

ورقة بحثية حول معيار التدقيق رقم (5300)

الدليل الإرشادي حول تدقيق تكنولوجيا المعلومات

المقدمة :

تناولت هذه الورقة معيار تدقيق تكنولوجيا المعلومات بعجالة و بشكل موجز مع تأكيدي على ضرورة الرجوع للمعيار لفهم المحاور التي تناولها بشكل موسع والتعرف على الصعوبات التي يواجهها مدقق الجهاز الرقابة الاعلى في هذا المجال ، اذ يعتبر المعيار (5300) اول معيار من سلسلة المعايير الدولية التي تقدم الارشادات التوجيهية الخاصة بتدقيق تكنولوجيا المعلومات في اطار عمل معايير الدولية لاجهزة الرقابة العليا (ISSAI)، ويعتبر دليلا ارشاديا و يصنف من معايير المستوى الرابع، كما يحرص هذا المعيار على دمج و ترابط الطبيعة الاساسية الكامنة في عمليات تدقيق تكنولوجيا المعلومات بشكل يتناسب مع الاشكال المختلفة لعمليات التدقيق المحددة على المستوى الثالث في اطار المعايير الدولية لاجهزة الرقابة العليا.

تعريف تدقيق تكنولوجيا المعلومات :

هو فحص و مراجعة نظم تكنولوجيا المعلومات و الرقابة المتعلقة بها للحصول على ضمان او تحديد الانتهاكات للمبادئ العامة و الكفاءة و الاقتصاد و فعالية نظم تكنولوجيا المعلومات و الرقابة ذات الصلة .

الهدف :

ويعتبر المعيار كحجر اساس و دليل للقيام بعمليات تدقيق تكنولوجيا المعلومات و تطوير قدرات تدقيق تكنولوجيا المعلومات و الاستفادة من الموارد المتاحة بهذا المجال ، حيث يقدم ضمانات حول النزاهة و الموثوقية للجهات الخاضعة للتدقيق و الحكومة و الشعب كما يبين مستوى النضج في نظم المعلومات في القطاع الحكومي .

الاطار:

يتصدر المعيار الدولي (5300) سلسلة المعايير (5300 – 5399) المختصة بالارشادات التوجيهية المحددة في مجال تدقيق تكنولوجيا المعلومات للتعامل مع الموضوعات ذات العلاقة والتي يهتم بها مجتمع الانتوساي ، و قد عمل فريق المشروع الذي يضم البرازيل و الهند و اندونيسيا و اليابان و بولندا و الولايات المتحدة على صياغة المعيار الدولي اعلاه لاجهزة الرقابة العليا.

المحتوى :

تم تقسيم المعيار الى فئتين ؛ فئة المتطلبات - المعايير الضرورية لاجراء عملية تدقيق تكنولوجيا المعلومات ذات الجودة ، و فئة التفسيرات – توضح المتطلبات بشكل اكثر سهولة و سلاسة ، كما تم تقسيم المحاور التي قام عليها المعيار و البالغة (32) محور الى مجموعات وهي ؛ المجموعة التي تحوي اطار تدقيق تكنولوجيا المعلومات ؛ و مجموعة المتطلبات العامة المتصلة تحديدا بتدقيق تكنولوجيا المعلومات ، و مجموعة متطلبات محددة (خاصة) لعملية تدقيق تكنولوجيا المعلومات ، و مجموعة تقنيات و ادوات تدقيق تكنولوجيا المعلومات ، و مجموعة متطلبات اعداد التقارير حول عمليات تدقيق تكنولوجيا المعلومات ، كما تم ارفاق ملحق منفصل لتحليل البيانات .

تم استعراض المجموعات اعلاه الواردة بالمعيار بشكل موجز مع محاورها الرئيسية كمايلي:

المجموعة الاولى : اطار عمل تدقيق تكنولوجيا المعلومات :

حيث تحتوي هذه المجموعة على عدة محاور يعتمد عليها المعيار بشكل اساسي وهي :

1- سلطة و نطاق المعيار الدولي (5300) :

يقدم الاطار الشامل الخاص باجراء عمليات تدقيق تكنولوجيا المعلومات من خلال اطار المعايير الدولية لاجهزة الرقابة العليا ، حيث يتوافق مع ؛ المبادئ الاساسية لتدقيق القطاع العام (ISSAI 100) ، والمبادئ الاساسية للتدقيق المالي (ISSAI 200) ، والمبادئ الاساسية لتدقيق الاداء (ISSAI 300) ، و المبادئ الاساسية لتدقيق الالتزام (ISSAI 400) .

