GUID 5259

أنظمة معلومات إدارة الدّين العام

إن الأدلة الإرشادية تصدر عن المنظمة الدولية للأجهزة العليا للرقابة(الإنتوساي) كجانب من إطار الإصدارات المهنية للإنتوساي.
(www.issai.org)لمزيد من المعلومات في الموقع

INTOSAI

INTOSAI

الإنتوساي, 2019

1) تمت المصادقة عليه ك GUID 5450 "التوجيهات الخاصة بتدقيق أنظمة معلومات إدارة الدين العام" في عام 2016

2) مع إنشاء إطار الإنتوساي للتصريحات المهنية (IFPP) ، تم إعادة تصنيفه وتسميته GUID 5259 " أنظمة معلومات إدارة الدّين العام" مع التغييرات التحريرية في عام 2019

الفهرس

تـــمـــهـيـــــــــــــد	**5**
قائمة الاختصارات	**7**
مقدمة	**8**
1. التخطيط	**10**
2. الضوابط العامة	**15**
الضوابط التنظيمية	16
ضوابط الوصول المادية	16
ضوابط الوصول المنطقية	16
ضوابط البيئة الحاسوبية	16
ضوابط تغيير البرامج	17
تخطيط استمرارية الأعمال والتعافي من الكوارث	17
3. ضوابط التطبيقات	**19**
1.3. معايير التوثيق	19
2.3. ضوابط الإدخال	21
شاشات إدخال البيانات	22
روتينات تحضير البيانات	22
الموافقة على إدخال البيانات	23
الاحتفاظ بمستندات الإدخال	23
التأكد من صحة إدخال البيانات	23
أخطاء إدخال البيانات	24
آليات دعم إدخال البيانات	25

3.3. ضوابط المعالجة 25

4.3. ضوابط المخرجات 27

5.3. اختبار ضوابط التطبيق 29

6.3. إعداد تقارير نتائج التدقيق 30

الملحق 1: جدول التخطيط 31

الملحق 2: منظومة اختبار الضوابط العامة 37

الملحق 3: مصفوفة اختبار ضوابط التطبيقات 44

الشكل 1: تدقيقات الدين العام التي تقوم بها الأجهزة العليا للرقابة والمحاسبة: حالة البرازيل 62

الشكل 2: تدقيقات الدين العام التي تقوم بها الأجهزة العليا للرقابة والمحاسبة: حالة مولدوفا 67

المصادر والمراجع 69

تـــمـــهيـــــــــــد

1) عندما نتحدث عن إدارة الموارد المالية العامة، فإن الدين العام هو الذي يتوسط المشهد. تواجه معظم الحكومات احتياجات مالية كبيرة في سعيها لتوسيع اقتصادها وتحسين الخدمات الاجتماعية فيبلدانها. نظرية، يعد الدين العام أداة فعالة للنمو الاقتصادي وتوزيع العبء الضريبي بإنصاف بين الأجيال الحالية والمستقبلية من دافعي الضرائب. يعد قياس الدين العام وإدارته بحر بالغ ضرورية بسبب أهميته بالنسبة للتوازن الاقتصادي.

2) إنّ الهدف الرئيس من إدارة الدّين هو توفير تمويل مستقر بأقل تكلفة ممكنة وبمستويات معقولة من المخاطر لأجل استمرار نشاطات الحكومة. تقدم "توجيهات صندوق النقد الدولي والبنك الدولي للإدارة الدّين العام" مجموعة من الممارسات الراسخة المرتبطة بالضوابط الداخلية لإدارة الدّين، ومنها الإقرار بأنه "يجب دعم نشاطات إدارة الدين بنظام إدارة معلومات دقيق وشامل ذي إجراءات حماية مناسبة. يجب على البلدان المعنية بالحصول على إدارة دين عام فعالة، أن تعطي أولوية عالية لتطوير الأنظمة الموثوقة لتسجيل وإصدار التقارير عن معلومات الدين. يعد هذا ضرورية ليس فقط من أجل تطوير بيانات الدين والتأكيد على دفعات خدمة الدين في الوقت الصحيح، ولكن أيضا من أجل تحسين جودة إصدار تقارير الميزانية وشفافية الحسابات المالية العامة، مما يسمح لصانعي القرار ومديري الدين العام بتحقيق الأهداف المتعلقة بالدين العام.

3) إن تدقيق نظام معلومات إدارة الدّين العام يسعى للمساهمة في زيادة كفاءة وفعالية وفاعلية إدارة الدين العام. ولهذا السبب يجب تصنيفه على أنه تدقيق للأداء إلا أن هذا العمل يمكن أن يكون ذا صلة وثيقة بسياق عمليات التدقيق المالي، التي تركز على تحديد ما إذا كانت المعلومات المالية للحكومة قد تم تقديمها بما يتوافق مع الإطار التنظيمي المطبق على عرض التقارير المالية

وفيما إذا كانت المعلومات موثوقة وخالية من التزوير والأخطاء في هذا السياق، يصبح هذا العمل ذا أهمية كبيرة لأنه يساهم في الحصول على نظام معلومات يجمع ويصدر معلومات دقيقة وموثوقة عن أحد أهم العناصر المالية للحكومة وهو الدين العام.

4) يهدف هذا الدليل إلى تزويد المدققين بتوجيهات موصفة عن تدقيق أنظمة معلومات إدارة الدين العام. ونظرا لأن المنظمة الدولية للأجهزة العليا للرقابة والمحاسبة – الإنتوساي (INTOSAI) سبق وكان لديها بعض الوثائق المتعلقة بتدقيق تقنية المعلومات، والتي طورتها مجموعة العمل على تدقيق تقنية المعلومات (WGITA) ، فإن التركيز في هذا الدليل ينصب على ضوابط التطبيق، والتي يجب أن تكون مخصصة لنظام معلومات إدارة الدّين العام.

قائمة الاختصارات

BCP تخطيط استمرارية الأعمال

CAAT تقنيات تدقيق بمساعدة الحاسوب

CS-DRMS نظام تسجيل وإدارة الدّين الخاص بأمانة الكومونويلث

DMFAS نظام إدارة الدّين والتحليل المالي

DMO مكتب إدارة الدّين

DRP خطة التعافي من الكوارث

FMIS نظام معلومات الإدارة المالية

IMF صندوق النقد الدولي

INTOSAI المنظمة الدولية للأجهزة العليا للرقابة والمحاسبة – الانتوساي

IT تقنية المعلومات

MF وزارة المالية

PDMIS نظام معلومات إدارة الدّين العام

SAI الجهاز الأعلى للرقابة والمحاسبة

SAIS الأجهزة العليا للرقابة والمحاسبة

UNCTAD مؤتمر الأمم المتحدة للتجارة والتطوير

WGITA مجموعة العمل على تحقيق تقنية المعلومات

WGPD مجموعة العمل على الدّين العام

مقدمة

وفقا لوثيقة الاختصاصات التي وضعها مجلس إدارة منظمة الإنتوساي (INTOSAI)، فقد أسندت إلى مجموعة العمل على الدين العام (WPGD) مهمة نشر التوجيهات وسواها من مواد المعلومات الأخرى التي ستستخدمها الأجهزة العليا للرقابة والمحاسبة SAIs للتشجيع على رفع التقارير عن الدين العام بصورة مناسبة وعلى الإدارة السليمة للدين العام.

