات الخاطئة؛ تطبيق التصحيحات للقضاء على نقاط الضعف هذه يقلل بشكل كبير من فرص الاستغلال.[74]

ي. حادث أمن تقنية المعلومات وإدارة الأحداث

كما هو مذكور في الفصل 4 بشأن عمليات تقنية المعلومات، فإن إدارة الحوادث هي الأنظمة والممارسات المستخدمة لتحديد ما إذا كانت الحوادث أو الأخطاء يتم تسجيلها وتحليلها وحلها في الوقت المناسب. في مجالات أمن الكمبيوتر وتقنية المعلومات، تتضمن إدارة حوادث أمن تقنية المعلومات مراقبة وكشف الأحداث الأمنية على جهاز كمبيوتر أو شبكة كمبيوتر، وتنفيذ الاستجابات المناسبة لتلك الأحداث. إدارة حوادث أمن تقنية المعلومات هي شكل متخصص من أشكال إدارة الحوادث.

يجب على المنظمات إنشاء عملية رسمية للاستجابة للحوادث وخطة وسياسة. تتكون عملية الاستجابة النموذجية للحوادث من أربع مراحل:

- **تحضير**. تتضمن هذه المرحلة إنشاء وتدريب فريق الاستجابة للحوادث؛ إنشاء القدرة على الاستجابة للحوادث حتى تكون المنظمة جاهزة للاستجابة للحوادث؛ ومنع الحوادث من خلال ضمان أن الأنظمة والشبكات والتطبيقات آمنة بشكل كافٍ من خلال تطبيق ضوابط أمنية مدروسة بالمخاطر على أنظمة المعلومات.
- **الكشف والتحليل**. تتضمن هذه المرحلة الكشف عن الحوادث من خلال مجموعة متنوعة من الوسائل بمستويات متفاوتة من التفاصيل والدقة. تشمل وسائل الكشف أنظمة الكشف عن التسلل والوقاية المستندة إلى الشبكة والقائمة على المضيف، وبرامج مكافحة الفيروسات، وأجهزة تحليل السجلات، وتقارير المستخدم. بمجرد اكتشاف حادثة ما، يجب أن يعمل فريق الاستجابة للحوادث في المنظمة بسرعة لتحليل كل حادثة والتحقق من صحتها، باتباع عملية محددة مسبقًا وتوثيق كل خطوة يتم اتخاذها.
- **الاحتواء والاستئصال والتعافي**. عند الكشف، يجب على المنظمات أن تسعى جاهدة لاحتواء الحادث. جزء أساسي من عملية الاحتواء هو اتخاذ القرار (على سبيل المثال، إيقاف تشغيل النظام، وفصله عن الشبكة، وتعطيل وظائف معينة). مثل هذه القرارات يكون أسهل بكثير لاتخاذها إذا كانت ثمة استراتيجيات وإجراءات محددة سلفا لاحتواء الحادث. يوفر احتواء الحادث وقتًا للمنظمة لتطوير استراتيجية علاجية مخصصة.

  عند الاحتواء، قد يكون الاستئصال ضروريًا للقضاء على مكونات الحادث، مثل حذف البرامج الضارة وتعطيل حسابات المستخدمين المخترقة، وكذلك تحديد وتخفيف جميع نقاط الضعف التي تم استغلالها.

---

[73] المعهد الوطني للمعايير والتقنية، *إطار عمل تحسين الأمن السيبراني للبنية التحتية الحرجة*، الإصدار 1.1، 2018.

[74] المعهد الوطني للمعايير والتقنية، *منشور خاص 800-40، مراجعة. 3: دليل لتقنيات إدارة تصحيح المؤسسات*، 2013.

أثناء الاسترداد، يقوم المسؤولون باستعادة الأنظمة إلى التشغيل العادي، والتأكد من أن الأنظمة تعمل بشكل طبيعي، و (إن أمكن) معالجة الثغرات الأمنية لمنع وقوع حوادث مماثلة. قد يتضمن الاسترداد إجراءات مثل استعادة الأنظمة من النسخ الاحتياطية النظيفة، وإعادة بناء الأنظمة من البداية، واستبدال الملفات المخترقة بإصدارات نظيفة، وتثبيت التصحيحات، وتغيير كلمات المرور، وتشديد أمان محيط الشبكة (على سبيل المثال، قواعد جدار الحماية وقوائم التحكم في الوصول إلى جهاز التوجيه الحدودي).

- **نشاط ما بعد الحادث**. بعد حل حادث ما، يجب على المؤسسات توصيل الخبرة لموظفي تقنية المعلومات ذوي الصلة والاستفادة منها كفرصة للتعلم والتحسين. تشمل أنشطة ما بعد الحادث عقد جلسات للدروس المستفادة، وجمع بيانات الحادث، والاحتفاظ بالأدلة، ومراجعة عمليات الاستجابة للحوادث بناءً على الدروس المستفادة من الحادث.

ك. إدارة استمرارية العمل

تخطيط استمرارية الأعمال هو العملية التي تستخدمها المنظمة لتخطيط واختبار استعادة عملياتها التجارية بعد حدوث اضطراب. ويصف أيضًا كيف ستستمر المنظمة في العمل في ظل الظروف المعاكسة التي قد تنشأ (على سبيل المثال، الكوارث الطبيعية أو غيرها من الكوارث). لُطفًا راجع الفصل 4 لمزيد من المعلومات بشأن إدارة استمرارية الأعمال.

ل. الالتزام

يجب على مدقق تقنية المعلومات مراجعة وتقييم الامتثال لجميع المتطلبات الداخلية والخارجية (على سبيل المثال، القانونية والبيئية وجودة المعلومات، والائتمانية والأمنية).

ثالثا. المخاطر على الهيئة الخاضعة للرقابة

تُمكِّن سياسات وإجراءات أمن تقنية المعلومات وإنفاذها المؤسسة من حماية البنية التحتية لتقنية المعلومات الخاصة بها من المستخدمين غير المصرح لهم. تحدد سياسة أمن تقنية المعلومات لمؤسسة ما المتطلبات عالية المستوى للمؤسسة وموظفيها لاتباعها بغية حماية الأصول الهامة. كما يوفر تدريبًا للموظفين على قضايا الأمن ويضمن اتباعهم للإجراءات المعمول بها للوصول إلى البيانات والتحكم فيها. بالإضافة إلى ذلك، تشير سياسة تقنية المعلومات إلى القوانين واللوائح الأخرى التي يتعين على المنظمة اتباعها. ثمة العديد من المعوقات التي تواجه المنظمات فيما يتعلق بتنفيذ نظام فعال لأمن المعلومات. بدون حوكمة فعالة للتعامل مع هذه العقبات، سيكون لأمن تقنية المعلومات مخاطر أكبر للفشل في تحقيق أهداف المنظمة.

تواجه كل منظمة تحدياتها الفريدة من نوعها حيث تختلف القضايا البيئية والسياسية والجغرافية والاقتصادية والاجتماعية الفردية الخاصة بها. يمكن أن تشكل أي من هذه المشكلات عقبات أمام توفير حوكمة فعالة لتقنية المعلومات، وتقع على عاتق مدقق تقنية المعلومات مسؤولية توضيح مخاطر أمن المعلومات للإدارة.

