GUID 5100

توجيهات بشأن مراجعة نظم المعلومات

التوجيهات الإرشادية

إن الأدلة الإرشادية تصدر عن المنظمة الدولية للأجهزة العليا للرقابة(الإنتوساي) كجانب من إطار الإصدارات المهنية للإنتوساي.

لمزيد من المعلومات في الموقع(www.issai.org)

INTOSAI


INTOSAI

الفهرس

مقدمة 4

الغرض من هذه التوجيهات اإلرشادية 6

التعريفات 7

النطاق 8

تخطيط مراجعة نظم المعلومات 9

إجراء مراجعة نظم المعلومات 14

إعداد التقاريرعن مراجعة نظم المعلومات 19

المتابعة 20

1 مقدمة

1-1 تقدم التوجيهات الإرشادية 5100 الإطار الشامل لإجراء مراجعة نظم المعلومات ضمن إطار الإنتوساي للتوجيهات والإصدارات المهنية. وتهدف التوجيهات الإرشادية 5100 إلى توفير الأساس لتطوير التوجيهات الإرشادية المستقبلية في سلسلة 5100-5109 في مجال موضوع مراجعة نظم المعلومات، وذلك ضمن إطار الإنتوساي للتوجيهات والإصدارات المهنية.

2-1 يتوافق الإطار المحدد في التوجيهات الإرشادية 5100 مع المبادئ الأساسية لمراجعة القطاع العام (المعايير الدولية لأجهزة العليا للرقابة المالية العامة والمحاسبة 100)، والمبادئ الأساسية للتدقيق المالية (المعايير الدولية لأجهزة العليا للرقابة المالية العامة والمحاسبة 200)، ومبادئ مراجعة الأداء (المعايير الدولية لأجهزة العليا للرقابة المالية العامة والمحاسبة 300)، ومبادئ مراجعة الامتثال (المعايير الدولية لأجهزة العليا للرقابة المالية العامة والمحاسبة 400.

3-1 تُعرّف الأجهزة العليا للرقابة المالية والمحاسبة بمراجعة الحكومات والهيئات التابعة لها وفقا الختصاصات المراجعة الخاصة بكل منهما[1]. ومن خالل أنشطتها، تهدف الأجهزة العليا للرقابة المالية والمحاسبة إلى تعزيز مستوى الكفاءة والمساءلة 2 والفعالية والشفافية في الإدارة العام[2]

4-1 اعتمدت الحكومات وغيرها من كيانات القطاع العام باستمرار سبل الابتكارات في مجال تكنولوجيا المعلومات في نظم المعلومات الخاصة بها، وذلك بهدف تعزيز مستوى الكفاءة والفعالية في أدائها وتقديم مختلف الخدمات العامة. ويرجع السبب في ذلك إلى أن تكنولوجيا المعلومات تتيح فرص جمع المعلومات وتخزينها ومعالجتها واسترجاعها وإيصالها إلكترونيًا، بما يخلق بدوره مجا كبيً را لتحسين دقة نظم المعلومات وسريتها وتوقيتاتها. وعالوة على ذلك، تنتقل طريقةً ال تقديم الخدمات العامة بسرعة من الخدمات المادية إلى الإلكترونية، مما يؤدي إلى اضطرار الحكومات إلى العمل كمنصات رقمية توفر الخدمات والبنية التحتية لنظم المعلومات الأخرى التي تعتمد على تكنولوجيا المعلومات.

---

١ معيار المنظمة الدولية لأجهزة العليا للرقابة المالية العامة والمحاسبة «الإنتوساي» رقم ١ - إعالن ليما

٢ A/حدة رقم ٦٦/٢٠٩

5-1 وقد أدى هذا االنتقال إلى نظم المعلومات المحوسبة والمعالجة اإللكترونية بواسطة الكيانات التي تمت مراجعتها في القطاع العام إلى حدوث تغيير كبير في البيئة التي تعمل فيها ألجهزة العليا للرقابة والمحاسبة. هذا إلى جانب الزيادة في إنفاق القطاع العام على تكنولوجيا المعلومات. وهناك أيًضا حاجة إلى ضمان اعتماد ضوابط تكنولوجيا المعلومات الداخلية للحفاظ على سرية البيانات وتكاملها وتوافرها من قبل كيانات القطاع العام. لذا، يصبح من الالزم على ألجهزة العليا للرقابة والمحاسبة القيام بطوير القدرات المالئمة إلجراء فحص شامل للضوابط المتعلقة بنظم المعلومات.

2

الغرض من هذه التوجيهات اإلرشادية

2-1 تضع المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 011 و911 و 111 و311 المبادئ ألاساسية للمراجعة فيما يتعلق بالمراجعة المالي ومراجعة ألاداء ومراجعة االمتثال. وتتعلق المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة هذذ بالمبادئ العامة واإلجراءات والمعايير وتوقعات المراجع. وهي تنطبق أيًضا على عمليات مراجعة نظم المعلومات.

2-2 ويتمثل الهدف من هذه التوجيهات اإلرشادية في تقديم التوجيه للمراجعين حول كيفية إجراء عمليات مراجعة ألاداء و/أو االمتثال المتعلقة بالموضوع المحدد لنظم المعلومات أو حيث قد تكون مراجعة نظم المعلومات جزًءا من مشاركة عملية مراجعة أكبر قد تكون مراجعة مالية أو مراجعة امتثال أو أداء

2-3 وقد يطبق المراجعون محتويات هذه التوجيهات اإلرشادية على مراحل التخطيط والتنفيذ وإعداد التقارير والمتابعة[3] 3 في عملية المراجعة.