يهدف هذا الدليل إلى رفع قدرة مجموعة العمل على الدين العام WGPD من خلال تزويدها بإطار عمل عام يمكن استخدامه في تدقيقات الأجهزة العليا للرقابة والمحاسبة SAIs لتقييم الضوابط العامة وضوابط التطبيق لنظام معلومات إدارة الدين العام. من المهم أن نذكر في المراجع أن نظام معلومات إدارة الدّين العام يشمل واحدة أو أكثر من أنظمة المعلومات المستخدمة في إدارة الدّين العام.

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. حسب ورقة عمل لصندوق النقد الدولي "عادة ما يشير نظام معلومات الإدارة المالية إلى حوسبة عملية إدارة الإنفاق العامة متضمنة صياغة الميزانية وتنفيذها وحساباتها بمساعدة نظام مدمج بشكل كامل للإدارة المالية للوزارات المعنية والمؤسسات الأخرى التي تقوم بالإنفاق."

يعرف معهد المهندسين الكهربائيين والإلكترونيين في معيار (IEEE 1471) الأنظمة على أنها "مجموعة من المكونات التي تم تنظيمها لتنفيذ وظيفة أو مجموعة من الوظائف المحددة." وعلى وجه الخصوص، فإن النشاط الرئيسي للنظام الحاسوبي في مكتب الدين هو المحافظة على قاعدة بيانات قروض القطاع العام باستخدام برامج حاسوب مناسبة لأمرين: تسجيل الوظائف التحليلية للمكتب إدارة الدين وكذلك لتولي

أمر إدارة هذه الوظائف.

يمكن تصنيف تدقيق تقنية المعلومات فيما يتعلق بالتوجهات السائدة كالتالي:

- إدارة تقنية المعلومات.
- تدقيق البيانات.
- تدقيق نظام المعلومات.
- عقود تقنية المعلومات.
- أمن المعلومات.

بشكل عام، يعمل مدقق تقنية المعلومات بأكثر من توجه واحد، إلا أن المدقق يستطيع أن يختار التوجه الذي سيكون سائدة. وفي هذا الدليل فإن التوجه السائد هو تدقيق نظام المعلومات.

يتكون هذا الدليل من تخطيط وتقييم الضوابط العامة وتقييم ضوابط التطبيق.

1. التخطيط

يمكن اعتبار نظام معلومات إدارة الدين العام على أنه مجموعة من الأجزاء المترابطة (بنى مادية، موظفون، وأدوات تقنية) التي تتفاعل مع بعضها البعض من أجل تسجيل وضبط وتقييم وإدارة المعاملات الحاصلة لأجل جمع الدين العام والمحافظة عليه وتصفيته.

تساعد هذه المرحلة المدقق على فهم العمليات المرتبطة بالنظام وأدوات ضبطه والمخاطر المتعلقة بالنظر إلى المخاطر المتأصلة في تدفق عملية الدين العام. وبالاعتماد على هذا الفهم، يقوم المدقق بتقييم بيئة الضبط الكلية، ويحدد الأنظمة المستخدمة في إدارة الدين 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 فحص لجميع البنى المتعلقة بمكتب الدين العام، مثل الموظفين، والعمليات، ونوع الديون، وأمن المعلومات، والأدوات التقنية، والأمور الأخرى.

يجب على المدقق في هذه المرحلة أن يضع تقييما أوليا لبنية مكتب الدّين العام وتدفقات عملية الدّين العام وعليه أن يغطي النقاط التالية:

- كيف يتم تنظيم نظام معلومات إدارة الدين العام: ما هي الأنظمة المستخدمة للتسجيل والمعالجة ورفع التقارير والضبط وإدارة الدين العام، وما هي العمليات والوظائف الأساسية التي يؤديها كل نظام.
- فعالية التدقيق الداخلي.
- نتائج عمليات التدقيق السابقة (الداخلية أو الخارجية المجراة على نظام معلومات إدارة الدّين العام).
- التخزين المادي لوثائق العمليات.
- استخدام برمجيات وعتاد الحاسوب ومسؤولية صيانتها والحفاظ عليها .
- العمليات التي تتم معالجتها من قبل أنظمة المعلومات وأهميتها.

- كيف يتم الربط بين مكونات معلومات الدّين العام.
- الطرق والإجراءات التي تم وضعها لتنفيذ العمليات الجديدة أو المراجعة العمليات الموجودة سابقا.
- التقييمات الماضية لعمليات الضبط الداخلية لمكتب إدارة الدين. إذا لم يتم إجراء أي تقييم سابق لعمليات الضبط الداخلية لمكتب إدارة الدين، فيجب أن يقوم الجهاز الأعلى للرقابة والمحاسبة بهذا التقييم. إن هذا الإجراء مهم جدا لتقييم درجة المخاطر الموجودة وتحديد اختبارات التدقيق التي يجب تنفيذها نتيجة لذلك.

لا تؤثر درجة تعقيد النظام على تقييم عمليات الضبط العامة والتي يجب إجراؤها دائما، إلا أنها ستحدد إجراءات التدقيق التي ستنفذ وكذلك عدد اختصاصي المعلوماتية اللازم للقيام بالتدقيق. من المقترح أن يكون هناك اختصاصي معلوماتية واحد على الأقل بين أعضاء الفريق للقيام بكل الأعمال المتعلقة بأنظمة المعلومات. أما بالنسبة للمدققين الموجودين في الفريق الذين هم حديثو عهد بالتدقيق المعلوماتي، فمن المهم أن يكتسبوا دراية بالمصطلحات المستخدمة عادة في هذه الحالة يكون من مصلحة الجهاز الأعلى للرقابة والمحاسبة الحصول على قاموس جيد عن تقنية المعلوماتية وكذلك ستكون مفيدة جدا لهذا الغرض وثيقة "تدقيق أنظمة المعلومات - قائمة المصطلحات" الصادرة عن المجموعة العاملة على التدقيق المعلوماتي في منظمة الإنتوساي(INTOSAI). ويمكن أن تكون بعض قوائم المصطلحات الموجودة على الإنترنت مفيدة جدا مثل:

http://www.webopedia.com أو http://whatis.techtarget.com

يجب على المدققين المطلعين على التعابير الخاصة بالمعلوماتية أن يكونوا ملمين بالمصطلحات المستخدمة في مكتب إدارة الدّين وخاصة الاختصارات (أنواع الترويسات، وقطاعات مكاتب إدارة الدّين، والدائنون، وأسماء الأنظمة، والبرمجيات التي يستخدمها مكتب إدارة الدين.. الخ). من الضروري الاطلاع على هذه المعلومات قبل إجراء المقابلات.

تم تطوير قائمة مصطلحات مفيدة جدا من قبل مؤتمر الأمم المتحدة للتجارة والتنمية UNCTAD، ويمكن الاطلاع عليه في المواقع التالية:

- قائمة المصطلحات الدين ونظام إدارة الدين ونظام التحليل المالي (النسخة الانجليزية): http://unctad.org/en/Docs/pogiddmfasm3r3.en.pdf
- قائمة مصطلحات الدين ونظام إدارة الدين ونظام التحليل المالي (النسخة الإسبانية): http://www/unctad.org/sp/docs//pogiddmfasm3r3.en.pdf

إن فهم تفاصيل أي نظام معلومات لإدارة الدين العام يعني معرفة التدفقات المتأصلة للبيانات والمعلومات. ولذلك من المهم جدا في مرحلة التخطيط أن ترسم خريطة للعمليات الرئيسة للدين العام (التسجيل، والمعالجة، والضبط، والأمن، ورفع التقارير والتحليل) فهم كيفية تنفيذ هذه العمليات عبر نظام المعلومات. وبعد ذلك، من الضروري إجراء تقييم المخاطر لتحديد أهم المخاطر المرتبطة بعمليات التشغيل والإدارة الرئيسة للدين العام بالنظر إلى تأثيرها واحتمالية حصولها. يعد تقييم المخاطر ضروري لتحديد مجال الإجراءات الضرورية لإدارة مستويات المخاطر المرتبطة. يقدم المعيار الدولي للأجهزة العليا للرقابة والمحاسبة ISSA:5410 لتوجيهات اللازمة لتخطيط وتنفيذ تدقيق عمليات الضبط الداخلية للدين العام توجيهات لإجراء دراسة تقييم المخاطر. بالإضافة إلى ذلك، يمكن تحديد تقييم المخاطر في سياق عمليات التدقيق المالي.