2- مقدمة حول عمليات تدقيق تكنولوجيا المعلومات :

عادة ما يشار الى مثل هذه النظم القائمة على اساس تكنولوجيا المعلومات و الاتصالات ، بنظم المعلومات (IS) او نظم تكنولوجيا المعلومات (IT) ، وقد تبنت الجهات الحكومية تكنولوجيا المعلومات و الاتصالات في اداء اعمالها وان اجهزه الرقابة العليا مخولة بالتدقيق على الحكومات و بالتالي اصبحت هذه الاجهزة ملزمة ان تنمي قدراتها للقيام بعمليات تدقيق تكنولوجيا المعلومات

3- التفويضات الممنوحة لعمليات تدقيق تكنولوجيا المعلومات :

عادة تشمل التفويضات العامة الممنوح لاجهزة الرقابة العليا القيام بعمليات تدقيق تكنولوجيا المعلومات ، و قد يكون لبعض الاجهزة تفويضات خاصة لاجراء عمليات تدقيق تكنولوجيا المعلومات او نظم تكنولوجيا المعلومات .

المجموعة الثانية: المتطلبات العامة المتصلة تحديدا بتدقيق تكنولوجيا المعلومات :

و تحتوي هذه المجموعة على عدة محاور وهي :

1. طريقة التدقيق المعتمدة على تحديد المخاطر لتدقيق تكنولوجيا المعلومات :

على المدقق اتباع طريقة التدقيق المعتمدة على المخاطر و يجب تحديد عناصر المخاطر ؛ الكامنة (المتأصلة) كتلك المخاطر التي تكون في صلب النظام ، و مخاطر الرقابة التي فشلت عمليات الرقابة من كشفها ، و مخاطر الاكتشاف المرتبطة بعدم كشف النقص او الفشل في انظمة تكنولوجيا المعلومات ، و يتم استخدام الطرق المناسبة و المنهجيات المتاحة لتقييم تلك المخاطر .

2. الاهمية النسبية :

يجب على اجهزة الرقابة العليا الاخذ بعين الاعتبار بمبدأ الاهمية النسبية في جميع مراحل عمليات التدقيق ومدى تأثيرها على القرارات المتعلقة بطبيعة و توقيت و مدى اجراءات التدقيق و تقييم نتائجها ، و نظرا لتعقيد عملية الربط بين عمليات تقييم المخاطر المستخدمة في التدقيق و المتطلبات الاهمية النسبية لعمليات التدقيق تكنولوجيا المعلومات لا بد من تقييم الاهمية النسبية - لعدم الالتزام - بناء على القدرة على التأثير على قرارات المستخدمين المستهدفين ، و لا بد للمدقق من الوقوف على العلاقة بين التكلفة و المنفعة عند ممارسة التدقيق وكذلك القيود بخصوص الموارد المتاحة .

3. التوثيق :

يجب ان يحتفظ الجهاز الرقابي الاعلى بالوثائق الكافية لعمليات تدقيق تكنولوجيا المعلومات و نتائجها لضمان عدم قيام المدققين الاخرين من ذوي الخبرة من غير المشاركين في عملية التدقيق بتكرار العمليات ، و على المدقق اعداد الوثائق المفصلة و الكاملة بحيث تعمل على تقديم الفهم شامل لعمليات التدقيق بحيث يتم التوصل لنفس الاستنتاجات في حال قام بها مدقق اخر .

4. الكفاءة :

يقدم جهاز الرقابة الاعلى ضمانات حول تشكيل فريق تدقيق يتألف من اعضاء يتمتعون بالكفاءة التي تمكنهم من اداء تدقيق تكنولوجيا المعلومات وفقا للمعايير ، ويمكن اكتساب المعرفة و المهارة و الكفاءة من خلال الجمع بين التدريب و توظيف الخبرة و مشاركة الخبرات الخارجية وفقا للخطة الاستراتيجية .