٣ المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة ١ ٣

3

التعريفات

1-3 نظم المعلومات: يمكن تعريف نظم المعلومات على أنها مزيج من االنشطة اإلستراتيجية واإلدارية والتشغيلية المشاركة في عمليات جمع المعلومات والتكنولوجيات ذات الصلة ومعالجتها وتخزينها وتوزيعها واستخدامها. وقد تتراوح درجة تعقيد نظام المعلومات هذا من مجرد سجل بسيط تدون فيه قيود استالم االموال ودفعها يدويًا، إلى نظام أكثر تعقيًدا قائم على تكنولوجيا المعلومات، مثل نظام لتقييم الضرائب، تتم فيه أتمتتة جميع العمليات - جمع البيانات)مثل اإلقرارات الضريبية المقدمة من خالل بوابة الويب عبر اإلنترنت(، والتخزين على الخوادم ، ومعالجة التقييم)على أساس البرمجة باستخدام قواعد الضرائب(وتوصيل الطلب الضريبي، واالسترداد واالعتراف)في الوقت الحقيقي أو على فترات زمنية محددة(. تشتمل تكنولوجيا المعلومات على االجهزة والبرامج واالتصال والمرافق االخرى المستخدمة إلدخال البيانات وتخزينها ومعالجتها ونقلها وإخراجها بأي شكل من االشكال.

2-3 يمكن تعريف مراجعة نظم المعلومات على أنها عملية فحص الضوابط المتعلقة بنظم المعلومات التي تعتمد على تكنولوجيا المعلومات، من أجل تحديد حاالت االنحراف عن المعايير، والتي تُحدد بدورها استناًدا إلى نوع المشاركة في المراجعة - أي المراجعة المالية أو مراجعة االمتثال أو مراجعة االداء.

4

النطاق

4-1 يمكن للمراجعين استخدام هذه التوجيهات اإلرشادية إلجراء عمليات مراجعة األلداء و/أو االمتثال بشأن موضوع محدد من نظم المعلومات، وكذلك عندما يكون مراجعة نظم المعلومات جزءًا من مشاركة عملية مراجعة أكبر قد تكون مراجعة مالية أو مراجعة امتثال أو أداء.

4-2 يوفر هذا المبدأ التوجيهي مزيدًا من اإلرشادات حول كيفية معالجة أي عملية مراجعة لنظم المعلومات باستخدام المراجعة المالية / مراجعة األلداء/االمتثال وال يحتوي على أي متطلبات إضافية إلجراء عملية المراجعة.

5

تخطيط مراجعة نظم المعلومات

5-1 قد تتبنى ألجهزة العليا للرقابة المالية والمحاسبة تخطيط المراجعة القائمة على المخاطر بالنسبة لمراجعة نظم المعلومات، وذلك تمشيًا مع العملية الموضحة في المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 011 ،والمعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 911(المراجعة المالي(، والمعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 111(مراجعة ألداء(والمعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 311)مراجعة االمتثال(، حسب أهداف المشاركة في عملية المراجعة.

5-2 تُحدد أعمال مراجعة نظم المعلومات حسب الهدف ونطاق المراجعة. وقد تشمل ألمثلة ما يلي: -

1) تقييم الضوابط العامة ذات الصلة[4] وضوابط التطبيق[5] التي لها تأثير على موثوقية البيانات من نظم المعلومات، والتي بدورها لها تأثير على البيانات المالية للجهة الخاضعة للمراجعة.

2) التأكيد على امتثال عمليات نظم المعلومات للقوانين والسياسات والمعايير المعمول بها في الجهة الخاضعة للمراجعة.

3) التأكيد على أن موارد تكنولوجيا المعلومات تتيح تحقيق ألهداف التنظيمية بكفاءة وفعالية، وأن الضوابط العامة ذات الصلة وضوابط التطبيق فعالة في منع واكتشاف وتصحيح حاالت اإلفراط واإلسراف وعدم الكفاءة في استخدام وإدارة نظم المعلومات.

5-3 بناًء على تقييم المخاطر، يجوز اختيار نطاق مراجعة نظم المعلومات من أي من أو كل المجاالت التالية[6] للجهة الخاضعة للمراجعة:

---

٤ .الضوابط العامة هي إجراءات يدوية أو آلية تهدف إلى ضمان سرية المعلومات وسالمتها وتوافرها في البيئة الفعلية التي يتم من خاللها تطوير نظم المعلومات وصيانتها وتشغيلها

٥ عناصر التحكم في التطبيق هي إجراءات يدوية أو آلية قائمة على تكنولوجيا المعلومات داخل نظام معلومات يؤثر على معالجة المعامالت، وقد تتعلق بالتحقق من صحة بيانات .المدخالت والمعالجة الدقيقة للبيانات وتسليم بيانات المخرجات والضوابط المتعلقة بسالمة البيانات الرئيسية

٦ IEC/I تم تكييف غالبية المجاالت الموصوفة من ٢٧٠٠١

1) السياسة التنظيمية بشأن تكنولوجيا المعلومات[7]