فيما يلي أمثلة على المخاطر الكبيرة التي تم تحديدها في معظم المؤسسات:

- الكشف غير المصرح به للمعلومات،
- التعديل غير المصرح به أو إتلاف المعلومات،
- هجوم نظام المعلومات،
- تدمير البنية التحتية لنظام المعلومات،
- تعطيل الوصول إلى أو استخدام المعلومات أو نظام المعلومات،
- تعطيل معالجة نظام المعلومات، و
- سرقة المعلومات أو البيانات.

عند تقييم تعرض المؤسسات الخاضعة للرقابة للمخاطر، ينبغي إيلاء اهتمام خاص للمجالات التالية:

- استراتيجيات أمن المعلومات غير المتوافقة مع تقنية المعلومات أو متطلبات العمل؛
- لا يتم تطبيق السياسات بشكل موحد مع تطبيق مختلف؛
- عدم الامتثال للمتطلبات الداخلية والخارجية؛
- أمن المعلومات غير مدرج في صيانة حافظة المشاريع وعمليات التطوير؛

- تصميم معماري ينتج عنه حلول غير فعالة أو غير فعالة أو مضللة لأمن المعلومات؛
- عدم كفاية تدابير الأمن المادي وإدارة الأصول؛
- تكوين تطبيق نظام الأجهزة غير الكافي؛
- التنظيم غير الفاعل لعمليات أمن المعلومات وهيكل مسؤولية أمن المعلومات غير المحدد أو المربك؛
- حلول الموارد البشرية غير المناسبة؛
- الاستخدام غير الفاعل للموارد المالية المخصصة لأمن المعلومات وقيمة أمن المعلومات (التكلفة والفائدة) وهيكل لا يتماشى مع احتياجات العمل أو أهدافه؛ و
- أمن المعلومات لا تتم مراقبته أو مراقبته بشكل غير فعال.

عند إجراء تدقيق لأمن المعلومات، يجب على المدقق معالجة القضايا المتعلقة بالنطاقات الـ 12 المذكورة سابقًا في أمن المعلومات.[75] يجب أن يبدأ المدقق بتقييم مدى كفاية طرق تقييم المخاطر وأن يأخذ في الاعتبار قضايا المراجعة المتعلقة بتنفيذ أمن المعلومات. ستساعد مصفوفة المراجعة المراجع على طرح أسئلة المراجعة ومعايير التقييم والوثائق المطلوبة والتحليل الفني الذي سيتم استخدامه. في النهاية، قد يقوم المدقق بتطوير برنامج تدقيق مفصل وفقًا للاحتياجات والتطور أثناء العمل الميداني للتدقيق.

رابعا المراجع وقراءات إضافيةٍ

سيشونسكي وبول وتوماس ميلار وتيم جرانس وكارين سكاروني. NIST Special Publication 800-61، rev 2: *دليل التعامل مع حوادث أمن الكمبيوتر*.
2012 https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final.

ISACA ITAF. *إطار الممارسات المهنية لضمان تقنية المعلومات*. الولايات المتحدة الأمريكية، 2008.

إيساكا. *إطار عمل مخاطر تقنية المعلومات*. 2020https://www.isaca.org/bookstore/bookstore-risk-digital/ritf2.

إيساكا. *إطار عمل COBIT 5*. https://www.isaca.org/bookstore/cobit-5/wcb5. 2012

إيساكا. *برنامج تدقيق / ضمان أمن المعلومات*. 2010.

إيساكا. *برنامج تدقيق / ضمان إدارة مخاطر تقنية المعلومات*. 2012.

المنظمة الدولية للتوحيد القياسي / اللجنة الكهروتقنية الدولية. *ISO / IEC 27000: نظام إدارة أمن المعلومات*.
2013 https://www.iso.org/standard/54534.html.

المنظمة الدولية للتوحيد القياسي / اللجنة الكهروتقنية الدولية. *ISO / IEC 27005: إدارة مخاطر أمن المعلومات*.
2018 https://www.iso.org/standard/75281.html.

المعهد الوطني للمعايير والتقنية. *منشور معايير معالجة المعلومات الفيدرالية 199: معايير التصنيف الأمني لأنظمة المعلومات والمعلومات الفيدرالية*.
فبراير 2004 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

المعهد الوطني للمعايير والتقنية. *إطار عمل تحسين الأمن السيبراني للبنية التحتية الحرجة*، الإصدار 1.1.
2018 https://www.nist.gov/cyberframework/framework.

المعهد الوطني للمعايير والتقنية. *منشور خاص 800-40، مراجعة. 3: دليل لتقنيات إدارة التصحيح للمؤسسات*.
2013 https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final.

المعهد الوطني للمعايير والتقنية. *المنشور الخاص 800-39: إدارة مخاطر أمن المعلومات: عرض المنظمة والرسالة ونظام المعلومات*.

[75] المنظمة الدولية للتوحيد القياسي، *نظام إدارة أمن المعلومات ISO 27000 Series*.

.2011 https://csrc.nist.gov/publications/detail/sp/800-39/final

مكتب محاسبة الحكومة الأمريكية. *دليل تدقيق ضوابط نظام المعلومات الفيدرالي (FISCAM)*. .https://www.gao.gov/products/gao-09-232g 2 فبراير 2009.

مكتب محاسبة الحكومة الأمريكية. *أمن المعلومات: توضح التهديدات السيبرانية وخروقات البيانات الحاجة إلى ضوابط أقوى عبر الوكالات الفيدرالية*. .https://www.gao.gov/products/gao-15-758t 8 يوليو 2015.

مكتب محاسبة الحكومة الأمريكية. *تقنية المعلومات: تحتاج الوكالات الفيدرالية إلى اتخاذ إجراءات عاجلة لإدارة مخاطر سلسلة التوريد*. GAO-21-171. .https://www.gao.gov/products/gao-21-171 15 ديسمبر 2020.

الفصل 8: ضوابط التطبيق

ما هي ضوابط التطبيق؟

كما ذكرنا سابقًا، فإن الرقابة الداخلية هي عملية مصممة لتوفير تأكيد معقول لذلك

- أن تكون العمليات، بما في ذلك استخدام موارد المنظمة، فعالة وكفؤة؛
- يمكن الاعتماد على التقارير المالية، بما في ذلك تقارير تنفيذ الميزانية والبيانات المالية والتقارير الأخرى للاستخدام الداخلي والخارجي؛ و
- يتم اتباع القوانين واللوائح المعمول بها.

تتكون ضوابط نظام المعلومات من تلك الضوابط الداخلية التي تعتمد على معالجة أنظمة المعلومات وتشمل الضوابط العامة (على مستوى المؤسسة وعلى مستوى النظام)، وضوابط تطبيق عمليات الأعمال، وضوابط المستخدم المعتمدة على تقنية المعلومات (الضوابط التي يقوم بها الأشخاص الذين يتفاعلون مع أنظمة المعلومات).

العمليات التجارية هي الوظائف الرئيسة التي تستخدمها المنظمة لإنجاز مهمتها. تطبيق إجراءات الأعمال عبارة عن مجموعة من الأجهزة والبرامج تُستخدم لمعالجة معلومات الأعمال لدعم عملية تجارية محددة. قد يشمل كلاً من الإجراءات اليدوية والمحوسبة لإنشاء المعاملات ومعالجة البيانات وحفظ السجلات وإعداد التقارير. قد يكون لكل مؤسسة عدد من التطبيقات قيد التشغيل، تتراوح في الحجم من نظام على مستوى المؤسسة يمكن الوصول إليه من قبل كل موظف إلى تطبيق عميل صغير يمكن الوصول إليه من قبل موظف واحد. يمكن أن يكون برنامج التطبيق عبارة عن نظام كشوف المرتبات أو نظام الفواتير أو نظام المخزون أو نظام تخطيط موارد المؤسسة المتكامل.

