ورقة عن التوجيهات الخاصة بتدقيق أنظمة معلومات إدارة الدّين رقم 5450
مقدمة من ديوان الرقابة المالية الاتحادي العراقي

يهدف هذا الدليل (5450) إلى تزويد المدققين بتوجيهات عن تدقيق أنظمة معلومات إدارة الدين العام فضلا عن رفع قدرة مجموعة العمل على الدين العام WGPD من خلال تزويدها بإطار عمل يمكن استخدامه لتقييم الضوابط العامة وضوابط التطبيق لنظام معلومات إدارة الدين العام.

تأتي أهمية هذا الدليل أو المعيار من أهمية إدارة الدين إذ أن الهدف الرئيس من إدارة الدَّيْن هو توفير تمويل مستقر بأقل تكلفة ممكنة وبمستويات معقولة من المخاطر لأجل استمرار نشاطات الحكومة، يجب على البلدان المعنية بالحصول على إدارة دين عام فعالة، أن تعطي أولوية عالية لتطوير الأنظمة الموثوقة لتسجيل وإصدار التقارير عن معلومات الدَّيْن. يعد هذا ضرورياً ليس فقط من أجل تطوير بيانات الدَّيْن والتأكيد على دفعات خدمة الدَّيْن في الوقت الصحيح، ولكن أيضاً من أجل تحسين جودة إصدار تقارير الميزانية وشفافية الحسابات المالية العامة، مما يسمح لصانعي القرار ومديري الدَّيْن العام بتحقيق الأهداف المتعلقة بالدَّيْن العام ،فضلا عن إدارة الدين العام تهدف بحسب التوجيهات الخاصة بتدقيق أنظمة معلومات إدارة الدين العام ISSAI 5450 الصادرة عن المنظمة الدولية للأجهزة العليا للرقابة والمحاسبة INTOSAI إلى هدف رئيسي آخر هو توفير تمويل مستقر بـأقل تكلفة ممكنة وبمستويات معقولة من المخاطر لأجل استمرار نشاطات الحكومة.

مع تطور تقنية المعلومات أصبحت المؤسسات الحكومية تعتمد بشكل كبير على استخدامها في تنفيذ أعمالها وخدمات التوصيل ومعالجة المعلومات الهامة والمحافظة عليها وإعداد تقارير عنها، حيث يمكن تصنيف تدقيق تقنية المعلومات فيما يتعلق بالتوجيهات الساندة بـ (إدارة تقنية المعلومات، تدقيق البيانات، تدقيق نظام المعلومات ، عقود تقنية المعلومات ، أمن المعلومات) بشكل عام يعمل مدقق تقنية المعلومات بأكثر من توجه واحد ، إلا إن المدقق يستطيع أن يختار التوجه الذي سيكون سائدا ، وفي هذا الدليل فان التوجه السائد هو تدقيق نظام المعلومات.

ويمكن الرجوع إلى ما يخص المعلومات عن الدين العام إلى مجموعة المعايير الصادرة عن منظمة الانتوساي الخاصة بها.

يتكون هذا الدليل من مجموعة من المراحل تتمثل بعناصر (التخطيط ، تقويم الضوابط العامة، تقويم ضوابط التطبيق) ونتناول في أدناه هذه العناصر أ و المراحل التي جاء بها هذ ا الدليل للتعرف على كل مرحله من هذه المراحل :-

1 - التخطيط

تساعد هذه المرحلة المدقق على فهم العمليات المرتبطة بالنظام وأدوات ضبطه والمخاطر المتعلقة بالنظر إلى المخاطر المتأصلة في تدفق عملية الدَّيْن العام ، وبالاعتماد على هذا الفهم، يقوم المدقق بتقييم بيئة الضبط الكلية، ويحدد الأنظمة المستخدمة في إدارة الدَّيْن العام ، ويطلع

على كل الوثائق المتعلقة بهذه الأنظمة، ويقوم بتقييم أولي للمخاطر، وبناء على نتيجة هذا التقييم، سيتم تحديد مدى الإجراءات التي يجب توظيفها في مرحلة الاختبار.
يتوجب على الجهاز الأعلى للرقابة والمحاسبة أن يجري فحصاً لجميع البنى المتعلقة بمكتب الدَّيْن العام ، مثل الموظفين، والعمليات، ونوع الديون، وأمن المعلومات، والأدوات التقنية، والأمور الأخرى.
لقد وضع هذا المعيار جدول على شكل مجموعة من الأسئلة مرفق به يمكن الاسترشاد بها.