2) هيكل الحوكمة التنظيمية حول موضوع تكنولوجيا المعلومات

3) الضوابط العامة المقدمة في مجال ألعمال الجاري أتمتتها

4) دارة ألصول

5) تطوير وشراء وصيانة نظم المعلومات، بما في ذلك رسم خرائط عمليات ألعمال ومنطق البرمجة المرتبطة بها

6) إدارة عمليات تكنولوجيا المعلومات

7) إدارة البيئة المادية

8) إدارة الموارد البشرية

9) إدارة االتصاالت

10) إدارة أمن المعلومات[8]

11) إدارة المتثال القانوني

12) استمرارية ألعمال وإدارة التعافي من الكوارث

13) إدارة ضوابط التطبيقات

5-4 يجوز لألجهزة العليا للرقابة والمحاسبة باختيار الفترة الزمنية لتحليل المراجعة)على سبيل المثال سنة واحدة، ثالث سنوات، إلخ(في تحديد نطاق مشاركة مراجعة نظم المعلومات. وقد يتم اختيار فترة زمنية مناسبة، والتي تتعلق باألهداف المحددة لمشاركة المراجعة.

5-5 عندما تكون مراجعة نظم المعلومات هي جزء من عملية المراجعة، فقد يضمن الجهاز أن يعمل فريق المراجعة ككل بطريقة متكاملة لتحقيق هدف المراجعة الشامل. لتحقيق التكامل الفعال، قد تنظر ألجهزة العليا للرقابة المالية والمحاسبة فيما يلي: -

1) توثيق شامل لألعمال التي يتعين على مراجعي نظم المعلومات القيام بها

٧ تشمل جوانب إلدارة االستراتيجية ٧

بما في ذلك ألمن السيبراني ٨

2) صياغة بروتوكول لتبادل المعلومات بين مراجعي نظم المعلومات والمراجعين آلخرين؛

3) تحديد نظم المعلومات وأهداف الرقابة التي تدخل في نطاق المراجعة؛

5-6 يجوز لألجهزة العليا للرقابة المالية والمحاسبة ضمان تكّون فريق المراجعة من أعضاء يتمتعون بشكل جماعي بالكفاءة للقيام بمهام مراجعة نظم المعلومات لتحقيق أهداف المراجعة المقصودة.

5-7 يمكن اكتساب المعرفة والمهارات والكفاءة الالزمة من خالل مزيج من التدريب والتوظيف وإشراك الموارد الخارجية، ا للخطة االستراتيجية للجهاز. وفقً

5-8 قد تضمن آلجهزة العليا للرقابة أن لدى فرق التدقيق نظم المعلومات مجتمعة القدرة على:

1) فهم العناصر الفنية لنظام المعلومات القائم على تكنولوجيا المعلومات، بما في ذلك جميع مثيالت التطبيق المستخدمة ذات الصلة كي تكون قادرة على الوصول إلى البنية التحتية لتكنولوجيا المعلومات واستخدامها في عملية المراجعة

2) فهم القواعد واللوائح القائمة والبيئة التي تعمل فيها أنظمة المعلومات التي تعتمد على تكنولوجيا المعلومات في الجهة الخاضعة للمراجعة

3) فهم عملية وضع خرائط عمليات آلعمال في منطق البرمجة لنظام المعلومات الخاصة بالجهة الخاضعة للمراجعة

4) تطبيق معرفة آلعمال ومعرفة تكنولوجيا المعلومات على حد سواء لتقييم خطر التخطي اليدوي لبرنامج النظام أو التهيئة التي تسمح بمعالجة استثنائية للمعامالت

5) تقييم التصميم واختبار الفعالية التشغيلية لضوابط التطبيق في نظم المعلومات ذات الصلة

6) فهم منهجية المراجعة، بما في ذلك معايير المراجعة ذات الصلة واإلرشادات المطبقة على الجهاز

7) فهم معايير أداء / االمتثال لتكنولوجيا المعلومات التي سيتم مقارنة نتائج التدقيق بها ، بما في ذلك أطر إدارة نظم المعلومات، مثل أهداف التحكم للمعلومات والتقنيات ذات الصلة، مكتبة البنية التحتية لتكنولوجيا المعلومات، وإطار عمل بنية المجموعة المفتوحة)TOGAF ،ITIL،COBIT)

8) فهم تقنيات نظم المعلومات لجمع أدلة المراجعة من النظم آللية

9) فهم نظم المعلومات أدوات المراجعة لجمع وتحليل وإعادة إنتاج نتائج هذا التحليل أو إعادة أداء المهام المراجعة

10) الوصول إلى نظم المعلومات واستخدامها للحصول على أدلة المراجعة واالحتفاظ بها

11) الوصول إلى نظم المعلومات واستخدامها أدوات المراجعة لتحليل األلدلة التي تم جمعه