غالبا ما تتم تسوية تدفقات نظام معلومات إدارة الدين العام في مكتب إدارة الدين. يمكن أن تكون المكاتب الأخرى مسؤولة عن إدخال بيانات الدين كحالة الدين التعاقدي على سبيل المثال. وحينما ينقسم مكتب إدارة الدين إلى مكاتب خلفية ووسطى وأمامية، فعندئذ يكون لكل مكتب بياناته وتدفقات المعلومات الخاصة به. عادة ما يكون المكتب الأمامي مسؤولا عن تنفيذ المعاملات في الأسواق المالية، ويشمل ذلك إدارة المزادات وأشكال الاقتراض الأخرى، وكذلك جميع عمليات التمويل الأخرى. أما المكاتب الخلفية فتتعامل مع تسوية المعاملات والمحافظة على السجلات المالية. عادة ما يقوم مكتب منفصل يسمى بالمكتب الأوسط أو مكتب إدارة المخاطر بتحليل المخاطر ومراقبة ورفع التقارير عن المخاطر المتعلقة بالسندات، وكذلك تقييم أداء مديري الدين للمقارنة مع أية أهداف/معايير استراتيجية. يتم التعامل مع معظم تدفقات البيانات المتعلقة بالدّين العام، بما في ذلك البيانات الخارجية، في المكتب الخلفي المسؤول عن إدخال البيانات وتسجيلها وضبطها.

وباعتبار أن كثيرا من البلدان تستخدم لإدارة الدين العام نظاما جاهز, تطوره وتحدثه منظمات دولية تعمل كطرف ثالث (مثل نظام إدارة الدين والتحليل المالي DMFAS، ونظام تسجيل وإدارة الدّين الخاص

بأمانة الكومونويلث (CS-DRMS))، فإن من المهم جدا استخدام التقارير المتعلقة بالأداء مثل التطورات الحاصلة وطلبات صيانة النظام وتسجيل الأحداث.

يركز برنامج نظام إدارة الدين والتحليل المالي DMFAS المطور من قبل مؤتمر الأمم المتحدة للتجارة والتطوير UNCTAD على النشاطات التي تعتبر "مع التيار". تتضمن هذه النشاطات المحافظة على قاعدة بيانات الدين، وتوثيق صلاحية بيانات الدين، وعمليات الدين، ورفع تقارير الدين الداخلي والخارجي، وإحصاءات الدين والتحليل الأساسي للدين وإقامة روابط معلوماتية بين إدارة الدين والبرمجيات المالية الأخرى. تتكامل هذه النشاطات مع مزيد من نشاطات "ضد التيار" مثل تحليل القدرة على تحمل الديون الذي تقدمه جهات أخرى مثل البنك الدولي. إضافة إلى ذلك، يساعد البرنامج البلدان بشكل متزايد على إنشاء روابط بين نظام برنامج نظام إدارة الدين والتحليل المالي (DMFAS)المطور لإدارة الدين والبرمجيات الحكومية الأخرى (مثل البرمجيات المستخدمة للميزانية، والإدارة النقدية، وإدارة المساعدات) أو ضمن أنظمة مدمجة معقدة للإدارة المالية كجزء من جهود البلدان في الإدارة المالية العامة. لمزيد من المعلومات يرجى زيارة الموقع: http://unctad.org/dmfa

إن التطبيق المقدم من قبل أمانة الكومونويلث يساعد الحكومات على تسجيل وإدارة وتحليل ديونها من وجهة نظر شاملة. حيث يوفر مستودعا مركزية لعدة أصناف من الديون المحلية والخارجية والعامة والمضمونة من القطاع الخاص، ويشمل ذلك الديون قصيرة المدى. يتعامل النظام أيضا مع المنح والإقراض الحكومي والاقتراض من أجل الإقراض

لمزيد من المعلومات يرجى زيارة الموقع

https://thecommonwealth.org/about-cs-drms

في حالة البلدان التي تستخدم لإدارة الدين العام أحد برامج نظام إدارة الدين والتحليل المالي DMFAS أو نظام تسجيل وإدارة الدين الخاص بأمانة الكومونويلث CS-DRMS، فيمكنها أن تستفيد من تقارير تدقيق نظام معلومات إدارة الدّين العام PDMIS التي نفذتها الأجهزة العليا للرقابة والمحاسبة في بلدان أخرى وذلك لتحديد مواطن الخلل الأكثر تكرار و/أو التي لها تأثير أكبر.

يوجد في الملحق[1] جدول عن المعلومات والإجراءات المطلوبة والأسئلة التي يجب أن يجيب عليها الجهاز الأعلى للرقابة والمحاسبة والتي يمكن استخدامها من قبل فريق التدقيق خلال مرحلة التخطيط لأعمال تدقيق أنظمة الدين العام.

1 هذا الإصدار تم استخراجه من الإطار في سبتمبر 2019

2. الضوابط العامة

توفر الضوابط العامة إطار العمل لمجمل الضوابط من أجل وظائف تقنية المعلومات. صممت هذه الضوابط للتعامل مع مشاكل التطوير والعمليات والمحافظة على البيئة المعلوماتية. تهدف الضوابط العامة إلى حماية البيانات وبرامج التطبيقات وضمان استمرار عمليات الحاسوب في حال حدوث عوائق غير متوقعة.

على الرغم من أن تدقيق نظام الدين 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 التقنية المعلومات بالتفصيل.

من المقترح أن يلجأ فريق العمل في حالة القيام بتدقيق للنظام إلى معيار ISSAI[2] 5310 توجيهات بشأن تدقيق أمن أنظمة المعلومات (ISec)، وهو دليل بخصوص مراجعة أمن أنظمة المعلومات (ISS) في المؤسسات الحكومية.

توجد أيضا 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 2 مصفوفة اختبار تتضمن بعض الضوابط العامة والاقتراحات لعدد من الاختبارات التي يمكن أن تساعد المدقق على القيام باختبار الضوابط العامة.

إن أي مجموعة شاملة من مختلف تصنيفات الضوابط العامة ينبغي أن تتضمن المواد الموصوفة أدناه:

2 هذا الإصدار تم استخراجه من الإطار في سبتمبر 2019. الإصدار الجديد GUID 5110 حول التدقيق أمن أنظمة المعلومات يمكن أن يكون مرجع.

« الضوابط التنظيمية

الضوابط التنظيمية تعني السياسات والإجراءات وإطار العمل التنظيمي التي تم تقريرها لضمان الحصول على ممارسات إدارية وسياسات موارد بشرية دقيقة، والفصل بين الواجبات، وسياسات أمن المعلومات، لتوفير طرق لتقييم الفاعلية ولضمان ضوابط العمل وكفاءتها.