تعتبر ضوابط تطبيق عمليات الأعمال، والتي يشار إليها عادةً باسم **ضوابط التطبيق**، عناصر تحكم خاصة فريدة لكل تطبيق من تطبيقات تقنية المعلومات. عندما تتم أتمتة العمليات التجارية في تطبيق تقنية المعلومات، يتم أيضًا تضمين قواعد العمل في التطبيق في شكل ضوابط التطبيق. تنطبق على قطاعات التطبيق وتتعلق بكل من المعاملات والبيانات الدائمة. ضوابط التطبيق هي تلك الضوابط على اكتمال ودقة وصلاحية وسرية وتوافر المعاملات والبيانات أثناء معالجة التطبيق.

- يجب أن توفر **ضوابط الاستيفاء** تأكيدًا معقولًا بأن جميع المعاملات التي حدثت هي إسهامات في النظام، وقبولها للمعالجة، ومعالجتها مرة واحدة فقط من قبل النظام، وإدراجها بشكل صحيح في المخرجات.
- يجب أن توفر **ضوابط الدقة**، من بين أمور أخرى، ضمانًا معقولًا بأن المعاملات يتم تسجيلها بشكل صحيح، بالمبلغ / البيانات الصحيحة، وفي الوقت المناسب.
- يجب أن توفر **ضوابط الصلاحية** تأكيدًا معقولًا (1) أن جميع المعاملات المسجلة حدثت بالفعل، وتتعلق بالمنظمة، وتمت الموافقة عليها بشكل صحيح وفقًا لتفويض الإدارة؛ و (2) يحتوي المخرجات على بيانات صالحة فقط.
- يجب أن توفر **ضوابط السرية** ضمانًا معقولًا بأن بيانات التطبيق والتقارير والمخرجات الأخرى محمية ضد الوصول غير المصرح به.
- يجب أن توفر **ضوابط التوفر** ضمانًا معقولًا بأن بيانات التطبيق والتقارير وغيرها من المعلومات التجارية ذات الصلة متاحة بسهولة للمستخدمين عند الحاجة.

تمكن مراجعة ضوابط التطبيق المدقق من تزويد الإدارة بتقييم مستقل لكفاءة وفعالية تصميم وتشغيل الضوابط الداخلية وإجراءات التشغيل المتعلقة بأتمتة عملية الأعمال، وتحديد القضايا المتعلقة بالتطبيق التي تتطلب الاهتمام. في حين أن الضوابط العامة لتقنية المعلومات في مؤسسة ما تحدد نغمة بيئة التحكم الشاملة لأنظمة المعلومات، فإن ضوابط التطبيق مدمجة في تطبيقات محددة لضمان وحماية دقة المعلومات وسلامتها وموثوقيتها وسريتها. على سبيل المثال، يتأكدون من أن بدء المعاملات مرخص بشكل صحيح وأن بيانات الإسهامات الصالحة تتم معالجتها وتسجيلها بالكامل والإبلاغ عنها بدقة. تساعد الضوابط العامة على ضمان أن العمل المنجز لتنفيذ ضوابط التطبيق متناسب مع مخاطر فشلها؛ على سبيل المثال، احتمالية الوصول إلى تكوين مفتاح لعنصر تحكم في التطبيق بواسطة أشخاص غير مناسبين أو تغييره دون إذن أو اختبار مناسب.

نظرًا لأن ضوابط التطبيق ترتبط ارتباطًا وثيقًا بالمعاملات الفردية، فإن اختبارها يمكن أن يزود المدقق بشكل مباشر أكثر بتأكيد على دقة وظيفة معينة. على سبيل المثال، من شأن اختبار الضوابط في تطبيق كشوف المرتبات أن يوفر ضمانًا فيما يتعلق برقم كشوف المرتبات في حسابات العميل. نظرًا لنطاقها الأوسع، فإن اختبار ضوابط تقنية المعلومات العامة للعميل (مثل إجراءات التحكم في التغيير) قد لا يوفر مستوى مماثلًا من الضمان لنفس رصيد الحساب.

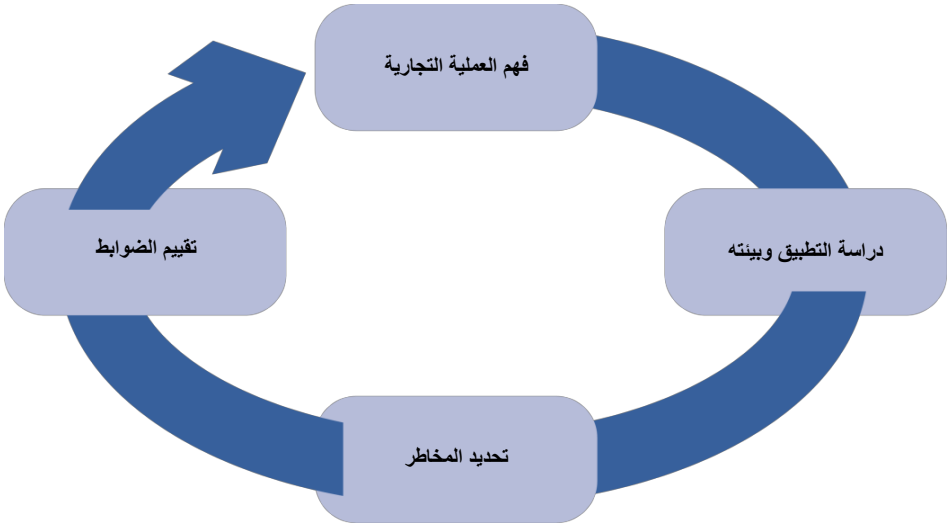
اعتمادًا على أهداف المراجعة المحددة، قد تكون ثمة طرق مختلفة لمراجعة واختبار ضوابط التطبيق. على سبيل المثال، قد تركز مراجعة التطبيق على الامتثال القانوني والمعايير، وفي هذه الحالة يكون الهدف هو التحقق مما إذا كانت ضوابط التطبيق تساعد بشكل صحيح في معالجة هذه المشكلات. بدلاً من ذلك، قد تكون مراجعة التطبيق جزءًا من تدقيق الأداء، وفي هذه الحالة سيكون من المهم معرفة كيفية ترجمة قواعد العمل في التطبيق. أثناء تحليل أمن المعلومات، قد يكون التركيز على ضوابط التطبيق المسؤولة عن ضمان سرية البيانات وسلامتها وتوافرها.

أ. عملية مراجعة مراقبة التطبيق

غالبًا ما تتضمن الخطوات التي يتعين القيام بها في إجراء مراجعة ضوابط التطبيق عملية دورية من الأنشطة. يوضح الشكل 10 الخطوات الشائعة في دورة المراجعة لعناصر تحكم التطبيق. على الرغم من أنه، كما هو موضح بالسهم، من البديهي البدء بفهم أوسع لعملية الأعمال، فمن المهم ملاحظة أنه لا يوجد تسلسل هرمي صارم بين هذه الخطوات.

يتبع الشكل وصفًا موجزًا لكل مرحلة من المراحل الأربع.

شكل10 : دورة مراجعة التطبيق



المصدر: مجهول.