9-5 قد تنظر األلجهزة العليا للرقابة المالية في خيارات مختلفة لتخصيص الموارد البشرية لمشاركات مراجعة نظم المعلومات وقد يتمثل هذا في إنشاء مجموعة مركزية مع متخصصي تكنولوجيا المعلومات الذين يقدمون المساعدة لفرق المراجعة األلخرى في الجهاز األلعلى للرقابة المالية والمحاسبة إلجراء عمليات المراجعة هذه أو نشر متخصصي تكنولوجيا ا للمتطلبات. مع ازدياد عدد أنظمة المعلومات التي تم التعهد بها من خالل عمليات المراجعة، قد تفكر المعلومات وفقً األلجهزة العليا للرقابة المالية والمحاسبة في إنشاء مجموعة أو وظيفة خاصة بمراجعة نظم المعلومات. وقد يُعهد إلى هذه المجموعة بمسؤولية إجراء جميع عمليات مراجعة نظم المعلومات الخاصة بالجهاز األلعلى للرقابة المالية والمحاسبة، والتفاعل مع فرق أخرى في الجهاز ممن لديهم معرفة قديمة بالجهة الخاضعة للمراجعة، وذلك من أجل الحصول على فهم سريع لوظائف الجهة وعمليات األلعمال ذات الصلة. نظ ًرا ألن التكنولوجيا أصبحت أكثر اندما ًجا في نظم المعلومات، فقد تضمن األلجهزة العليا للرقابة المالية والمحاسبة اكتساب جميع المراجعين مهارات مراجعة نظم المعلومات المناسبة.

10-5 قد تستعين األلجهزة العليا للرقابة المالية والمحاسبة بمصادر خارجية مثل االستشاريين في مجال تكنولوجيا المعلومات والمقاولين والمتخصصين والخبراء إلجراء عملية مراجعة نظم المعلومات، في حاالت قيود الموارد. قد تضمن األلجهزة العليا للرقابة أن هذه الموارد الخارجية قد جرى تدريبها وتوعيتها بشكل كا ٍف بشأن المبادئ التوجيهية للسلوك المهني ولعمليات ومنتجات مراجعة نظم المعلومات التي تنطبق على الجهاز، وأن أعمالها تخضع للمراقبة الكافية من خالل عقد موثق أو اتفاق على مستوى الخدمة والمشاركة المناسبة من جانب موظفي الجهاز في مراحل التخطيط والمراجعة وإعداد التقارير والمتابعة. قد تحتاج األلجهزة العليا للرقابة والمحاسبة عندئذ إلى أعضاء فريق من ذوي المهارات والمعرفة داخل الشركة لمراقبة عمل الموارد الخارجية وفرض االلتزام بالمبادئ التوجيهية واتفاقيات مستوى الخدمة.

11-5 للقيام بتقييم المخاطر لنظم المعلومات، يمكن أن يستخدم المراجعون المبادئ المنصوص عليها في المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 001 ،و911 ،و111 ،و311 بواسطة المراجعين باإلضافة إلى تلك المستخدمة في إدارة موضوع محدد لمراجعة نظم المعلومات كما هو موضح أدناه:

1) تتمثل المخاطر الكامنة في احتمال أن تؤدي بعض ميزات نظم المعلومات التي تعتمد على تكنولوجيا المعلومات الخاصة بالجهة الخاضعة للمراجعة، حسب بطبيعتها الخاصة، إلى تأثير سلبي على تقديم الوظيفة المطلوبة من قبل الجهة. على سبيل المثال، ينطوي نظام معلومات الجهة الخاضعة للمراجعة والمطلوب إلتاحة المعلومات لجميع األلعضاء بشكل عام على مخاطر األلداء الكامنة التي قد تتجاوز مستوى الحد األلقصى المتوقع للمستخدم، وقد يخفق نظام المعلومات في االستجابة ولن تكون المعلومات متاحة إلى أي مستخدم. بينما قد تتبنى الجهة

الخاضعة للمراجعة ضوابط لتخفيف المخاطر الكامنة، في كثير من الحاالت، وقد يتوجب على الجهة أن يتسامح ببساطة مع وجود مثل هذه المخاطر، ضمن مستوى خطر مقبول. يمكن تقييم المخاطر الكامنة قبل النظر في تأثير الرقابة أو مخاطر الكشف من قبل المراجعين.

2) تتألف مخاطر التحكم في أنظمة المعلومات من احتمال فشل عناصر التحكم في تكنولوجيا المعلومات المعتمدة لها. على سبيل المثال، قد يعتمد بواسطة الجهة الخاضعة للمراجعة في التخفيف من التأثير الضار المصمم استجابةً نظام المعلومات الخاص بالجهة الخاضعة للمراجعة والمطلوب على ضمان تقييد الوصول إلى البيانات السرية على الموظفين المصرح لهم السيطرة على طلب تقديم اسم مستخدم وكلمة مرور بواسطة الموظفين الذين يحاولون الحصول على حق الوصول. تتمثل مخاطر التحكم في هذا الموقف في كون اسم المستخدم وكلمة المرور غير آمنين بشكل كاف ويمكن تخمينهما من قبل موظفين غير مصرح لهم من خالل محاوالت متكررة، مما قد يؤدي إلى فقدان السرية وتأثير سلبي محتمل على الجهة. ستكون الجهة التي تصر على استخدام كلمات مرور آمنة وغير تافهة تحتوي على مجموعة من الحروف االبجدية واألرقام والرموز الخاصة، وتضمن منع نظام المعلومات وصول اسم المستخدم بعد عدد معين من المحاوالت الفاشلة للوصول، أقل تعرًضا لمخاطر التحكم من جهة أخرى ليس لديها هذه الميزات.