« ضوابط الوصول المادية

تتضمن هذه الضوابط قواعد وممارسات لمنع الوصول غير المصرح به إلى خدمات تقنية المعلومات والتلاعب بها. ويشمل ذلك الإجراءات الإدارية مثل بطاقات الهوية للموظفين، والتحكم بحركة الزوار، وإجراءات مادية مثل الأقفال الميكانيكية والأقفال الإلكترونية للأبواب، وكاميرات المراقبة ووسائل أخرى تحد من الوصول إلى أجهزة الخوادم وإلى مواقع حساسة أخرى من البنية التحتية.

« ضوابط الوصول المنطقية

تستخدم هذه الضوابط الأدوات الأمنية المدمجة في أنظمة الحاسوب لمنع أي وصول غير مصرح به إلى الملفات والبيانات الحساسة ولضمان أن جميع المستخدمين يملكون حقوق وصول تقيدها المتطلبات الموجودة في مسمياتهم الوظيفية. تتضـــــــــمن هذه الأدوات الأمنية: جدران الحماية (Firewall) ومضادات الفيروسات، والكشف عن البرامج الخبيثة وبرامج التطفل.

يتم الحصول على هذه الضوابط في الأنظمة الحديثة بطرق متعددة، حيث يتم تفعيلها من خلال برمجيات التطبيقات، ونظام التشغيل، ونظام إدارة قواعد البيانات، وبرمجيات ضبط الوصول، وأدوات مراقبة معالجة المعاملات المباشرة (OLTP)، والخوادم، والشبكة، والشبكة المحلية، وربما برمجيات أخرى.

« ضوابط البيئة الحاسوبية

هذه الضوابط هي القوانين والممارسات والشروط المبنية لمنع حصول أي ضرر قد تسببه التقلبات الكهربائية، أو الحريق، أو الغبار، أو الماء، أو الطعام، أو درجات الحرارة الحادة، أو الرطوبة، أو الكهرباء الساكنة.

على الرغم من أن هذه الضوابط تركز على مركز البيانات (أو المنطقة المخصصة لأجهزة تقنية المعلومات، والتي تحتاج إلى محيط خاص أو على الأقل إلى الحماية من السرقة)، إلا أن هذه الضوابط تنطبق أيضا على كل البيئة المكتبية.

» ضوابط تغيير البرامج

تتضمن هذه الضوابط قواعد تضمن أن يكون التعامل مع كل التغييرات الحاصلة في إعدادات الأنظمة بشكل صحيح، وكامل، وفي الوقت المناسب.

يجب أن يوجد خطوات رسمية لإجراء التحديثات والتغييرات، وذلك لضمان تسجيل جميع التغييرات ولتوفير إمكانية التراجع في حال وجود مشاكل في الإصدار الجديد.

يجب أن يكون الحصول على موافقة رسمية مطلوبة قبل الانتقال بالبرامج من مرحلة الاختبار إلى مرحلة مكتبات الإنتاج، ويجب أن تكون جميع الأنظمة والعمليات ووثائق البرامج كاملة ومحدثة ومتوافقة مع المعايير والسياسات والإجراءات المعتمدة.

» تخطيط استمرارية الأعمال والتعافي من الكوارث

يتم تصميم خطط استمرارية الأعمال (BCP) وما يتعلق بها من خطة التعافي من الكوارث (DRP) لأجل تلبية الحاجة إلى استمرار توافر النظام. يعتبر كل من التخطيط للطوارئ والتعافي من الكوارث، وصلاحية الخطط، واختبارها، ومراقبتها، والحاجة إلى التحديث المستمر للخطط، تعتبر جميعها عوامل هامة[3].

إن تخطيط استمرارية الأعمال (BCP) هو توجه شامل يقدم طرق بديلة تدعم إجراءات العمليات الهامة في حال حدوث أي طارئ أو كارثة أو أي اختلال آخر. ينبغي أن يكون التركيز على إنقاذ العمل بشكل كامل وليس فقط حماية تقنية المعلومات. إلا أن مجمل الخطة يجب أن يأخذ في الحسبان متطلبات شبكات الاتصالات السلكية واللاسلكية وأنظمة المعلومات. إن هذا الجزء من تخطيط استمرارية الأعمال (BCP) هو ما يعرف بخطة التعافي من الكوارث (DRP).

3 Information Technology Audits, Xenia ley Parker

يمكن تطوير خطط استمرارية الأعمال (BCP) وخطط التعافي من الكوارث (DRP) المرتبطة بها التخطيط في الوقت نفسه لكي تؤخذ جميع العوامل بعين الاعتبار معا في الوقت نفسه. وعلى أقل تقدير يجب أن تتضمن الخطة الإجراءات والمعايير اللازمة لتحديد ما إذا كان الوضع يعتبر كارثة، وتحديد الشخص المسؤول عن اتخاذ ذلك القرار، وكيفية الإعلان عن الكارثة بشكل رسمي وكيفية وضع الخطة قيد التنفيذ.

3. ضوابط التطبيقات

يتم جعل ضوابط التطبيقات آلية في تطبيقات أنظمة المعلومات لتساعد على ضمان صحة 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 جميعا مسجلة وكاملة وصحيحة.

يمكن تصنيف ضوابط التطبيقات كالتالي:

- إدخال
- معالجة
- إخراج

1.3. معايير التوثيق

تضمن معايير التوثيق أن يتم الحفاظ على توثيق مناسب ومحث للتطبيقات، كما أن القيام بالتحديث المتقن للتوثيق مهم أيضا[4].

4 Information Technology Audit - General Principles (IT Audit Monograph Series #1) - India Office of the Comptroller and Auditor General.

يعد التوثيق المناسب مهمة 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 كيفية عمل كل تطبيق، وقد يساعده ذلك على ملاحظة وجود مخاطر معينة.

- 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 إنشاؤه 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 مع 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.
- وثائق المستخدمين: يجب أن تتضمن وصفا لكل من سير العمل الآلي واليدوي لتساعد في التدريب الأولي على التطبيق ولتكون مرجعا دائما لهم. في كلتا الحالتين، يجب أن يتم تحديث وثائق المستخدمين كلما عدل التطبيق.

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.

2.3. ضوابط الإدخال

تعد ضوابط الإدخال هامة جدا للتقليل من مخاطر الخطأ أو التزوير في التطبيقات المحوسبة. إن ضوابط الإدخال حياتية بالنسبة لسلامة البيانات.

تساعد ضوابط الإدخال على التأكد من صحة إقرار البيانات المدخلة في التطبيق، ودقتها وكمالها وتوقيتها. يتم التأكد من صحة إقرار البيانات عن طريق طلب موافقات إضافية للعمليات التي تتجاوز حد معين. 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.

قد يتم تخطي الضوابط المذكورة أعلاه في حال إمكانية تجاوزها عن طريق إدخال بيانات أو تعديلها من خارج التطبيق. يجب أن يكون هناك إجراءات آلية للتحقق من سلامة التطبيق لكشف أي تغييرات تطرأ من الخارج على البيانات والإبلاغ عنها. على سبيل المثال، يجب أن يوجد إجراء تحقق لكشف أي تغييرات غير مصرح بها ضمن قاعدة بيانات العمليات وللإبلاغ عن هذه التغييرات.

شاشات إدخال البيانات

يمكن لشاشات إدخال البيانات المعيارية أن تضمن إدخال البيانات بشكل متسق.

يمكن لنظام معلومات إدارة الدين العام PDMIS أن يتضمن الوظائف التالية:

- شاشات الإدخال مرتبة بطريقة معيارية ومنسقة.
- تستطيع حقول إدخال البيانات تحديد ما هو مسموح للمستخدمين بإدخاله.
- الإدخال الإجباري لبعض الحقول المعينة.
- وظيفة للمساعدة (مثل زر F1) لمساعدة المستخدمين على تعبئة حقول بيانات الإدخال.