2 - الضوابط العامة

توفر الضوابط العامة إطار العمل لمجمل الضوابط من أجل وظائف تقنية المعلومات ، اذ صممت هذه الضوابط للتعامل مع مشاكل التطوير والعمليات والمحافظة على البيئة المعلوماتية ، حيث تهدف الضوابط العامة إلى حماية البيانات وبرامج التطبيقات وضمان استمرار عمليات الحاسوب في حال حدوث عوائق غير متوقعة.
على الرغم من أن تدقيق نظام الدَّيْن العام يحتاج إلى التحقق من الضوابط العامة لتقنية المعلومات ، إلا أن هذه الوثيقة الحالية لا تهدف إلى الإسهاب في هذه القضية وذلك بسبب وجود وثائق أخرى أعدتها منظمة الإنتوساي INTOSAI عن تدقيق تقنية المعلومات والتي تعالج فيها الضوابط العامة لتقنية المعلومات بالتفصيل من المقترح أن يلجأ فريق العمل في حالة القيام بتدقيق للنظام إلى معيار ISSAI 5310 : توجيهات بشأن تدقيق أمن أنظمة المعلومات (ISec) ؛ وهو دليل بخصوص مراجعة أمن أنظمة المعلومات (ISS) في المؤسسات الحكومية.
توجد أيضاً وثيقة أخرى يمكن أن تكون مفيدة في تخطيط الضوابط العامة، وهو كتيب مجموعة العمل على تدقيق تقنية المعلومات WGITA - IDI للأجهزة العليا، والذي يزود مستخدميه بالمعلومات اللازمة والأسئلة الرئيسية من أجل تخطيط فعال لعمليات تدقيق تقنية المعلومات، وتوجد في الملحق المرفق بالمعيار الذ ي سبق المشار إليه مصفوفة اختبار تتضمن بعض الضوابط العامة والاقتراحات لعدد من الاختبارات التي يمكن أن تساعد المدقق على القيام باختبار الضوابط العامة.
إن أي مجموعةً شاملةً من مختلف تصنيفات الضوابط العامة ينبغي أن تتضمن ما يلي:

- الضوابط التنظيمية
- ضوابط الوصول المادية
- ضوابط الوصول المنطقية
- ضوابط البيئة الحاسوبية
- ضوابط تغيير البرامج
- تخطيط استمرارية الأعمال و التعافي من الكوارث

3 - ضوابط التطبيقات

تتم أتمتة ضوابط التطبيقات في تطبيقات أنظمة المعلومات لتساعد على ضمان صحة الإذن والسلامة والدقة وصلاحية المعاملات. يتم تضمين هذه الضوابط داخل برمجة التطبيقات وهي منتشرة في عمليات الإدخال والمعالجة والإخراج التابعة لهذه التطبيقات. إن هدف هذه الضوابط هو ضمان كمال وموثوقية ودقة معالجة البيانات.

تتضمن أمثلة ضوابط التطبيقات: أن تقوم التطبيقات بإجراءات التحقق من صيغة البيانات المدخلة لمنع إدخال البيانات غير الصالحة، وضوابط المعالجة التي تمنع المستخدمين من إدخال العمليات غير المسموح بها، بالإضافة إلى إخراج تقارير مفصلة وضوابط على جميع المعاملات للتأكد من أنها جميعاً مسجلة وكاملة وصحيحة.

ومن الضوابط الخاصة بالتطبيقات التي جاء بها الدليل (5450) ما يلي:

أ - معايير التوثيق

تضمن معايير التوثيق أن يتم الحفاظ على توثيق مناسب ومحدَّث للتطبيقات، كما أن القيام بالتحديث المتقن للتوثيق مهم أيضاً.

يعد التوثيق المناسب مهماً لتحسين فهم ماهية الضوابط الموجودة أو التي يجب أن تطبق. كما يقلل توثيق التطبيقات الجيد من مخاطر عدم اتباع المستخدمين لإجراءات الضبط التي تقرها الإدارة. وسيستفيد المدقق من مراجعة التوثيقات الشاملة والمحدثة لكي يستوعب توثيق التطبيقات: يساعد هذا التوثيق مبرمجي الصيانة على استيعاب التطبيق، وتصحيح المشاكل، وإجراء التحسينات اللازمة. يبنى التوثيق مع كل مرحلة من مراحل عملية التطوير ويمكن إنشا في صيغ مختلفة مثل المخططات الانسيابية أو البيانية أو الجداول أو النصوص. من الممكن أن يتضمن التوثيق تفاصيل عن مصدر البيانات وصفاتها، وشاشات الإدخال، والتأكد من صحة البيانات، وإجراءات الأمن، ووصف الحسابات، وتصميم البرنامج، والربط التطبيقات الأخرى، وإجراءات الضبط، والتعامل مع الأخطاء، وتعليمات التشغيل، والأرشفة، والنسخ الاحتياطي، والتخزين وإجراءات التعافي. يجب أن يتم تحديث توثيق التطبيق كلما تم تعديل هذا التطبيق .كيفية عمل كل تطبيق، وقد يساعده ذلك على ملاحظة وجود مخاطر معينة.