3) تتكون مخاطر االكتشاف من احتمال عدم الكشف عن غياب أو فشل أو عدم كفاية ضوابط تكنولوجيا المعلومات المعتمدة من قبل الجهة، والتي قد يكون لها تأثير سلبي محتمل على الجهة، بواسطة المراجع.

12-5 إلجراء تقييمات مستندة إلى المخاطر لألنظمة التي تعتمد على تكنولوجيا المعلومات، قد تختار االجهزة العليا للرقابة والمحاسبة منهجية مناسبة ألغرضها الخاصة. قد تتراوح هذه المنهجيات بين التصنيفات البسيطة لملف تعريف المخاطر المعلومات في الجهة الخاضعة لمراجعة بأنها مرتفعة ومتوسطة ومنخفضة بناًء لبيئة تكنولوجيا على فهم الجهاز للجهة وبيئتها والحكم المهني لفريق مراجعة أنظمة المعلومات التابع للجهاز االعلى للرقابة والمحاسبة، حسابات أكثر تعقيًدا ورقمية والتي تحدد تصنيف المخاطر استناًدا إلى البيانات الموضوعية التي تم جمعها من الجهة الخاضعة للمراجعة[9] .

13-5 يمكن تحديد مدى أهمية مشكلة مراجعة نظم المعلومات بموجب اإلطار العام لتقرير االهمية في أي من االجهزة العليا للرقابة والمحاسبة. قد يختلف منظور االهمية المادية اعتماًدا على طبيعة على طبيعة مشاركة مراجعة نظم المعلومات.. تحتوي المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 011 و911 و111 و311 على وصف ألهمية 10 المراجعة المالية ومراجعة االداء والمتثال الخاصة بالقطاع العام، والتي سيتم استخالصها من مراجعة نظم المعلومات[10] .

٩ دليل مجموعة العمل حول تدقيق تكنولوجيا المعلومات - مبادرة تطوير اإلنتوساي حول مراجعات تكنولوجيا المعلومات للمؤسسات العليا للرقابة والمحاسبة ٩

١٠ مبادئ المراجعة المالية وفقا للمعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة ٢١١ ،ومبادئ مراجعة االداء وفقا للمعايير الدولية لألجهزة العليا ١٠ للرقابة المالية العامة والمحاسبة ٣١١ ،ومبادئ مراجعة المتثال وفقا للمعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة ٤

6

إجراء مراجعة نظم المعلومات

6-1 قد تقوم ألجهزة العليا للرقابة والمحاسبة بإجراء عمليات مراجعة لنظم المعلومات بما يتماشى مع العملية الموصوفة لمشاركات المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 011 ،والمعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 911(المراجعة المالي(، والمعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 111)مراجعة ألداء(والمعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 311(مراجعة االمتثال(، حسب مقتضى الحال، بناًء على طبيعة المشاركة.

6-2 بالنسبة لمراجعة نظم المعلومات على وجه التحديد، قد يطلب المراجعون التعاون والدعم الالزمين من الجهة الخاضعة للمراجعة في إنجاز عملية المراجعة، بما في ذلك االطالع على السجالت والمعلومات. وقد يحدد المراجعون طريقة الوصول إلى البيانات اإللكترونية بالشكل الالزم للسماح بالتحليل، بالتشاور مع الجهة الخاضعة للمراجعة. وسيكون وضع

6-3 الوصول إلى البيانات خاًصا باألجهزة العليا للرقابة المالية العامة والمحاسبة.

قبل الشروع في تقييم الضوابط في أي من نظم المعلومات، يمكن للمراجعين تطوير فهم بنية النظام والبيانات ألساسية ومصادرها من أجل تحديد أدوات وتقنيات المراجعة المطلوبة.

6-4 في حالة تلقي تفريغات البيانات من الجهة الخاضعة للمراجعة، قد يضمن المراجعون أن يكون كل تفريغ للبيانات[11] مصحوبًا بخطاب من الجهة الخاضعة للمراجعة. قد يحدد خطاب إعادة التوجيه هذا:

١١ يُعّرف تفريغ البيانات على أنه كمية كبيرة من البيانات المنقولة من نظام أو موقع إلى آخر

1) مصدر)من خالل اإلشارة إلى الطابع الزمني لتوليد رقم تفريغ / تجزئة البيانات لتفريغ البيانات(البيانات ألغراض ضمان سالمة البيانات والتوثيق[12] وعدم التنصل[13]

2) 9 .معلمات االستخراج المستخدمة إلنشاء تفريغ البيانات، على سبيل المثال االستعالمات المستخدمة / تشغيل التقارير. إذا لم يتم استالم خطاب إعادة التوجيه هذا من الجهة الخاضعة للمراجعة، فقد يتم إنشاء المستندات الداخلية بواسطة المراجعين مع اإلشارة إلى معلومات مهمة مثل التاريخ الذي تم فيه تسليم البيانات، ومن أي الملفات تم إنشاء ملف تفريغ البيانات، وما إذا كانت البيانات قد تم من بيئة اإلنتاج أو من بيئة أخرى، إلخ.