روتينات تحضير البيانات

إن هدف روتينات تحضير البيانات هو تجنب حصول الإخفاقات أثناء عمليات إدخال البيانات.

يمكن أن يتضمن نظام معلومات إدارة الدين العامPDMIS: بيئات مدمجة لإجراءات مشاركة البيانات من أجل نقلها مع تطبيقات أخرى.

» الموافقة على إدخال البيانات

تهدف الموافقة على إدخال البيانات إلى ضمان أن كل عمليات إدخال البيانات قد تم تسجيلها والموافقة عليها من قبل الشخص المناسب.

يمكن أن يتضمن نظام معلومات إدارة الدين العام PDIMS الوظائف التالية:

- » تطلب نظام معلومات إدارة الدين العام PDMIS كلمة مرور للدخول.
- » تدوين سجل الولوج عند إدخال البيانات بشكل يدوي.
- » يستلزم طلب موافقتين لأجل بعض العمليات الحساسة (مثل تفعيل العقود، وتعديل سعر الفائدة، وتعديل قيم العقود).

» الاحتفاظ بمستندات الإدخال

يشير هذا البعد من ضوابط إدخال البيانات إلى الاحتفاظ بالمستندات الأصلية التي تدعم سجلات بيانات الدين وضبط هذه المستندات. في حالة النقل الآلي للملفات بين التطبيقات، يجب أن يحتفظ نظام معلومات إدارة الدين العام PDMIS بالبيانات الأصلية المستلمة من التطبيقات الأخرى وذلك المدة يحددها مكتب إدارة الدين DMOمسبقا.

» التأكد من صحة إدخال البيانات

تصمم ضوابط التأكد من صحة إدخال البيانات للتأكد من أن البيانات المدخلة صالحة ودقيقة.

يمكن أن يتضمن نظام معلومات إدارة الدين العام PDMIS الوظائف التالية:

- » قوائم تحقق تلقائية للتأكد من غياب القيم (مثلا عندما يتم تنزيل سلسلة مخزنة من الملاحق، يقوم نظام معلومات إدارة الدين العام PDMIS بالتحقق من غياب قيمة يومية أو شهرية أو سنوية).

- يتم تحديد الحقول الإجبارية بوضوح في جميع شاشات إدخال البيانات، ويسمح التطبيق بتأكيد العملية فقط في حال إدخال كافة المعلومات المطلوبة في الحقول الإجبارية.
- يجب أن يحتوي كل جدول في قاعدة البيانات على قاعدة محددة حيث لا يمكن تكرار البيانات نفسها.
- إذا اعتبر التطبيق أن إدخال البيانات يتم بشكل مكرر، فلن يوافق على عملية الإدخال حتى يتم معالجة موضوع هذا التكرار.
- لن يسمح التطبيق بتعديل بعض البيانات بعد إدخالها (كسعر الصرف في يوم العملية). أما بالنسبة للبيانات الأخرى، فيمكن أن يسمح التطبيق بالتعديل في حال توفر بعض الشروط (مثلا لا يجوز تعديل أي بيانات عند "إغلاق" العقد أو عند الإشارة إليه با "إقفال").
- تتطلب بعض الحقول عند تعبئتها أن يتم تعبئة حقول أخرى (مثلا عندما يدخل المستخدم رسوم الالتزام الخاصة بالعقد، يجب على المستخدم أن يدخل أيضا الضريبة المتعلقة بهذا الالتزام).
- حقول "التاريخ" ضرورية للتمكن من ضبط عقود الدين بصورة شاملة. وهذه الحقول مفيدة خصوصا في حساب الأقساط، ولتجنب التأخير في الدفعات، ولفرض الغرامات... الخ. ولذلك فيجب أن يكون للتطبيق قوانين أساسية للإلزام بإدراج تفاصيل "التاريخ".
- باستثناء العمليات التي يتم إدخالها بغرض المحاكاة، لا يسمح التطبيق بتسجيل بعض البيانات بتاريخ مستقبلي يتعلق بالعمليات الفعالة فقط. مصرف الأموال، والتراجع عن الصرف، وإلغاء العقود، والإضافة إلى العقود.

أخطاء إدخال البيانات

إن "سجل تعقب التدقيق" أو "سجل التدقيق" هو سجل مرتب زمنيا يتعلق بالأمن، أو هو مجموعة من السجلات، أو هو عبارة عن سجلين أحدهما لوجهة والآخر لمصدر السجلات، والتي توفر دليلا توثيقيا لسلسلة النشاطات التي أثرت في أي وقت على عملية محددة أو إجراء أو حدث يجب أن يكون الوصول

إلى سجل تعقب التدقيق أو ملفات سجلات الملفات محصورة بمجموعة الموظفين المسؤولة عن ذلك.

يمكن أن يتضمن نظام معلومات إدارة الدين العام PDMIS الوظائف التالية:

- يجب أن يحدد مكتب إدارة الدّين DMO المسؤولية تجاه الملفات المعلقة.
- يجب أن تدمج ضمن التطبيق: برامج تسجل الأخطاء، وترفع التقارير عن الأخطاء القائمة، وتسجل تصحيح الأخطاء.
- أثناء التنزيل الآلي للبيانات، وعندما يكتشف التطبيق ثغرات في السلاسل، فإنه يرسل بريد الكترونية بصورة تلقائية.
- يجب أن يرسل التطبيق تقارير دورية بالأخطاء التي لم يتم حلها - بما في ذلك كم من الوقت ظلت الأخطاء دون حل وأولويتها - للموظفين الناسبين.

آليات دعم إدخال البيانات

ترتبط هذه الضوابط بإجراءات الدعم في مكتب إدارة الدين DMO الذي يساعد المستخدمين على إدخال البيانات في التطبيق الحاسوبي، وعلى إعادة تشغيل التطبيقات، ومراقبة نشاطات المستخدمين لتجنب أي تجاوز للقوانين الموضوعة.

غالبا ما تكون هذه الآليات متضمنة في الضوابط العامة.

3.3. 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[5].

5 Information Technology Control and Audit - Second Edition, Frederick Gallegos.

» الشمولية

يمكن ضمان الشمولية أثناء معالجة مجموعة البيانات من خلال موازنة العمليات التي استقبلها النظام مع العمليات التي أرسلها النظام الفرعي.

يجب أن تتم الموازنة بين التطبيقات التي تتشارك في البيانات من خلال إعداد تقرير ملاءمة يعدد البيانات في كلا التطبيقين ويرفع تقريرا عن أي اختلافات إلى مجموعة معينة من المستخدمين[6].

يجب أن تتضمن موازنة المجاميع عدد المعاملات و المجاميع 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[7] تجمع كل الأرقام الموجودة في عمود للتأكد من أن الحصيلة نفسها سيتم قبولها في عملية المعالجة التالية. مثلا، إن حساب مجموع أرقام اتفاقية الدين لا يعني شيئا، لكن يمكن استخدام هذا المجموع للتأكد من أن جميع الأرقام الصحيحة لاتفاقية النقد تم تضمينها في عملية المعالجة[8].

يمكن أن يتضمن نظام معلومات إدارة الدين العام PDMIS الوظائف التالية:

- في حال حدوث خطأ في معالجة الملفات عند الربط مع أنظمة أخرى بين التطبيقات، يتم توليد ملف عن الأخطاء وتسجيله في تطبيق النظام. بالإضافة إلى تطوير منهجية للعمل التشاركي في الجانب التقني والتدريب عبر أقسام الشركة.
- يتضمن التطبيق مجموعة من الأعمال المجدولة لمهام عديدة. مثل تحديث أصل الدين والتخطيط المالي والجداول و الملاحق والدفعات المستقبلية...الخ. يجب تقييم مخرجات المنظومات الفورية المرنة بالتركيز على سجلات العمليات المعتمدة على المجموعات بالإضافة إلى إمكانيات التطبيقات الفورية القياسية لقياس معالجة المعلومات.