1. فهم عملية الأعمال:

بغية استكشاف المسائل التقنية المتعلقة بالتطبيق، من المفيد أولاً الحصول على نظرة عامة على العمليات التجارية المؤتمتة بواسطة التطبيق - قواعده وتدفقاته والجهات الفاعلة والأدوار ومتطلبات الامتثال ذات الصلة. يعد فهم عملية الأعمال الأساسية خطوة مهمة لتكون قادرًا على التحقق من اتساق ضوابط التطبيق والعمليات الآلية. ستختلف الأنشطة التي تشكل جزءًا من هذه الخطوة وفقًا لهدف المراجعة. وعادة ما يتم ذلك من خلال دراسة إجراءات التشغيل والعمل، أو مخطط تدفق العمليات الخاص بالمنظمة، أو أي مواد مرجعية أخرى. قد يحتاج فريق المراجعة أيضًا إلى مقابلة ومقابلة مديري الأعمال والمديرين التنفيذيين لتقنية المعلومات ومستخدمي التطبيقات الرئيسيين. يمكن لفريق المراجعة أيضًا العثور على قيمة في إنشاء مخططات التدفق الخاصة بهم ومن خلال ملاحظة العمليات والضوابط والأنظمة والواجهات والتقارير التي تشكل العملية. يمكن أن تكون مخططات التدفق التي أنشأها فريق المراجعة مفيدة لأنه غالبًا ما تكون تدفقات العمليات المملوكة للعميل إما معقدة للغاية ومفصلة، أو غير مفصلة بشكل كافٍ، بحيث يمكن فهمها وتحديد الجوانب والمخاطر ذات الصلة في العملية.

2. دراسة التطبيق وبيئته:

بعد اكتساب الوعي بعملية الأعمال، يجب أن يحصل المدقق على فهم للشبكات والأنظمة المحددة المستخدمة لدعم تطبيقات عمليات الأعمال الرئيسة. المعلومات التي تم الحصول عليها خلال هذه الخطوة مهمة للمساعدة في تحديد نقاط التحكم الحرجة ولتوفير أساس لفهم مكان تطبيق الضوابط على مستوى التطبيق. تشمل الأنشطة في هذه الخطوة مراجعة الوثائق (مثل المخططات التنظيمية، ومخططات تدفق البيانات، وأدلة المستخدم)؛ إجراء مقابلات مع الموظفين الرئيسيين؛ إجراء دراسات للوظائف الرئيسة للبرنامج في العمل من خلال المراقبة والتفاعل مع موظفي التشغيل أثناء العمل؛ ومن خلال المناقشات، إجراء جولة تفصيلية لعملية الأعمال والتطبيق من إدخال المصدر وحتى المخرجات والتسوية لمعرفة كيف تتدفق العمليات فعليًا. تسمح هذه الخطوات أيضًا للمراجع بمراقبة أي أنشطة يدوية مرتبطة يمكن أن تكون بمثابة ضوابط تكميلية.

يمكن للمدققين أيضًا الحصول على وثائق بشأن البنية التحتية التقنية (على سبيل المثال، نظام التشغيل؛ بيئة الشبكة؛ نظام إدارة قاعدة البيانات؛ واجهات مع التطبيقات الأخرى؛ مصدر داخلي أو خارجي؛ وإدخال دفعات، في الوقت الفعلي، ومعالجة المعاملات عبر الإنترنت)، والتي يمكنهم مناقشتها مع المديرين والمشغلين والمطورين. يمكن أن تكون هذه المناقشات والوثائق مؤشرًا مفيدًا لكيفية تأثير البنية التحتية على التطبيق.

3. تحديد المخاطر:

بناءً على فهم المراجع الذي تم الحصول عليه في الخطوات السابقة، يجب على المراجع أن يقيم، على أساس أولي، طبيعة ومدى مخاطر أنظمة المعلومات المتعلقة بالتطبيقات الرئيسة. الهدف من هذه الخطوة هو تحديد المخاطر المرتبطة بالنشاط / الوظيفة التجارية التي يخدمها التطبيق، لتحديد الخطأ المحتمل في التطبيق، ومعرفة كيفية معالجة هذه المخاطر من خلال الضوابط الموجودة في البرنامج التطبيقي. قد يكون تقييم مخاطر إجراءات العمل متاحًا بالفعل، من مصادر مثل المراجعة السابقة أو المراجعة الإدارية. يمكن للمراجع الاستفادة من استخدامه بعد تقييم الثقة في تقييم المخاطر القائم.

4. فهم الضوابط وتقييمها:

ضمن كل تطبيق رئيسي لعملية الأعمال، يجب أن يحصل المدقق على فهم لأنواع معينة من ضوابط مستوى التطبيق التي تعتبر مهمة لأهداف المراجعة. بمجرد أن يكون على دراية بالبيئة (التجارية والفنية) المحيطة بالتطبيق، قد يكون المدقق أكثر قدرة على تقييم الضوابط المستخدمة لمعالجة المخاطر القائمة. يجب على المدقق استخدام الحكم عند تقييم ضوابط التطبيق ويجب أن يأخذ في الاعتبار التكاليف والفوائد عند تقديم توصيات للتحسينات. على سبيل المثال، قد تؤدي التفاصيل الزائدة في تسجيل المعاملات إلى زيادة التكاليف العامة، وقد لا تشير إلى المسارات المرغوبة. يتضمن هذا التقييم تقييم ضوابط التطبيق على غرار ما هو موصوف في القسم التالي. قد يحدد المراجع أيضًا أن ثمة أكثر من رقابة واحدة تخفف من نفس المخاطر، مما قد يؤدي إلى توصية تحسين العملية للعميل.

ب. توضيح

للحصول على توضيح لعناصر ضوابط التطبيق، لُطفًا راجع الشكل 11. في تطبيق الدفع عبر الإنترنت، قد يكون أحد شروط الإسهامات هو أن تاريخ انتهاء صلاحية بطاقة الائتمان يجب أن يتجاوز تاريخ المعاملة. قد يكون الآخر هو أن رقم البطاقة يجب أن يكون صالحًا ومطابقًا لكل من اسم حامل البطاقة وقيمة التحقق من البطاقة (رقم CVV) وفقًا لقاعدة بيانات جهة إصدار بطاقة الائتمان. قد يكون آخر هو أن التفاصيل عند إرسالها عبر الشبكة يجب أن تكون مشفرة. الضوابط، مثل تلك المضمنة في التطبيق، ستضمن أن هذه الشروط مصونة وتحقق المعاملات بشكل أفضل.

شكل11 : مثال ضو ابط التطبيق

المصدر: مجهول.

بالإضافة إلى عناصر التحكم الآلية مثل هذه، تتضمن ضوابط التطبيق أيضًا إجراءات يدوية تعمل بالقرب من أحد التطبيقات. لا يتم تضمين عناصر التحكم هذه فقط في تطبيقات محددة، ولكن أيضًا في عمليات الأعمال المحيطة. على سبيل المثال، قد يطلب كاتب إدخال البيانات توقيع نموذج إدخال البيانات (أي الموافقة عليه) قبل إدخاله في الطلب. غالبًا ما يكون الجمع بين عناصر التحكم اليدوية والآلية المختارة نتيجة اعتبارات التكلفة والتحكم عند تصميم التطبيق لأول مرة.