5-6 يجوز للمراجعين إجراء تقييم لعناصر التحكم في تكنولوجيا المعلومات)الضوابط العامة والتطبيقية(التي اعتمدتها الجهة الخاضعة للمراجعة، من أجل فحص موثوقيتها وكفايتها. يمكن إجراء التقييم باستخدام مزيج مناسب من اأساليب التالية: مقابلة، استبيان، مراقبة، جولة، مخططات تدفق، التقاط البيانات وتحليلها، تحقق، إعادة حساب، إعادة معالجة، تأكيد طرف ثالث. قد يشمل نطاق تقييم ضوابط تكنولوجيا المعلومات فحص يفيد بأنه:

1) تم تحديد سياسة نظم المعلومات واعتمادها وإبالغها

2) تم تطبيق وتشغيل هيكل حوكمة نظم المعلومات

3) تم إجراء جرد ألصول أنظمة المعلومات بشكل دوري وتم تحديد المتطلبات الخاصة بالزيادة واالستبدال واإلزالة

4) تم تطبيق وتشغيل عمليات مشاركة البنية التحتية والخدمات المشتركة لنظم المعلومات مع الجهات العامة اأخرى

5) تم تحديد واعتماد وإبالغ عمليات تطوير واقتناء وصيانة نظم المعلومات)بما في ذلك إدارة التغيير(

6) تم تحديد واعتماد وإبالغ عمليات عمليات تكنولوجيا المعلومات)االستعانة بمصادر داخلية، االستعانة بمصادر خارجية، اتفاقيات الخدمة(

7) تم اتخاذ تدابير لضمان اأمن المادي وظروف العمل الجسدية المقصودة.

8) تم اعتماد تدابير لتدريب الموارد البشرية وتوعيتها لضمان سرية وسالمة وتوافر المعلومات باإلضافة إلى االمتثال لمتطلبات السياسة ونظم هيكل نظم المعلومات.

9) تم اعتماد تدابير لضمان السرية والنزاهة وتوافر مختلف وسائل االتصال والقنوات

---

١٢ يُعّرف التصديق على أنها عملية التحقق من هوية مستخدم - مسرد مصطلحات المراجعة والرقابة على نظم المعلومات

١٣ يتم تعريف عدم التنصل على أنه التأكيد على أنه ال يمكن للطرف فيما بعد رفض البيانات اأصلية؛ تقديم إثبات على سالمة وأصل البيانات ويمكن التحقق منها من قبل طرف ثالث - مسرد مصطلحات المراجعة والرقابة على نظم المعلومات

10) تم اعتماد تدابير إلدارة أمن المعلومات

11) تم اعتماد تدابير إلدارة االمتثال القانوني

12) تم اعتماد تدابير الستمرارية أألعمال وإدارة التعافي من الكوارث

13) ن ضوابط التطبيق المعتمدة في كل نظام معلومات كافية وموثوقة. قد يشمل هذا التقييم تحديد مكونات التطبيق المهمة، وتحديد مدى أهمية التطبيق على الجهة، ومراجعة الوثائق المتاحة، ومقابلة الموظفين، وفهم مخاطر التحكم في التطبيق وتأثيرها على الجهة، وتطوير اختبارات لفحصها كفاية وموثوقية ضوابط التطبيق هذه.

6-6 قد يشمل تقييم الضوابط العامة والتطبيقية سياسات الجهة المدققة وعملياتها وأفرادها وأنظمتها بما يتماشى مع أهداف مراجعة نظم المعلومات.

7-6 اعتماداً على هدف المراجعة، قد يهتم المراجعون بتصميم الضوابط وتنفيذها وفعاليتها التشغيلية. متى كان المراجع معنيًا بتصميم المراقبة، قد تكون المقابلة أو التفتيش على قواعد العمل الموثقة أمًرا كافيًا. متى كان المراجع معنيًا بتنفيذ الضوابط، قد ال يكون التحقيق كافياً وقد يكون من الضروري إجراء تجول أو إجراء تحليل للبيانات إلثبات أن التحكم كما تم تصميمه قد تم تنفيذه. أخيراً، إذا كان المراجع معنيًا بالفعالية التشغيلية للرقابة، فقد يطلب منه اختبار عينة من المعامالت إلثبات أن الرقابة قد عملت بفعالية خالل الفترة ذات الصلة.

8-6 قد ينظر المراجعون أيضاً في كيفية تأثير أألدلة المتعلقة بالضوابط العامة على طبيعة وتوقيت ومدى أألدلة المطلوبة للحصول على تأكيد بشأن تشغيل ضوابط التطبيق. إذا حصل المراجع على أدلة مراجعة كافية ومناسبة فيما يتعلق بفعالية الضوابط العامة التي تدعم الوصول المنطقي للعاملين إلى أنظمة تكنولوجيا المعلومات وإدارة التغيير داخل بيئة اإلنتاج، فقد يكون قادراً على االستنتاج بشأن الفعالية التشغيلية إلجراءات مراقبة التطبيقات آاللية. ويمكن القيام بذلك عن طريق اختبار عينة أصغر من المعامالت ألن فعالية بيئة تكنولوجيا المعلومات العامة توفر أدلة للمراجع على فعالية التحكم في التطبيق في الفترة ذات الصلة. في حالة إجراءات التحكم اليدوي في التطبيق، قد يضطر المراجعون إلى اختبار حجم عينة مناسب لمستوى الثقة المحدد.