6 Information Technology Control and Audit - Second Edition, Frederick Gallegos.

7 Information Technology Control and Audit - Second Edition, Frederick Gallegos.

8 Information Technology Control and Audit - Second Edition, Frederick Gallegos.

- في حال حدوث خطأ في معالجة عمليات المجموعات، يرسل التطبيق رسالة للمستخدم تتضمن معلومات عن الخطأ الحاصل ويجب التأكد من إمكانيات التجميع داخل النظام لتنفيذ سياسات تصحيح الأخطاء وإجراءات التحكم بالأرقام.
- بعد إنهاء عملية ما، يعرض التطبيق رسالة تؤكد أن المعالجة تمت بنجاح وتعرض ملخص عن البيانات المدخلة.
- بعد تعديل بيانات مسجلة سابقا، يعرض التطبيق رسالة عن نجاح التعديل كما يعرض ملخصا عن البيانات المعدلة.
- بعد حذف بيانات مدخلة سابقا، يعرض التطبيق رسالة عن نجاح الحذف كما يعرض ملخص عن البيانات المحذوفة.
- إذا أثر مسح أحد السجلات على سلامة قاعدة البيانات، لا يسمح التطبيق بالحذف ويعرض رسالة تقول بأنه لا يمكن حذف السجل. كما في حالة بيانات البنك الدائن التي لا يمكن حذفها من جدول الدائنين إذا كان هناك في التطبيق عقود قيد التنفيذ لهذا الدائن.
- يقوم التطبيق ببعض التحقيقات بين بيانات المكتب الأمامي والخلفي. على سبيل المثال، عندما يطلب من المكتب الخلفي التحقق من صحة البيانات المدخلة من المزادات. يجب التأكد من الاتصالات بخصوص العلاقات البينية للبيانات، وذلك بين المكونات والأنظمة، للتحقق من تدفق البيانات حسب مخطط إمكانية التشغيل البينية.

4.3. ضوابط المخرجات

إن ضوابط المخرجات تضمن سلامة المخرجات والتوزيع الصحيح وفي الوقت المناسب للمخرجات الناتجة[9]. قد يتم تعويض ضعف المعالجة أحيانا بوضع ضوابط صارمة على المخرجات. إن أي تطبيق للإدخال والمعالجة، مع كونه مضبوطا بصورة حسنة، قد يتقوض تماما إذا لم تكن المخرجات مضبوطة[10].

9 Information Technology Control Audit - Second Edition, Frederick Gallegos.

10 IT Audit Guidelines, ASOSAI

تعتمد شمولية وسلامة تقارير المخرجات على تقييد إمكانية تعديل المخرجات وعلى تضمين عمليات لفحص الاكتمال مثل أرقام الصفحات وحصيلة التدقيقات[11].

يجب أن يتم حماية ملفات المخرجات لتقليل خطر إمكانية حصول التعديلات غير المصرح بها. تتضمن دوافع تعديل المخرجات الحاسوبية التغطية على أي معالجة غير مصرح بها أو التلاعب بالنتائج المالية غير المرغوب بها[12].

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[13].

في نظام معلومات إدارة الدين العام PDMIS، يمكن برمجة ضوابط المخرجات لتحديد المعلومات الحساسة التي تحتاج إلى أن تحتل الأولوية في العمل من قبل إدارة الدين العام. على سبيل المثال: في حالة العقود التي سوف تنتهي في الشهر الحالي، يمكن أن يعرض التطبيق تنبيهات يومية على الشاشة الأولى للنظام، بخصوص العقود التي تستوجب الدفع في الأيام الخمسة المقبلة.

يمكن أن يسمح التطبيق أيضا لبعض المستخدمين المعينين بتوليد التقارير بحسب الأولوية، مما يسمح للتطبيق بترتيب التقارير التي سوف يولدها وفق أولوية معينة.

يمكن أن يتضمن نظام معلومات إدارة الدين العام PDMIS الوظائف التالية:

- المقارنة الآلية لحاصل البيانات الأصلية مع حاصل البيانات المعالجة.
- يجب أن يخبر التطبيق مستخدميه بوضع طلبات توليد التقرير، مثل: "لم يبدأ" "قيد التنفيذ" "وانتهى".

11 Information Technology Audit - General Principles (IT Audit Monograph Series # 1) – India Office of the Comptroller and Auditor General.

12 Information Technology Audit - General Principles (IT Audit Monograph Series # 1) – India Office of the Comptroller and Auditor General.

13 هذا الإصدار تم استخراجه من الإطار في سبتمبر 9102. الإصدار الجديد حول التدقيق في الدين العام يمكن أن يكون مرجع

- في نهاية عملية توليد أي تقرير، يرسل التطبيق رسالة للمستخدم الذي أنشأ الطلب ليخبره بانتهاء المهمة.

5.3. اختبار ضوابط التطبيق

ما إن يتم تحديد الضوابط، فإن الخطوة التالية في عملية التدقيق هي التحقق من فاعلية هذه الضوابط.

يمكن تحقيق ذلك من خلال:

- إدخال مجموعة من بيانات الاختبار، التي تؤدي إلى نتائج معروفة في حال عمل التطبيق بشكل جيد.
- تطوير برامج مستقلة لتكرر العمل بحسب المنطق الخاص بالتطبيق و;
- تقييم نتائج التطبيق.

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

إذا كان للتطبيق بيئة تجريبية، فيمكن استخدامها لاختبار الضوابط طالما أن البيئة التجريبية هي نسخة مؤكدة عن بيئة العمل الحي للتطبيق.

لكي تختبر قواعد الحساب، مثل تلك المتعلقة بتحديث أصل الدين أو خدمة الدين، قد يحتاج المدقق إلى استخدام تقنيات التدقيق المحوسبة CAAT والتي تتضمن عدة أنواع من الأدوات والتقنيات مثل برمجيات التدقيق العام، والبرمجيات الخدماتية، 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 أدوات التحليل تطبيقات قاعدة البيانات وإخراج جدول تدفق منطقي. ويمكن استخدام برمجيات التدقيق المعممة لتحليل البيانات الصادرة عن معظم التطبيقات.

يجب أن يقوم المدقق بتقييم الحاجة إلى استخدام تقنيات التدقيق المحوسبة CAAT، والذي يجب أن يكون حسب مستوى تعقيد التطبيق المستخدم لإدارة الدين العام.

إن هذه الوثيقة تقدم منظومة اختبار مقترحة (الملحق 3)، والتي يمكن أن يستخدمها فريق التدقيق كمرجعية لاختبارات ضوابط التطبيق. تحدد هذه المنظومة بعض المتطلبات والوظائف التي يجب أن توفرها أنظمة الدين 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 الدين العام ستكون لها مواصفات مختلفة. وهكذا فإنه من مسؤولية فريق التدقيق أن يحدد ويستخدم البنود المتعلقة بأنظمة الديون في بلادهم ويعدلها عند اللزوم .

6.3. إعداد تقارير نتائج التدقيق

بالإضافة إلى الالتزام بإعلان ليما للمبادئ التوجيهية لقواعد التدقيق والمحاسبة، يجب أن تتوافق تقارير تدقيق أنظمة معلومات إدارة الدين العام مع المتطلبات المذكورة في المعيار الدولي للأجهزة العليا للرقابة ISSAI 5440 -المبادئ التوجيهية للقيام بتدقيق الدين العام- استخدام الاختبارات الأساسية في التحقيقات المالية، 2.6 إصدار تقارير نتائج التحقيق.