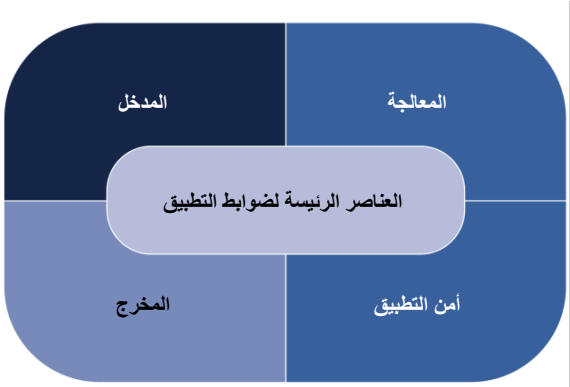
ثانيًا. العناصر الرئيسة لضوابط التطبيق

يمكن تقسيم التطبيق إلى الأجزاء الأولية التالية: إدخال البيانات (إنشاء البيانات وإدخال البيانات)؛ معالجة المعاملات إخراج البيانات (توزيع النتائج) والأمن (التسجيل، الاتصالات، التخزين). يتم تضمين ضوابط التطبيق في كل جزء من التطبيق، إلى جانب عناصر التحكم التي تقيد الوصول إلى التطبيق والملفات الرئيسة.

على الرغم من أنه ليس من الواقعي تقديم خطوات اختبار مفصلة وقوائم مراجعة لكل تبديل ممكن للتطبيق، يجب أن يكون المدقق على دراية بمفاهيم التحكم الشائعة في جميع التطبيقات والعمليات التجارية تقريبًا. يمكن استخدام فهم ضوابط التطبيق الشائعة هذه لتوليد الأفكار والأفكار المتعلقة بخطوات اختبار تدقيق أكثر تحديدًا للتطبيق الذي يتم تدقيقه.

بعض عناصر التحكم الأكثر شيوعًا لكل مجال من المجالات الرئيسة الأربعة موضحة في الشكل 13:

شكل12 : العناصر الرئيسة لضوابط التطبيق



المصدر: مجهول.

شكل13 : أمثلة على ضوابط التطبيق

ضوابط المدخلات	▪ ما هي الأسئلة أو الفرضيات المعينة التي جيب فحصها؟ ▪ إدخال البيانات/فحص المجال (مثل صلاحية أرقام كارت الائتمان الذي تم إدخاله) ▪ إدارة وثائق المصدر (مثل تجهيز الإجراءات والإبقاء عليها) ▪ آليات معالجة الخطأ (رسائل الخطأ، الملفات المعلقة) ▪ قواعد التفويض بإدخال البيانات (مثل الفصل بين المهام)
ضوابط المعالجة	▪ وضع خارطة لقواعد العمل ▪ فحص النزاهة والإبلاغ عن الظروف غير المتزنة ▪ الحسابات المؤتمتة ▪ التوفيق بين المدخلات
ضوابط المخرجات	▪ تمام وتطبيق الدقة وعمليات التوفيق ▪ مراجعة وتعقب المخرجات ▪ مراجعة وتتبع التقارير الاستثنائية المتولدة عن التطبيق ▪ وسم المخرجات، ومعالجتها، والإبقاء عليها، وإجراءات التوزيع
ضوابط أمن التطبيق	▪ آليات التعقب (محاولات التدقيق، مراجعة السجل، استخدام المعرفات المميزة) ▪ التحكم المنطقي في الوصول إلى الوظائف وبيانات التطبيق ▪ حماية البيانات المخزنة

المصدر: مجهول.

أ. ضوابط الإسهامات

تهدف أهداف ضوابط الإسهامات إلى التحقق من صحة أعمال إعداد بيانات المصدر والترخيص والإسهامات والمصادقة عليها بحيث يتم قبول البيانات الدقيقة والموثوقة والكاملة من قبل التطبيق في الوقت المناسب. في حين أن إدخال البيانات يمكن أن يكون يدويًا أو مدفوعًا بواجهة النظام، يمكن التقليل من الأخطاء والسهو من خلال الإسهامات الجيد من التصميم، والفصل الكافي للواجبات فيما يتعلق بإنشاء واعتماد مستندات الإسهامات، ووضع فحوصات الموثوقية والدقة والاكتمال ذات الصلة (مع خيارات القائمة أو رسائل تفاعلية). يستعرض الجدول التالي العناصر الرئيسة للتحكم في الإسهامات.

ضوابط الإسهامات	وصف

عمليات التحقق من إدخال البيانات (الصلاحية، والاكتمال، والشيكات المكررة)	التحقق الآلي من صلاحية البيانات المدخلة (على سبيل المثال، يقع تاريخ الرحلة خارج فترة الحجز المفتوحة)؛ عمليات التحقق من الاكتمال للتأكد من إدخال جميع معلومات المعاملة الرئيسة (على سبيل المثال، تاريخ الرحلة، وأسماء الركاب، وأرقام الهوية هي حقول مطلوبة)؛ الشيكات المكررة تقارن المعاملات الجديدة بالمعاملات التي تم نشرها مسبقًا (على سبيل المثال، التحقق من الفواتير المكررة)؛ والتأكد من أن الإسهامات التي تتجاوز المعايير التي تحددها الإدارة يترتب عليها خطأ.
إدارة وثائق المصدر	توثيق إجراءات إعداد وثيقة المصدر، بما في ذلك استراتيجية محددة لبيانات المعاملات وإجراءات الاحتفاظ بالوثائق؛ يتم تسجيل المستندات المصدر لإسهامات البيانات ويمكن تتبعها؛ يجب أن توفر مستندات المصدر أكواد إدخال محددة مسبقًا لتقليل الأخطاء وتضمين جزءًا من ترخيص الوثيقة.
إجراءات معالجة الخطأ	توجد إجراءات للتعامل مع الإسهامات المرفوضة. (على سبيل المثال، استخدام رسائل الخطأ المناسبة، والمطالبات التي تمكن من إعادة الإسهامات، واستخدام البيانات المعلقة)؛ يتم التحقيق في الأخطاء واتخاذ تدابير التصحيح اللاحقة.
إذن الإسهامات	يلزم وجود إجراءات يدوية وترخيص مستوى إشرافي للبيانات في نموذج إدخال البيانات. (على سبيل المثال، تفاصيل تفويض سجل الدخول من قبل المشرف قبل إدخالها بواسطة كاتب إدخال البيانات للمعالجة في الطلبات الجمركية)؛ يتم اتباع إجراءات الموافقة لإدخال البيانات.

ب. ضوابط المعالجة

يكمن الهدف من معالجة تدابير التحكم في السعي لحماية سلامة البيانات وصلاحيتها وموثوقيتها والحماية من أخطاء المعالجة طوال دورة معالجة المعاملة - من وقت استلام البيانات من نظام الإسهامات الفرعي إلى وقت إرسال البيانات إلى قاعدة البيانات أو الاتصال أو نظام المخرجات الفرعي. كما أنها تضمن معالجة بيانات الإسهامات الصالحة مرة واحدة فقط وأن اكتشاف المعاملات الخاطئة لا يعطل معالجة المعاملات الصالحة. وعند القيام بذلك، فإنهم يسعون إلى تعزيز موثوقية برامج التطبيقات التي تنفذ التعليمات لتلبية متطلبات المستخدم المحددة.

كما وتشمل إجراءات التحكم في هذا المجال أيضًا إنشاء وتنفيذ آليات للسماح ببدء معالجة المعاملات، وفرض استخدام التطبيقات والأدوات المناسبة والمصرح بها فقط، والتحقق بشكل روتيني من أن المعالجة تتم بشكل كامل ودقيق باستخدام الضوابط الآلية، عند الاقتضاء. هذا وقد تتضمن عناصر التحكم التحقق من أخطاء التسلسل والنسخ أو تجاوز سعة المخزن المؤقت، ومراقبة عدد المعاملات / السجلات، وإجراء فحوصات السلامة المرجعية وفحوصات النطاق، ومقارنة إجماليات التحكم والتجزئة.