9-6 بناء على تقييم ضوابط تكنولوجيا المعلومات، قد يحدد المراجعون المجاالت ذات أألولوية إلجراء اختبار موضوعي، لضوابط تكنولوجيا المعلومات من خالل استخدام مختلف تقنيات المراجعة بمساعدة والذي يتضمن اختباراً مفصالً الكمبيوتر لالستعالم عن البيانات واستخراجها وتحليلها.

يمكن للمراجعين تصميم وتنفيذ االختبارات الفنية من أجل إثبات أهداف المراجعة.يمكن للمراجعين اختيار تقنيات المراجعة بمساعدة الكمبيوتر المناسبة بناء على متطلباتهم.

10-6 يجوز للمراجعين استخدام تقنيات المراجعة بمساعدة الكمبيوتر في تنفيذ تقنيات مراجعة أنظمة المعلومات مثل تحليل سجل المستخدم، وتقرير االستثناءات، احتساب اإلجمالي الميداني، ومقارنة الملفات، والتقسيم الطبقي، وأخذ العينات، وعمليات الفحص المكررة، واكتشاف الثغرات، والشيخوخة، وحسابات الحقل االفتراضية، إلخ. ويشمل استخدام تقنيات المراجعة بمساعدة الكمبيوتر تحليل كميات كبيرة من البيانات وتكرار االختبارات على مجموعات بيانات مختلفة ومع معايير مختلفة وتوثيق آلي الختبارات التدقيق والنتائج ذات الطوابع الزمنية.

11-6 قد ال يكون المراجعون دائ ًما في وضع يسمح لهم بدراسة جميع الحاالت أو المعامالت أو الوحدات النمطية أو نظم تكنولوجيا المعلومات، بالنظر إلى القيود المفروضة على الموارد والمفاضالت بين التكلفة والعائد لعملية المراجعة. في مثل هذه الحالة، قد تعتمد ألجهزة العليا للرقابة والمحاسبة، على أساس االعتبارات المادية، أخذ عينات المراجعة للفحص المفصل الستخالص استنتاجات المراجعة المعقولة. قد تستخدم ألجهزة العليا للرقابة والمحاسبة تقنيات المراجعة المناسبة بمساعدة الكمبيوتر لتنفيذ أنواع مختلفة من أخذ العينات، وتحديد حجم العينة المناسب، اعتما ًدا على المخاطر الكامنة من أجل تزويد المراجع بأساس معقول يمكن من خالله استخالص[14] والتحكمية الكامنة. يتم أخذ عينات المراجعة استنتاجات حول مجموعة البيانات بأكملها، على أساس االستنتاجات المستخلصة من تطبيق إجراءات التدقيق والتحليل إلى نموذج المراجعة. قد ينظر المراجعون في الغرض من إجراء المراجعة وخصائص السكان التي سيتم استخالصها من العينة وتحديد حجم العينة بما يكفي لتقليل مخاطر أخذ العينات ضمن مستوى مقبول. المراجعة في بيئة تكنولوجيا المعلومات قد تسهل تحليل 100 في المئة من السكان، وخاصة في مرحلة التقييم ألولي. ومع ذلك، إلجراء االختبارات الموضوعية، قد تكون العينات ضرورية. عند القيام بأخذ العينات في نطاق المراجعة المالية، يجوز لمراجعي نظم المعلومات تطبيق المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 100 الختيار العينة[15]

12-6 قد يضمن المراجعون أن ألدلة اإللكترونية التي تم جمعها وتوثيقها كافية وموثوقة ودقيقة للحفاظ على مالحظات المراجعة. قد يتألف هذا الدليل اإللكتروني من ملفات البيانات، وسجالت المستخدمين، والنماذج التحليلية، وتقارير نظم المعلومات اإلدارية، وما إلى ذلك، ويمكن جمعها وتخزينها بطريقة مناسبة بحيث تكون متاحة للتأكيد على دقة وصحة عملية المراجعة. قد يكون لألدلة التي تم جمعها أثناء تدقيق أنظمة المعلومات طوابع زمنية وتفاصيل ضرورية تحتوي على خطوات من تحليل البيانات التي تم إجراؤها، بحيث يكون هناك وضوح عند إنشاء ألدلة وتخزينها وتعديلها أخي ًرا للتخفيف من مخاطر التغييرات الالحقة.

13-6 نظم المعلومات يمكن االحتفاظ بوثائق التدقيق وحمايتها من أي تعديل أو حذف غير مصرح به. قد تقوم ألجهزة العليا للرقابة بتطوير معايير جديدة لالحتفاظ بوثائق تدقيق أنظمة المعلومات أو تكييف المعايير الحالية للوفاء بمتطلبات االحتفاظ بالوثائق المتعلقة بتدقيق أنظمة المعلومات. وستكون فترة االحتفاظ التي تم التوصل إليها بمثابة مهمة من اختصاص الجهاز ألعلى للرقابة المالية، والنظام ألساسي الذي يحكم أنشطته. قد يتم إيالء اهتمام خاص للوسائط والشكل والعمر المتوقع ومتطلبات التخزين لهذه البيانات ، للتأكد من أن البيانات قابلة للقراءة في

١٤ المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة ٢٥٣١ ،المراجعة المالية، أخذ عينات المراجعة، ألقسام ٦ إلى ٩.

١٥ المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة ٢٥٣١ ،المراجعة المالية، أخذ عينات المراجعة، ألقسام ٦ إلى ٩.