يجب أن يتضمن التوثيق:

- ❖ فكرة عامة عن التطبيق
- ❖ مواصفات متطلبات المستخدمين
- ❖ وصف البرنامج وقوائمه
- ❖ وصف الإدخال والإخراج
- ❖ وصف لمحتويات الملفات
- ❖ دليل المستخدمين
- ❖ تعليمات مكتبية
- ❖ وصف لضوابط أمن التطبيق
- ❖ ملخص حديث لتقييمات الأمن
- ❖ القرارات الأمنية الأخيرة والإجراءات الموصى بها
- ❖ وضع الإجراءات الموصى بها

ب -ضوابط الإدخال

تعد ضوابط الإدخال هامة جداً للتقليل من مخاطر الخطأ أو التزوير في التطبيقات المحوسبة ،إذ تساعد ضوابط الإدخال على التأكد من صحة إقرار البيانات المدخلة في التطبيق ودقتها وكمالها وتوقيتها، و يتم التأكد من صحة إقرار البيانات عن طريق طلب موافقات إضافية للعمليات التي تتجاوز حداً معيناً. ويتم تأكيد دقة البيانات من خلال آليات

التحقق التي تتأكد من صحة البيانات المدخلة قبل الموافقة على معالجة هذه العملية. يتم ضمان كمال البيانات من خلال إجراءات معالجة الخطأ التي تؤمن تسجيل الأخطاء، والإبلاغ عنها وتصحيحها .يتم ضمان دقة التوقيت من خلال مراقبة تدفق المعاملات والتسجيل والإبلاغ عن الحوادث الاستثنائية. يمكن أن توجد ضوابط الإدخال في:

- ❖ شاشات إدخال البيانات
- ❖ روتينات تحضير البيانات
- ❖ السماح بإدخال البيانات
- ❖ الاحتفاظ بمستندات الإدخال
- ❖ التأكد من صحة إدخال البيانات
- ❖ الإجراءات في حال حدوث خطأ في إدخال البيانات
- ❖ آليات دعم إدخال البيانات

ج - ضوابط المعالجة

تضمن ضوابط المعالجة دقة وشمول وتوقيت البيانات أثناء المعالجة سواء كانت على شكل مجموعات أو مباشرة على الشبكة. تساعد هذه الضوابط على ضمان معالجة البيانات بدقة عبر التطبيق وضمان عدم إضافة أو ضياع أو تعديل أي بيانات أثناء المعالجة.

يجب أن تتم الموازنة بين التطبيقات التي تتشارك في البيانات من خلال إعداد تقرير ملاءمة يعدد البيانات في كلا التطبيقين ويرفع تقريراً عن أي اختلافات إلى مجموعة معينة من المستخدمين.

يجب أن تتضمن موازنة المجاميع عداً للعمليات وللمجاميع بالنسبة لكل حقول الكميات ولكل نوع من العمليات، وكذلك يجب أن تتضمن مقارنة بين مجاميع الحقول التفصيلية وبين حقول المجموع العام وفي الملفات التي لا يوجد فيها مجاميع ذات فائدة، يمكن إيجاد مجاميع خليطة Hash Totals تجمع كل الأرقام الموجودة في عمود للتأكد من أن الحصيلة نفسها سيتم قبولها في عملية المعالجة التالية. مثلاً، إن حساب مجموع أرقام اتفاقية الدَّيْن لا يعني شيئاً، لكن يمكن استخدام هذا المجموع للتأكد من أن جميع الأرقام الصحيحة لاتفاقية الدَّيْن قد تم تضمينها في عملية المعالجة.