في أنظمة الوقت الفعلي، فإن بعض عناصر التحكم التعويضية الأخرى المستخدمة هي الفحص الفردي، والتجميع بأثر رجعي، وتقارير الاستثناءات، وتقارير الحساب المعلق. يستعرض الجدول التالي العناصر الرئيسة لضوابط المعالجة.

ضوابط المعالجة	الوصف
وضع خرائط قواعد العمل	فحص التكوينات للتأكد من أن المعاملات يتم تنفيذها وفقًا للمعلمات والتفاوتات المحددة مسبقًا، الخاصة بإدارة مخاطر المؤسسة. توثيق المعلمات والتفاوتات واطلب من الإدارة مراجعة القيود الناتجة بانتظام. التأكد من مطابقة المعاملات مع تصاريح الإدارة.
فحوصات النزاهة والاكتمال	فحص مجموعة مختارة من سجلات النظام للمعاملات. تحديد ما إذا كانت التطبيقات تقوم بإجراء فحوصات التحرير والتحقق المناسبة مقابل البيانات المعالجة، وتنتج رسائل خطأ أو حالات رفض مناسبة، وتبلغ بأخطاء المعالجة للمستخدمين بشكل مناسب.
الحسابات الآلية	تحديد مدى أتمتة وتوحيد معالجة التطبيق للبيانات. فحص وثائق التصميم الداعمة للمعالجة وتحقق من استخدام الإصدارات المناسبة من التطبيقات والبيانات.
تسوية الإسهامات	فحص إجراءات التسوية الدورية لتحديد ما إذا كان قد تم إجراء التسويات وتوثيقها، وفحص بعضها بشكل إضافي للحصول على أدلة داعمة كافية. تحديد ما إذا كان النظام قد تم تكوينه لتحقيق التوازن التلقائي، حيثما أمكن ذلك.

ج. ضوابط المخرجات

أهداف ضوابط المخرجات عبارة عن إجراءات مدمجة في التطبيق لضمان أن مخرجات المعاملة كاملة ودقيقة وموزعة بشكل صحيح. كما أنهم يسعون إلى حماية البيانات التي تتم معالجتها بواسطة تطبيق ما من التعديل والتوزيع غير المصرح بهما.

تشمل عمليات التحكم التحديد المناسب للمخرجات، والتقارير المطلوبة في مرحلة تصميم النظام وتطويره، والتوثيق المناسب لمنطق استخراج التقرير، والضوابط التي تحد من الوصول إلى البيانات المعالجة، ومراجعة المخرجات، والتسوية، والمراجعة. يستعرض الجدول التالي العناصر الرئيسة لعناصرضوابط المخرجات

عناصر ضوابط المخرجات	الوصف
فحوصات النزاهة بغية الإكمال والدقة	إجراء فحوصات سلامة البيانات من خلال تسوية مخرجات العملية مع الإسهامات بغية الدقة والاكتمال، وفقًا للإجراءات الموثقة. مراجعة المخرجات للتأكد من قبولها وإنجازها، بما في ذلك مجاميع التحكم وسجلات الأخطاء. مراجعة حجم المخرجات وقيمتها ونوعها مقابل التوقعات.
مراجعة المخرجات ومتابعتها وتتبعها بما في ذلك النتائج المعالجة	فحص إجراءات الإدارة لتحديد وتعيين المخرجات أو التقارير فيما يتعلق باحتياجات المستخدم النهائي. فحص تقارير تتبع نتائج المعالجة، ومحتوى وتوقيت مراجعات الإدارة للنتائج المعالجة، ودرجة تجاوز مراقبي الإدارة المطبق على المعاملات. مراجعة ومتابعة تقارير الاستثناءات التي تم إنشاؤها بواسطة التطبيق. فحص تقارير المخرجات للامتثال للقوانين واللوائح المعمول بها.
وسم المخرجات، والتعامل معها، وتوزيعها، والاحتفاظ بها	فحص الإجراءات المعمول بها لمراقبة استخدام بيانات المخرجات في تقارير الإدارة أو الاتصالات الخارجية الأخرى وفحص البيانات المختارة من هذه الاتصالات. التأكد من أن وصول المستخدم إلى بيانات المخرجات يتماشى مع دوره.

د. ضوابط أمان التطبيق

يتولى أمان التطبيق الحفاظ على سرية المعلومات وسلامتها وتوافرها في طبقة التطبيق. لغرض مراجعة أمان التطبيق، من المهم فهم الواجهات (أي المصادر المختلفة لإدخال البيانات وإخراجها من التطبيق) وكذلك طريقة تخزين البيانات.

يتم الوصول إلى معظم التطبيقات من خلال معرفات المستخدم الفردية وكلمات المرور إلى التطبيق. بيد أنه، أصبحت أشكال تسجيل الدخول الأخرى شائعة بشكل متزايد، نظرًا لحجم التطبيقات المستخدمة في بيئة الشركة. لذلك، ينبغي فهم تصميم التطبيق لتوفير المستخدم والوصول إليه مقدمًا. على سبيل المثال، قد يحتاج المدقق إلى مراجعة سياسات المنظمة وإجراءاتها للحصول على وصول المستخدم وإلغاءه لفهم قواعد الوصول التي يستخدمها التطبيق. يمكن التحكم في وصول المستخدم محليًا من خلال التطبيق، أو عبر أنظمة متعددة ذات صلة على مستوى المؤسسة باستخدام نظام تسجيل دخول واحد.[76]

لتكون قادرًا على فهم إجراءات التحكم في أمان التطبيق، يحتاج المدقق أيضًا إلى فهم الجهات الفاعلة والأدوار والمسؤوليات التي ينطوي عليها التطبيق، مثل المسؤولين والمستخدمين المتميزين / الحاصلين على امتياز والمستخدمين العاديين. ومن الممكن أن تختلف طريقة التحكم في الوصول للتطبيق ويمكن أن تتضمن معرف مستخدم قياسيًا ونموذج كلمة مرور، واستخدام الشهادات الرقمية لتحديد هوية المستخدم بشكل مؤكد،[77] استخدام رمز أو مقاييس حيوية[78] المعلومات واستخدام طرق متعددة في المصادقة الثنائية أو متعددة العوامل.[79] يمكن التحكم في الوصول لكل وحدة نمطية أو خيار قائمة أو شاشة في تطبيق ما، أو يمكن التحكم فيه من خلال الكائنات والأدوار. يجب على مدقق تقنية المعلومات مراجعة تصميم وحدة التحكم في الوصول، مع الأخذ في الاعتبار أهمية الوظائف / الإجراءات المتاحة.

تتضمن أمثلة المشكلات القابلة للتدقيق المتعلقة بضوابط أمان التطبيقات ما يلي:

- **فحص رقابة المراجعة وإدارة التكوين.** يشمل هذا الفحص إمكانية تتبع المعاملات، مثل تسجيل المعاملات وتسجيل مسار المراجعة؛ تسجيل التقارير والمراقبة؛ والتحكم

[76] يسمح تسجيل الدخول الأحادي للمستخدم باستخدام مجموعة واحدة من بيانات اعتماد تسجيل الدخول للوصول إلى تطبيقات متعددة.