المجموعة الثالثة: متطلبات المحددة (الخاصة) لعملية تدقيق تكنولوجيا المعلومات :

اما هذه المجموعة فتضم المتطلبات الخاصة لعملية تدقيق تكنولوجيا المعلومات ، حيث تحتوي على عملية التخطيط لتدقيق تكنولوجيا المعلومات وهي المرحلة الاهم من بين جميع مراحل التدقيق وكما هو الحال في انواع التدقيق الاخرى ؛ كالتدقيق مالي او تدقيق التزام او تدقيق اداء ، ويمكن التخطيط لعمليات تدقيق تكنولوجيا المعلومات من قبل الجهاز الاعلى للرقابة بناء على تفويضات قانونية او طلبات تشريعية / تنفيذية او وفقا لمبادرتهم ، حيث تم تناول هذه المرحلة كمايلي :

- التخطيط لعمليات تدقيق تكنولوجيا المعلومات :

يجب على جهاز الرقابة الاعلى ان يخطط لعملية التدقيق على اساس تقييم المخاطر ، ويمكن التخطيط للتدقيق بحيث يتم على ثلاثة مستويات – المستوى الاستراتيجي ، والمستوى السنوي ، و مستوى الفريق ، كما يمكنه المزج بين مستويين او اكثر من المستويات اعلاه. اذ يجب ان تتضمن الخطة الاستراتيجية على مستوى الجهاز الرقابة الاعلى عنصرا يعمل على معالجة عمليات تدقيق تكنولوجيا المعلومات و الاحتياجات المرتبطة بها وفقا لخطة تدقيق شاملة .

كما ينبغي أن تكون الخطة السنوية لتدقيق تكنولوجيا المعلومات وفقا للخطة لاستراتيجية للتدقيق و يجب ان تغطي الامور الهامة و المدرجة في الخطة الاستراتيجية وفقا للاولويات التي تم تحديدها من خلال تقييم المخاطر ، بحيث تتضمن هذه المرحلة من التخطيط اختيار نظام تكنولوجيا المعلومات او الجهة التي ستخضع للتدقيق .

يتم وضع خطة تدقيق على مستوى الفريق وفقا لتقييم المخاطر الواردة في الخطة السنوية و تغطي الامور المدرجة ضمن نطاق المخاطر الهامة التي تم تحديدها في الخطة السنوية والتي تحتوي على برنامج التدقيق المفصل ، ويشمل تدقيق تكنولوجيا المعلومات ؛ و تدقيق حوكمة تكنولوجيا المعلومات ، و تدقيق العمليات الرقابية العامة ، و تدقيق العمليات الرقابية (الخاصة) لتطبيق تكنولوجيا المعلومات ، كما يمكن للمدقق المزج بينها.

- اختيار العينة وفقا للاهداف:

على مدقق تكنولوجيا المعلومات تحديد حجم عينة مناسب للتقليل من مخاطر تحديد العينات الى مستوى منخفض و مقبول على ان تتطابق اهداف تدقيق تكنولوجيا المعلومات مع المخاطر التي تم تحديدها خلال مرحلة تخطيط تدقيق تكنولوجيا المعلومات على مستوى الفريق ، كما يتم تحديد نطاق تدقيق تكنولوجيا المعلومات خلال مرحلة التخطيط لضمان تحقيق الاهداف المرجوة من التدقيق .

- إجراء تقييم لعملية تدقيق تكنولوجيا المعلومات :

وعلى الأجهزة الرقابة العليا ان تتمكن من اجراء عمليات تقييم اداء المدققين المشاركين في عملية التدقيق والعمل على تطوير قدرات المدققين عند القيام بعملية تدقيق تكنولوجيا المعلومات ، وعلى اجهزة الرقابة تخصيص الموارد الملائمة لاجراء عمليات التدقيق تكنولوجيا المعلومات وكما يمكنها استخدام جهات تدقيق خارجية لاجراء عمليات تدقيق عند الضرورة، و يتوجب القيام بمناقشة الجهات الخاضعة للرقابة بنطاق و اهداف و معايير التقييم الخاصة بالتدقيق وذلك قبل البدء في عملية التدقيق .