اإلطار الزمني المحدد في سياسة االحتفاظ بالبيانات وأرشفتها لكل جهاز من االجهزة العليا للرقابة المالية والمحاسبة. قد يستلزم ذلك تحويل البيانات من صيغة إلى أخرى لمواكبة التطورات التكنولوجية والتقادم.

14-6 في حالة فحص التقارير الفنية التي يعدها مدققو الحسابات الخارجيون بشأن مسائل متعلقة بالتكنولوجيا ، يجوز للمراجعين[16] . إذا تم، نتيجة لهذه اعتماد اإلجراءات المناسبة للتأكيد على جوانب االمتثال أو الجوانب المالية أو االداء لهذه التقارير اإلجراءات، االعتماد على محتويات هذه التقارير، فقد يتم الكشف عن حقيقة االعتماد بشكل مناسب.

15-6 تنص المعايير الدولية للرقابة المالية والمحاسبة على أنه يجب على المراجعين إنشاء اتصال فعال طوال عملية المراجعة وإبقاء الجهة الخاضعة للمراجعة على علم بجميع االمور المتعلقة بالمراجعة)راجع المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 111 ،الفقرة 43 .)في عمليات المراجعة التي تنطوي على أعمال تدقيق نظم المعلومات، قد يتم إرسال نتائج مراجعة نظم المعلومات في بعض الحاالت إلى الجهة من خالل خطاب منفصل. في هذه الحاالت، قد يكون من المهم شرح كيف ترتبط نتيجة أعمال المراجعة باالتصاالت االخرى التي تشكل جزء من االداء أو االمتثال وكيف يمكن أن تكون ا من نفس المراجعة المالية أو مراجعة نتائج عمل تدقيق نظم المعلومات وثيقة الصلة بتقرير مراجعة للجهاز االعلى للرقابة المالية والمحاسبة

١٦ عندما يكون النطاق ضمن المراجعة المالية، يجوز للمراجعين استخدام اعتبارات المراجعة لمعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة ٢٤١٢ ١٦ المتعلقة بجهة تستخدم منظمة خدمات

7

إعداد التقاريرعن مراجعة نظم المعلومات

7-1 نظ ًرا ألن مشاركة مراجعة نظم المعلومات ستكون إما المراجعة المالية)المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 911)أو مراجعة األلداء)المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 111)أو مراجعة االمتثال)المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 311 ،)فقد يبحث المراجعون متطلبات ا لذلك. وقد يكون ذلك خاً صا باألجهزة العليا للرقابة المالية العامة والمحاسبة. وبالمثل، قد يكون لكل إعداد التقارير وفقً جهاز من األلجهزة العليا للرقابة المالية العامة والمحاسبة خطوات خاصة بها إلعداد التقارير استنا ً دا إلى األلهمية المادية لنتائج المراجعة. وعلى نفس المنوال، قد ينظر المراجع، أثناء إعداد التقارير عن مشاركة في مراجعة نظم المعلومات، في القيود القانونية والداخلية على الكشف عن المعلومات المالية والتقنية.

7-2 قد يكون المراجعون على دراية بضرورة الحد من استخدام المصطلحات الفنية وحساسية المعلومات المقدمة) مثل كلمات المرور وأسماء المستخدمين ومعرف الهوية والمعلومات الشخصية(في التقرير. على الرغم من الطبيعة التقنية لعملية مراجعة نظم المعلومات، فقد يضمن المراجعون أن يكون التقرير مفهوما تما ً ما من قبل اإلدارة العليا للجهة الخاضعة للمراجعة وأصحاب المصلحة والجمهور العام. قد يُضمن المراجعون مسر ً دا تفصيليًا مناسبًا للمصطلحات الواردة في التقارير، والذي يشير إلى تعريف االختصارات أو المصطلحات مع شرح يستند إلى سيناريو لكيفية عمل هذا في بيئة محكومة.

7-3 قد ينظر المراجعون في التأثير السلبي المحتمل للتقرير بمجرد نشر تقرير مراجعة نظم المعلومات. على سبيل المثال، إذا اكتشف تقرير مراجعة نظم المعلومات بعض المخاطر أألمنية في نظام المعلومات الخاص بجهة خاضعة للمراجعة وتم اإلبالغ عنها قبل اعتماد الضوابط الالزمة للتخفيف من المخاطر، فقد تتعرض نقطة ضعف نظام المعلومات للجمهور. في مثل هذا السيناريو ، قد ينظر المراجعون في خيارات مثل إعداد التقارير فقط بعد اعتماد الضوابط الالزمة، أو عدم اإلبالغ عن المخاطر أألمنية الكاملة بالكامل، من أجل تجنب التأثير السلبي المحتمل على الجهة الخاضعة للمراجعة.

8

المتابعة

8-1 نظ ًرا ألن المشاركة في مراجعة نظم المعلومات مستمدة من واحد أو أكثر من االنواع الرئيسية للمراجعة، فقد ينظر المراجعون في متطلبات المتابعة لمثل هذه االرتباطات الخاصة بالمراجعة على أنها مماثلة لمتطلبات المراجعة المالية)المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 200)ومراجعة االداء)المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 300)ومراجعة االمتثال)المعايير الدولية لألجهزة العليا للرقابة المالية العامة والمحاسبة 400).