[77] يتم إنشاء الشهادات الرقمية بواسطة مصدر موثوق به لتوفير ضمان بشأن هوية الفرد.

[78] تُستخدم قدرات القياسات الحيوية لتحديد الأفراد بناءً على الخصائص التشريحية والفسيولوجية والسلوكية القابلة للقياس.

[79] تتطلب المصادقة متعددة العوامل نوعين مختلفين على الأقل من عناصر المصادقة بغية الوصول.

في حركة البرامج والبيانات ومكتبات البرامج والوصول إليها؛ وتقييم التغييرات بشكل دوري؛ واستخدام معرفات المستخدم الفريدة والأدوار في إجراء التغييرات. ومن الناحية المثالية، يجب أن يسجل سجل مسار المراجعة ما هي السجلات أو الحقول التي تم تعديلها، ومتى تم تعديلها، ومن ماذا إلى ماذا، ومن قام بالتعديل.

- **فحص ضوابط الوصول**. يتضمن هذا الفحص مراجعة حسابات المستخدمين والأذونات وسياسات إدارة كلمات المرور واستخدام حسابات الضيف والاختبار والحسابات العامة واستخدام حسابات الامتياز والمسؤول والضوابط التعويضية وإجراءات منح وإلغاء الوصول وإجراءات إنهاء الوظيفة وإزالة الوصول واعتماد مبدأ الامتياز الأقل، ووصول فريق تكنولوجيا المعلومات / التطوير إلى قواعد بيانات الإنتاج، والإجراءات الرسمية للموافقة ومنح الوصول، واستخدام كلمات مرور قوية، وتنفيذ التغييرات الدورية، وتشفير كلمة المرور.
- **التحكم في إعداد وصيانة البيانات الرئيسة**. البيانات الرئيسة هي معلومات أساسية يتم مشاركتها بين وظائف التطبيق المتعددة. تشمل الضوابط فحص تكوين البيانات للحقول الرئيسة؛ التأكد من أن التعديلات على البيانات الدائمة مصرح بها ويتم إجراؤها وفقًا لقواعد التغيير الدائمة؛ البيانات الدائمة محدثة ودقيقة ومتسقة عبر المؤسسة؛ والحفاظ على سلامة وسرية البيانات الرئيسة. من أمثلة البيانات الدائمة تفاصيل المورد والعميل (الاسم والعنوان والهاتف ورقم الحساب)؛ معدلات التضخم؛ بيانات إدارة النظام، مثل ملفات كلمات المرور وأذونات التحكم في الوصول.
- **فصل وصول المستخدم**. يجب فصل وصول المستخدم إلى المعاملات والأنشطة المتضاربة، ويجب مراقبة هذا الوصول من خلال إجراءات التشغيل الرسمية والإشراف والمراجعة.
- **التخطيط للطوارئ**. يتضمن هذا التخطيط تقييم مدى أهمية التطبيق وحساسيته، وتقييم الخطوات لمنع وتقليل الضرر المحتمل أو الانقطاع للتطبيق، وتقييم تخطيط الطوارئ الأوسع للمنظمة.

ثالثا. ضوابط نظام إدارة الواجهة والبيانات

بالإضافة إلى ضوابط تطبيق العمليات التجارية المذكورة أعلاه، تلعب ضوابط إدارة الواجهة والبيانات دورًا تكميليًا رئيسيًا في ضمان عمل التطبيقات بشكل صحيح.

أ. ضوابط الواجهة

تؤثر ضوابط الواجهة على كيفية تفاعل تطبيقات العمليات التجارية مع بعضها البعض. وهي تتكون من تلك الضوابط على أ) معالجة المعلومات في الوقت المناسب ودقيقة وكاملة بين التطبيقات وأنظمة التغذية والاستقبال الأخرى على أساس مستمر، و(ب) الترحيل الكامل والدقيق للبيانات النظيفة أثناء التحويل. تؤدي الواجهات إلى تبادل منظم للبيانات بين تطبيقين للكمبيوتر. قد توجد هذه التطبيقات على نفس أنظمة الكمبيوتر أو أنظمة كمبيوتر مختلفة، والتي قد تكون موجودة أو لا توجد في نفس البيئة المادية. الواجهات دورية ومتكررة في طبيعتها.

تتمثل أهداف ضوابط الواجهة في تنفيذ استراتيجية وتصميم فعالين، وتنفيذ إجراءات المعالجة لضمان معالجة الواجهات بشكل كامل ودقيق، وتصحيح الأخطاء، وتقييد الوصول إلى بيانات وعمليات الواجهة بشكل صحيح، وأن البيانات موثوقة وتم الحصول عليها فقط من المصادر المصرح بها. إلى الحد الذي يتم فيه الحصول على إدخال البيانات من التطبيقات الأخرى، يجب تنسيق تقييم المراجع لهذه البيانات مع ضوابط إدخال البيانات المدرجة أعلاه.

ب. ضوابط إدارة البيانات

عادةً ما تقوم التطبيقات التي تدعم عمليات الأعمال بإنشاء البيانات وتجميعها ومعالجتها وتخزينها وتوصيلها وعرضها. غالبًا ما تستخدم التطبيقات التي تتعامل مع أحجام كبيرة من البيانات أنظمة إدارة البيانات لأداء وظائف معالجة بيانات معينة داخل أحد التطبيقات. تستخدم أنظمة إدارة البيانات برامج متخصصة قد تعمل على أجهزة متخصصة. كما تشمل أنظمة إدارة البيانات أنظمة إدارة قواعد البيانات، وبرامج نقل البيانات / الاتصالات المتخصصة (غالبًا ما تسمى البرامج الوسيطة)، والتشفير المستخدم جنبًا إلى جنب مع ضوابط سلامة البيانات، وبرامج مستودع البيانات، وبرامج الإبلاغ / استخراج البيانات. يتم تنفيذ العديد من ضوابط إدخال البيانات ومعالجتها، مثل فحوصات التحرير وفحوصات الوجود والحدود الموضحة في الأقسام السابقة في وظائف أنظمة إدارة البيانات. غالبًا ما يشار إلى هذه الأنواع من الضوابط المطبقة في أنظمة إدارة البيانات على أنها قواعد العمل.

عند تقييم فعالية ضوابط التطبيق، يجب على المدقق تقييم وظائف أنظمة إدارة البيانات الخاصة بعمليات الأعمال قيد المراجعة، بالإضافة إلى الضوابط العامة. في معظم التطبيقات واسعة النطاق و / أو عالية الأداء، توجد مكونات مختلفة لأنظمة إدارة البيانات على خوادم مختلفة، والتي غالبًا ما تستخدم أنظمة تشغيل وتقنيات أجهزة مختلفة. يجب أن يحصل المدقق على فهم للمجموعة المترابطة لتقنيات إدارة البيانات وأن يأخذ في الاعتبار المخاطر ذات الصلة بشكل مناسب.

يعد فهم التصميم المنطقي والبنية المادية لمكونات إدارة البيانات للتطبيق ضروريًا للمدقق لتقييم المخاطر بشكل مناسب. بالإضافة إلى دعم وظائف تخزين البيانات واسترجاعها، من المعتاد أن تستخدم التطبيقات أنظمة إدارة البيانات لدعم الجوانب التشغيلية للتطبيق، مثل إدارة بيانات حالة جلسة المستخدم العابرة، ومعلومات الأمان الخاصة بالجلسة، وسجلات تدقيق المعاملات وغيرها من الوظائف الضرورية لتشغيل التطبيق. يمكن أن تكون عناصر التحكم المرتبطة بهذه الأنواع من الوظائف ضرورية لأمان التطبيق.