- تنفيذ عملية التدقيق و الاشراف عليها:

على مدقق تكنولوجيا المعلومات اجراء تقييم اولي لرقابة تكنولوجيا المعلومات في الجهات الخاضعة للتدقيق والانطلاق منها للبدء بجمع ادلة التدقيق الملائمة و الكافية والموثوقة لتحليلها لضمان تحقيق الاهداف المرجوة من التدقيق مع ضرورة تقديم ضمانات حول حصول ادلة التدقيق على طواع زمنية (اظهار وقت اعداد المعلومات وتجميعها وتعديلها) ، وبيان الطرق المستخدمة في تجميع و تخزين ادلة التدقيق و الاحتفاظ بها ، على ان يتم الاشراف على اعمال موظفي التدقيق من قبل الجهاز الرقابة الاعلى و رئيس الفريق و مراجعة عمليات التدقيق بشكل دوري.

- حالات الاحتيال و الفساد و غيرها من الانتهاكات :

ينبغي على مدققي تكنولوجيا المعلومات في جهاز الرقابة الاعلى تحديد و تقييم المخاطر المترتبة على الاحتيال و مدى تأثيرها و ارتباطها باهداف التدقيق ، و اتخاذ الاجراءات اللازمة وفقا للقوانين المعمول بها للتعامل مع اي حالات فساد او احتيال او اي انتهاكات اخرى تم رصدها خلال التدقيق ، كما يجب الوقوف عند مواطن الشك لتقييم احتمالية وقوع حالات الاحتيال و الفساد خلال اجراءات عمليات التدقيق ، وقد يتوجب على مدقق تكنولوجيا المعلومات التواصل مع الاطراف الاخرى خارج الجهة الخاضعة للرقابة بهذا الخصوص.

- القيود والمتابعة :

يتوجب على جهاز الرقابة الاعلى تحديد القيود على عملية التدقيق في كل مرحلة من مراحل التدقيق والتواصل مع المستويات الادارية المناسبة بهذا الخصوص سواء كانت قيود اعتيادية مثل عدم كفاية الفرص للوصول الى البيانات و المعلومات او القصور عمليات التوثيق الملائمة لعمليات الحوسبة ، كما ينبغي على جهاز الرقابة الاعلى متابعة اية تقارير صادرة بخصوص البنود التي يتم التدقيق عليها و الاطلاع على الاجراءات المتخذة من قبل الاطراف المسؤولة للموضوعات المثارة و ان يتم معالجتها في التقارير بشكل ملائم .

المجموعة الرابعة :تقنيات و أدوات تدقيق تكنولوجيا المعلومات :

و تحتوي هذه المجموعة على تقنيات تدقيق تكنولوجيا المعلومات الواردة بالمعيار ، و تتبنى تقنيات التدقيق نشر الطرق و الاجراءات التي من خلالها يمكن التحكم بالبيئة المحيطة بنظام تكنولوجيا المعلومات بحيث يمكن ؛ اعداد الدراسات ، و تجميع الادلة ، و تنفيذ التحليلات اللازمة للحصول على الضمانات عن مدى موثوقة انظمة الرقابة داخل الجهة الخاضعة للتدقيق ، حيث اوجب المعيار على جهاز الرقابة الاعلى نشر هذه التقنيات و مدى توافقها مع طبيعة الالتزامات و المتطلبات التدقيقية المفروضة بناء على اهداف التدقيق الموضوعة في جميع مراحل التدقيق.

ولا بد للمدقق من الفهم الكامل لكيفية قيام كل تطبيق يدعم سير العمليات المنوطة في الجهات الخاضعة للتدقيق قبل البدء بعملية التخطيط ، و تعد تقنيات التدقيق التقليدية كعمليات دراسة الوثائق و اجراء المقابلات مع الموظفين في الجهات الخاضعة ذات فائدة كبيرة تركز الفهم الجيد لكيفية تطبيق الانظمة التكنولوجية بتلك الجهات.