كما هو مذكور سابقا، فإن هذا التدقيق هو تدقيق للأداء. لذا فمن المهم أن يتبع التقرير معايير إصدار التقارير عن تدقيق الأداء، وذلك كما يحددها المعيار الدولي للأجهزة العليا للرقابة والمحاسبة ISSAI 3000 -معايير لتدقيق الأداء والمعيار ISSA/ 300 - المبادئ الأساسية لتدقيق الأداء.

الملحق 1: جدول التخطيط

الملحق 1: جدول التخطيط

المعلومات والوثائق والتقارير المطلوبة
» جرد أنظمة المعلومات التي يستخدمها مكتب الدين العام DMOوكذلك جرد وثائق الأنظمة ذات العلاقة.
» جرد كل من أنظمة تشغيل الحاسوب وأنظمة تشغيل الشبكات التي يستخدمها مكتب إدارة الدين DMO
» المخططات المحدثة لتدفقات عمليات مكتب إدارة الدين DMO
» تقارير الرقابة والمحاسبة السابقة والصادرة بخصوص مكتب إدارة الدين DMO
» تقارير الرقابة والمحاسبة السابقة بخصوص أنظمة تقنية المعلومات المتعلقة بالدين
» القوانين والأنظمة المتعلقة بإطار عمل مكتب إدارة الدين DMOوإدارة الدين العام
» لائحة بأسماء مدراء مكتب إدارة الدينDMO، وإدارة تقنية المعلومات، وإدارة استمرارية الأعمال، وإدارة الموارد البشرية، وإدارة المخاطر، والرقابة والمحاسبة الداخلية، وأمور أخرى، بالإضافة إلى مهامهم وعناوينهم وبريدهم الإلكتروني وأرقام هواتفهم.

» الوثائق المقصود منها إظهار واجبات مكتب إدارة الدين DMOو/أو أنظمته، مثل السياسات المكتوبة وأدلة إجراءات مكتب إدارة الدين DMO أو وزارة المالية:

- إدارة الموظفين
- أمن المعلومات
- إدارة التغيير
- الدخول إلى البني المادية
- متطلبات تقنية المعلومات ذات العلاقة ببيئة العمل والموقع
- الدخول إلى أنظمة المعلومات
- تخطيط استمرارية الأعمال BCP.
- خطة التعافي من الكوارث DRP
- خطة النسخ الاحتياطي
- الخدمات التي تقدمها أطراف ثالثة (خدمات تقنية المعلومات)
- تقارير تقييم المخاطر قبل حدوثها .
- الملخص الأخير للتقييمات الأمنية.
- القرارات الأمنية الأخيرة والتوصيات المتعلقة بها
- وضع التوصيات.
- موافقة الإدارة العليا على البدء باستخدام النظام

» التقارير التي أصدرتها الجهات الخارجية المسؤولة عن صيانة النظام

» الوثائق الاخرى المتعلقة بمكتب إدارة الدين العام و/أو النظام الخاص به (شرائح وعرض، نصوص، أهداف وتقارير سنوية عن إدارة الدّين)

- عدد موظفي مكتب إدارة الدين DMO الذين يستخدمون النظام وصلاحيات الولوج الخاصة بهم.
- عدد موظفي تقنية المعلومات ووصف العمل (تحديد المهام) لموظفي كل من مكتب إدارة الدين DMO وتقنية المعلومات.
- قائمة بالموظفين الذين يسمح لهم بالدخول إلى غرفة المختم.
- شرح مجموعة مواصفات السماح بالولوج إلى نظام معلومات إدارة الدين العام PDMIS
- المواصفات الرسمية للبرنامج الزمني وأسلوب تحديث نظام التشغيل وأنظمة الحماية والبرامج المضادة للفيروسات.
- قائمة الحواجز المادية والأدوات الآلية المستخدمة في منع الدخول غير المصرح به إلى الحاسوب الرئيسي ومحطات العمل (الحواسيب والخوادم وسوى ذلك من مرافق مكتب إدارة الدّين DMO
- موقع كل غرفة داخل وخارج مكتب إدارة الدّين DMO
- قائمة بأعداد كل من الموظفين والحواسيب والخوادم ومقادير المبالغ المخصصة في ميزانيات السنوات الخمس الماضية
- لائحة بدورات التدريب السابقة على استخدام نظام معلومات إدارة الدين العام PDMIS(بالنسبة لموظفي مكتب إدارة الدين) وتحديث خبرات تقنية المعلومات (بالنسبة لموظفي تقنية المعلومات).
- الأنظمة الرسمية والممارسات والمواصفات الموضوعة لمنع الأذى الذي قد تسببه حالات عدم استقرار الكهرباء والنار والغبار والماء والطعام ودرجات الحرارة الشديدة أو الرطوبة أو الكهرباء الساكنة.

- مواصفات عمل جهاز التزويد بالطاقة الكهربائية غير المنقطعة (في حال وجوده)
- سجلات الوقائع المتعلقة بطلبات مكتب إدارة الدين DMO بخصوص أخطاء نظام معلومات إدارة الدين العام PDMIS أو استخدام تقارير التعليمات
- التقارير الخاصة بسجلات وقائع الأمن
- لائحة بتغيرات برنامج نظام معلومات إدارة الدين العام في ال 12 شهر الماضية.
- السجلات والتقارير المتعلقة بالاختبارات الماضية لتخطيط استمرارية الأعمال BCP وخطة التعافي من الكوارث DRP والأحداث المؤثرة.
- توثيق التطبيقات والمستخدمين
- شروط استخدام كل تطبيق
- دليل الإجراءات للتعامل مع أخطاء المعالجة
- عينة البيانات اللازمة لإعادة تنفيذ عمليات إختبار ضوابط التطبيق وحساباته.

الإجراءات

- دراسة توثيق النظام (الكتيبات وشروط الاستخدام) لمعرفة العمليات الرئيسة للدين المنفذة في أنظمة المعلومات. في حال وجود توثيقات غير كافية لعمليات مكتب إدارة الدين، فيجب أن يقوم فريق التدقيق بمسح العمليات وعمل مخطط لها.

- التحقق من وجود القواعد القانونية المتعلقة باستخدام وصيانة وإدارة عمل نظام معلومات إدارة الدين العام.

- تحديد نتائج التحقيقات السابقة المتعلقة بنقاط الضعف في تدفقات عملية الدين العام و / أو أنظمة إدارة الدين العام.

- تحديد الضوابط العامة الرئيسة بناء على وثائق النظام.

- تحديد ضوابط التطبيق الرئيسة بناء على وثائق النظام: إدخال البيانات، ومعالجتها، وضوابط المخرجات.

- إجراء عملية تقييم للمخاطر على ضوابط التطبيق الرئيسية والعامة المذكورة لتقييم ماهية المخاطر التي تؤثر على هذه الأنظمة وشدة تأثيرها على إدارة الدين العام.

- تحديد أي من الأنظمة يؤثر على البيانات والوظائف الحساسة، مثل المدخلات، والمعالجة ومخرجات البيانات، ولائحة الدائنين، وحسابات الدين العام، وإنشاء التقارير، وصنع القرار.

- تحديد الضوابط الداخلية التي تنفذ لتخفيف المخاطر المكتشفة أو تقليصها.

- تصنيف الأنظمة والعمليات بناء على تقييم المخاطر وتحديد مجال التدقيق. تقدير الموارد والجدول الزمني.