يجب أن تشمل الضوابط في نظام إدارة البيانات النظر في مسارات الوصول إلى نظام إدارة البيانات. بشكل عام، يمكن الحصول على الوصول إلى نظام إدارة البيانات مباشرة، من خلال مسارات الوصول التي يسهلها التطبيق، أو من خلال نظام التشغيل الأساسي لنظام إدارة قاعدة البيانات.

تحتوي أنظمة إدارة البيانات على حسابات مميزة مضمنة تُستخدم لإدارة نظام إدارة البيانات وصيانته. هدف المدقق هو تحديد ما إذا كانت الضوابط المناسبة موجودة لتأمين هذه الحسابات المميزة. بالإضافة إلى الحسابات ذات الامتياز، يجب على المدقق الحصول على فهم للدور الذي يلعبه نظام إدارة البيانات في المصادقة والترخيص للتطبيق.

رابعا. المخاطر الطارئة على الهيئة الخاضعة للرقابة

عادة ما تعتمد عواقب إخفاقات التحكم في التطبيق على طبيعة تطبيق الأعمال. ويمكن أن تختلف المخاطر من استياء المستخدم إلى الكوارث الحقيقية وفقدان الأرواح. على سبيل المثال، قد تفقد المنظمة حصتها في السوق إذا أصبحت الخدمة غير متوفرة، وقد تخسر المنظمة المال إذا كانت أنظمة المبيعات عبر الإنترنت تفتقد لأوامر الشراء، وقد تنخفض ثقة المواطنين في الخدمات الحكومية، ويمكن أن يترتب على عدم الامتثال للمعايير القانونية تحريك دعاوى قضائية، وقد لا تصل الكهرباء إلى منازل الأشخاص، وقد تكون الحسابات المصرفية عرضة للاحتيال.

وعلى وجه التحديد، في غياب ضوابط الإسهامات المناسبة، تخاطر المؤسسات بحدوث معالجة خاطئة أو احتيالية وأن التطبيق سيفشل في تحقيق أهداف العمل. في حالة حدوث ذلك، قد تكون البيانات التي تتم معالجتها بواسطة التطبيق غير متسقة وسيتم توفير مخرجات غير صحيحة بواسطة البرامج. ولا يفوتنا في هذا المقام أن نذكر أنه، من الممكن تجاوز ضوابط النظام في مواقف محددة للغاية. في هذه الحالة، يجب أن تكون ثمة عناصر تحكم تعويضية مثل السجلات وقواعد التفويض؛ خلاف ذلك، قد يتم إساءة استخدام امتياز التجاوز ويؤدي إلى إدخال بيانات غير متسقة في التطبيق.

تعد إدارة مستندات المصدر أو تجنب الإذن بإدخال البيانات غير المناسب ضوابط إدخال مهمة أيضًا في التخفيف من المخاطر التي تتعرض لها المؤسسة. في حالة عدم وجود إدارة مناسبة للوثائق المصدر، قد لا يكون من الممكن تتبع مصدر المعلومات في النظام، وقد لا يتحقق الامتثال القانوني، وقد يتم انتهاك سياسات الاحتفاظ، مما يؤدي إلى إدخال بيانات غير موثوقة في التطبيق. على العكس من ذلك، في حالة عدم وجود ضوابط الترخيص، قد تؤدي البيانات غير المصرح بها إلى أخطاء أو احتيال.

قد يؤدي الفشل في معالجة الضوابط إلى أخطاء المعالجة والفشل في تلبية أهداف العمل للتطبيق. قد تظهر هذه الإخفاقات بسبب التعيين غير الصحيح لقواعد العمل، أو الاختبار غير الكافي لرمز البرنامج، أو عدم كفاية التحكم في الإصدارات المختلفة من البرامج لاستعادة تكامل المعالجة بعد حدوث مشكلة أو انقطاع غير متوقع. في حالة عدم وجود ممارسات مراقبة المعالجة الضرورية، يمكن أن تكون ثمة معاملات خاطئة متكررة تؤثر على أهداف العمل والشهرة.

مع أنظمة المعالجة في الوقت الفعلي، لا تتوفر بعض إجراءات التحكم، مثل تسوية مجاميع دفعات الإسهامات والمخرجات للتأكد من اكتمال الإسهامات والاحتفاظ ببعض مستندات إنشاء البيانات للاحتفاظ بسجل مراجعة الحسابات. بيد أنه، تقوم أنظمة الوقت الفعلي بتضمين عناصر تحكم تعويضية أخرى داخل التطبيق، بما في ذلك اكتمال البيانات التفاعلية، ومطالبات التحقق من الصحة، وتسجيل محاولات الوصول.

يؤدي الافتقار إلى ضوابط المخرجات الكافية إلى مخاطر تعديل / حذف البيانات غير المصرح به، وإنشاء تقارير إدارة مخصصة بشكل خاطئ، وخرق سرية البيانات. أيضًا، ستعتمد نتائج إنشاء مخرجات خاطئة إلى حد كبير على الطريقة التي يتم بها استخدام المعلومات من قبل الشركة.

في سياق أمان التطبيق، قد يجعل عدم كفاية آليات التسجيل من المستحيل تتبع سوء السلوك إلى المؤلفين المحددين. كما أن وعي المستخدم بوجود إجراءات مراجعة التسجيل وآليات الإبلاغ يمكن أن يخفف من مخاطر إساءة استخدام نظم المعلومات. أخطاء البيانات الدائمة لها تأثيرات بعيدة المدى على التطبيق، حيث يمكن استخدام هذه البيانات لمدى كبير جدًا من معاملات التطبيق.

على نطاق أوسع، يمكن أن يؤدي الاستخدام غير الكافي لضوابط أمن المعلومات إلى مخاطر بدرجات متفاوتة من الخطورة، بما في ذلك فقدان الدخل، وتعطل الخدمة، وفقدان المصداقية، وانقطاع الأعمال، وإساءة استخدام المعلومات، والعواقب القانونية، والقضايا القضائية، وإساءة استخدام الملكية الفكرية. تمت تغطية هذه المخاطر والضوابط التخفيفية بمزيد من التفصيل في الفصل السابع الخاص بأمن المعلومات.

رابعا. المراجع والقراءات الإضافية

ديفيس وكريس ومايك شيلر وكيفن ويلر. *تدقيق تقنية المعلومات: استخدام الضوابط لحماية أصول المعلومات*، الطبعة الثانية. 31 يناير 2011.

إيساكا. *الدليل الإرشادي G38 لتدقيق تقنية المعلومات والتأكد منها، ضوابط الوصول*. 2007.

المعهد الوطني للمعايير والتقنية. *الإصدار الخاص 800-53: ضوابط الأمن والخصوصية لأنظمة المعلومات والمنظمات*، مراجعة. 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. سبتمبر 2020.

مكتب المراقب المالي والمراجع العام في الهند. *دليل تدقيق تقنية المعلومات*، المجلد. ا. https://ag.ap.nic.in/GSSA/PDF_Files/ITAM Vol_I.pdf.

مكتب محاسبة الحكومة الأمريكية. *دليل تدقيق نظم المعلومات الفيدرالية (FISCAM)*. https://www.gao.gov/products/gao-09-232g. 2 فبراير 2009.