كما تعتبر عملية اختيار التقنيات الخاصة بتنفيذ عمليات التدقيق امرا حيويا في اثناء اجراء اختبارات المصدقية ؛ كالمقابلات و الاستبانات و الملاحظات ، و من اجل تقييم مدى ملائمة انظمة الرقابة المحوسبة مع التقنيات المستخدمة و العمل على نشر تقنيات مشابهة لتلك المستخدمة في الانواع الاخرى من عمليات التدقيق ، ويتم تطبيق تقنيات التدقيق الخاصة بتكنولوجيا المعلومات من خلال تقييم عملية الرقابة الفعلية الموجودة في الجهات الخاضعة للتدقيق و عكس نتائج التقييم على مدى صحة تنفيذ تطبيقات تكنولوجيا المعلومات .

و يتوجب على مدققي تكنولوجيا المعلومات حفظ النتائج التدقيق و توثيق ادلة التدقيق و تخزينها بشكل مناسب ، و ينبغي ان تتصف هذه الادلة بخصائص تعنى بالكفاءة و الشمولية و الموثوقية و الصحة و الدقة وفقا لمعايير ضمان الجودة الداخلية الخاصة بجهاز الرقابة الاعلى ، و على المدقق اتخاذ قرارات المناسبة بخصوص استخدام واحدة او اكثر من تقنيات تكنولوجيا المعلومات التي تعزز النزاهة و تحقق الفائدة المرجوة من عملية التدقيق .

و تتطلب عملية تدقيق تكنولوجيا المعلومات المعرفة الوافية و السليمة من قبل المدقق للعمليات و التقنيات المستخدمة من قبل الجهات الخاضعة للتدقيق بهذا الخصوص و كذلك الاستخدام الكفؤ و الفعال لادوات تدقيق تكنولوجيا المعلومات عند اجراء عملية التدقيق ، و يتم تناول المعلومات المخزنة و معالجتها من خلال استمارات الكترونية و تعقب عمليات التدقيق المحاسبية الغير مرئية ظاهريا .

المجموعة الخامسة :متطلبات اعداد التقارير حول عمليات تدقيق تكنولوجيا المعلومات :

وهي المجموعة الاخيرة المكونة للمعيار والتي تبين كيفية اعداد تقارير التدقيق ، و يجب ان تعكس تقارير تدقيق تكنولوجيا المعلومات نتائج عمليات التدقيق وفقا للأهمية النسبية و مدى توافقها مع اهداف التدقيق و يجب ان يكون التقرير شاملا و متوازنا و سهل القراءة و ان يصدر في الوقت المناسب ، كما ينبغي للمدقق ان يكون على علم تام بجميع محتويات التقرير ؛ الخاصة القيود و المصطلحات الفنية و حساسية المعلومات المقدمة مثل كلمات السر و اسماء المستخدمين الواردة في التقرير .

و يجب ان يحتوي التصميم العام لتقرير تدقيق تكنولوجيا المعلومات على اهداف و نطاق التدقيق ، و الفترة الزمنية المستهدفة في العملية التدقيق ، و معايير و منهجية التدقيق ، و التلخيص و التصنيف الطبقي ، و النتائج النهائية لعملية التدقيق ، و استنتاجات و توصيات التدقيق ، و دراسات الحالة ذات الصلة و المخاطر و القيود و التحفظات و اوجه القصور او المخاوف التي واجهت المدقق بعملية التدقيق التي تم اجرائها.

ولمدقق تكنولوجيا المعلومات مناقشة مسودة التقرير مع ادارة نظام تكنولوجيا المعلومات و ذلك قبل الانتهاء من التقرير و نشره ، و في حال اختلاف مدققي تكنولوجيا المعلومات و الوحدة الخاضعة للتدقيق في الاراء حول بعض التوصيات يجب ان ينص التقرير على موقف الطرفين و اسباب الخلاف و ذلك كملحق للتقرير او اي طريقة اخرى مناسبة ، و يجب على المدقق اعادة زيارة الجهة التي خضعت للتدقيق بعد مرور فترة معقولة من الزمن لضمان تنفيذ جميع التوصيات .

إعداد المدقق

محمد

ديوان المحاسبة

الأردني

الشخاتره