د - ضوابط المخرجات

يجب أن يتم حماية ملفات المخرجات لتقليل خطر إمكانية حصول التعديلات غير المصرح بها ،إذ تتضمن دوافع تعديل المخرجات الحاسوبية: التغطية على أي معالجة غير مصرح بها أو التلاعب بالنتائج المالية غير المرغوب بها، إن البيانات الناتجة عن تطبيق حاسوبي قد تتحول إلى بيانات داخلة لتطبيق حاسوبي آخر. وفي هذه الحالة يجب أن يقوم المدقق بالبحث عن الضوابط المناسبة ليضمن نقل المخرجات بدقة من إحدى مراحل المعالجة إلى المرحلة التالية.

هـ - اختبار ضوابط التطبيق

ما أن يتم تحديد الضوابط، فإن الخطوة التالية في عملية التدقيق هي التحقق من فاعلية هذه الضوابط. ويمكن تحقيق ذلك من خلال:

- إدخال مجموعة من بيانات الاختبار، التي تؤدي إلى نتائج معروفة في حال عمل التطبيق بشكل جيد

- تطوير برامج مستقلة تكرر العمل بحسب المنطق الخاص بالتطبيق
- تقييم نتائج التطبيق

تقوم الإجراءات المذكورة أعلاه باختبار سلامة البرنامج المدمج في نظام معلومات إدارة الدَّيْن العام PDMIS، لكنها لا تختبر سلامة البيانات نفسها.

إذا كان ضمن التطبيق بيئة تجريبية، فيمكن استخدامها لاختبار الضوابط طالما أن البيئة التجريبية هي نسخة مؤكدة عن بيئة العمل الحي للتطبيق. لكي يختبر قواعد الحساب، مثل تلك المتعلقة بتحديث أصل الدين أو خدمة الدَّيْن، قد يحتاج المدقق إلى استخدام تقنيات التدقيق المحوسبة CAAT والتي تتضمن عدة أنواع من الأدوات والتقنيات مثل برمجيات التدقيق العام، والبرمجيات الخدمية، والبيانات التجريبية، ومتابعة وتخطيط البرامج التطبيقية، وتطبيقات التدقيق الاختصاصية. يمكن أن يتضمن ما سبق :أدوات لتحليل منطق جداول البيانات والحسابات من حيث صحتها .كما قد تستخدم الأدوات لتحليل تطبيقات قاعدة البيانات وإخراج جدول تدفق منطقي. ويمكن استخدام برمجيات التدقيق المعممة لتحليل البيانات الصادرة عن معظم التطبيقات.

إن هذه الوثيقة تقدم منظومة اختبار مقترحة في ملحق المعيار المشار إليه أنفا، والتي يمكن أن يستخدمها فريق التدقيق كمرجعية لاختبارات ضوابط التطبيق. تحدد هذه المنظومة بعض المتطلبات والوظائف التي يجب أن توفرها أنظمة الدَّيْن العام، والاستعلامات التي يجب أن تتمكن هذه الأنظمة من تنفيذها، بالإضافة إلى المتطلبات الدنيا للإمكانيات التي ينبغي أن تتمتع بها أمثال هذه الأنظمة. من المهم ملاحظة أنه بما أن ديون كل دولة يختلف تركيبها وخصائصها، فإن أنظمة الدَّيْن العام ستكون لها مواصفات مختلفة. وهكذا فإن مسؤولية فريق التدقيق هي أن يحدد ويستخدم البنود المتعلقة بأنظمة الديون في بلادهم ويعدلها عند اللزوم .

و- إعداد تقارير نتائج التدقيق

بالإضافة إلى الالتزام بإعلان ليما للمبادئ التوجيهية لقواعد التدقيق والمحاسبة، يجب أن تتوافق تقارير تدقيق أنظمة معلومات إدارة الدَّيْن العام مع المتطلبات المذكورة في المعيار الدولي للأجهزة العليا للرقابة والمحاسبة ISSAI 5440 المبادئ التوجيهية للقيام بتدقيق الدَّيْن العام – – استخدام الاختبارات الأساسية في التدقيقات المالية.

ز - إصدار تقارير نتائج التدقيق.

كما هو مذكور سابقاً، فإن هذا التدقيق هو تدقيق للأداء. لذا فمن المهم أن يتبع التقرير المعايير والتجربة العملية لمنظمة الإنتوساي (، المعيار ISSAI 300 المبادئ – الأساسية لتدقيق الأداء).

إصدار التقارير عن تدقيق الأداء، وذلك كما يحددها المعيار الدولي للأجهزة العليا للرقابة والمحاسبة ISSAI 3000 معايير ومبادئ توجيهية لتدقيق الأداء بناء على معايير التدقيق.