- ترتيب المقابلات مع رئيس وحدة تقنية المعلومات، والمدراء والمجموعة التقية المسؤولة عن العمل على تطوير وصيانة وتشغيل النظام.

- تطوير منظومة تدقيق الضوابط العامة وضوابط التطبيق وتحديد الاختبارات التي سيتم تنفيذها. (انظر إلى المنظومة المقترحة في الملحق III).

يجب أن يجيب الجهاز الأعلى للرقابة والمحاسبة (/SA) على الأسئلة التالية

- ما هي أنظمة معلومات إدارة الدين العام وما هو دور كل منها في إدارة الدين العام؟
- هل تم تطوير نظام معلومات إدارة الدين العام PDMISمن قبل مكتب إدارة الدين DMO بشكل حصري أم هل تم اقتناؤها من طرف ثالث؟ في الحالة الثانية، فهل تم إجراء أي تعديل لتلبية أي حاجة محددة لمكتب إدارة الدّين؟
- من الذي يجب أن تتم مقابلته لمناقشة قضايا الضوابط العامة لتقنية المعلومات في مكتب إدارة الدّين؟
- من الذي يجب أن تتم مقابلته لتوضيح ضوابط التطبيقات في نظام معلومات إدارة الدّين العام؟
- من هم المستخدمون الرئيسيون لنظام معلومات إدارة الدّين العام؟
- ما هي الضوابط العامة وضوابط التطبيقات في نظام معلومات إدارة الدّين العام؟
- هل الضوابط الداخلية قادرة على تخفيف مخاطر أنظمة المعلومات التي يمكن أن تؤثر على إدارة الدّين العام؟
- ما هي أكبر المخاطر المتعلقة بإدخال البيانات ومعالجتها ومخرجاتها في نظام معلومات إدارة الدّين العام؟
- ما هي الاختبارات المتعلقة بالضوابط العامة وضوابط التطبيقات والتي يجب أن تنفذ؟

الملحق 2: منظومة اختبار الضوابط العامة

الضوابط العامة		
إن هدف الضوابط العامة هو تأمين البيانات وحماية برامج التطبيقات وضمان استمرار عمليات الحاسوب في حال طروء أي عوائق غير متوقعة.		
المتطلبات/ الوظائف	الضوابط العامة	اقتراحات من أجل إجراءات الاختبار
أسئلة عامة	يجب أن تكون أنشطة قطاع تقنية المعلومات متوافقة مع مهمة مكتب إدارة الدّين. يجب أن يتم مراقبة أداء نظام معلومات إدارة الدّين العام PDMIS بما يتناسب مع أهداف مكتب إدارة الدّين DMO.	مراجعة عينات من قرارات الإدارة أو المذكرات المتعلقة بأعمال تقنية المعلومات، لضمان كونها واضحة، ومبررة ومتوافقة مع مهمة مكتب إدارة الدين العام. تقييم معايير أداء نظام معلومات إدارة الدين مقابل المؤشرات المتوقعة والتأكد من إقرار الإدارة العليا لهذه المعايير. تقييم تقارير التدقيق الداخلية السابقة عن ضوابط تقنية المعلومات العامة من أجل تحديد مواطن الضعف المهمة .

أسئلة عامة	يجب تنفيذ تدقيق داخلي دوري على عمليات مكتب إدارة الدّين/ نظام معلومات إدارة الدّين العام.	تقييم كل من أعداد وقدرات الحواسب والأجهزة الأخرى، وكذلك الموظفين، والتأكد من خلفية الموظفين الأساسية المطلوبة . تقييم المبالغ المخصصة من الميزانية ومقارنتها مع الفترات السابقة وقطاعات تقنية المعلومات في الأجهزة الحكومية الأخرى.
الضوابط التنظيمية	يجب أن يلتزم مكتب إدارة الدين أو إدارة صندوق النقد بتطوير وصيانة بيئة تقنية معلومات عامة جيدة. يجب أن يحصل الموظفون في إمكتب إدارة الدين وفي تقنية المعلومات على تدريب دوري وملائم يتضمن الوعي الأمني . يجب وجود برنامج تدريب. يجب وجود سياسات مكتوبة وإجراءات موحدة في: • أمن المعلومات. • الموارد البشرية. • خدمات تقنية المعلومات التي يقدمها طرف ثالث. • إدارة التغيير. • الولوج المادي والمنطقي إلى الأنظمة. • تخطيط استمرارية الأعمال والتعافي من الكوارث. يجب أن يتم تحديث السياسات والإجراءات الموحدة بشكل دوري.	إجراء مقابلة مع الإدارة العليا لمكتب إدارة الدين للتعرف على مدى اهتمامهم بتقنية المعلومات من أجل تقييم التزامهم بتطوير والحفاظ على بيئة تقنية معلومات عامة جيدة. الاطلاع على الأدلة التي تشير إلى حدوث الدورات التدريبية. إجراء مقابلات مع المستخدمين من مكتب إدارة الدين ومع موظفي تقنية المعلومات بشأن: • وتيرة التدريب. • الحاجة إلى المعرفة / التدريب. • المعرفة بالسياسات. تقييم ملاءمة السياسات المكتوبة والإجراءات الموحدة لخدمات تقنية المعلومات. مراقبة ما إذا كان فريق عمل مكتب إدارة الدين يعمل وفقا للإجراءات الموحدة (الموجودة في دليل الاستخدام).

الضوابط التنظيمية	يجب أن يكون موظفو مكتب إدارة العاملين بهذه السياسات. يجب أن يوجد توثيق إجرائي يغطي كل نشاطات إدارة الدّين. يجب أن تفصل المؤسسة بصورة مناسبة بين واجبات المستخدمين، لكي تضمن عدم حصولهم على أكثر من السلطات التي تتطلبها مهامهم.	
الضوابط المادية	يجب أن يكون الوصول إلى الحاسوب الرئيسي والخوادم محمية جيدا (باب، قفل، الخ...). يجب أن يكون هناك مراقبة عن طريق كاميرات الفيديو. يجب أن تكون نوافذ غرفة الحاسوب الرئيسي والخوادم محمية من اي دخول قسري. يجب أن يكون كل من يدخل إلى غرفة المخدم مخولا بذلك.	التحقق من وجود العوائق المادية الفعالة ومن عملها لمنع الدخول غير المصرح به إلى الحاسوب الرئيسي والخوادم وأجهزة الحاسوب في مكتب إدارة الدّين. التحقق من أن الإجراءات الادارية للموظفين، والتي تمنع الدخول غير المصرح به وتمنع التدخل في عمل خدمات تقنية المعلومات، تتوافق مع المعايير الرسمية وتعمل بطريقة مرضية. من أجل تحديد أي ضعف في الضوابط الآلية، يتم تفحص كيفية عمل الأدوات الإلكترونية مثل أقفال الأبواب الإلكترونية، ونظام الأقفال ذات المفتاح الإلكتروني، وكاميرات المراقبة والوسائل الأخرى لتقييد الدخول المادي إلى الخوادم والبني التحتية الحساسة.

الضوابط المادية		في حال وجود أنظمة الأقفال ذات المفاتيح، ينبغي البحث عما إذا ما كان الموظفون يتشاركون في كلمات السر بينهم.
الضوابط المنطقية	إذا قامت مصادر خارجية بتعهد خدمات تقنية معلومات الدين العام، يجب أن يحدد العقد ضوابط كافية لضمان عدم وصول أي طرف ثالث إلى أسرار العمل والبيانات الهامة واستراتيجيات الدّين العام. لا يجب أن يوجد وضع وصول نشط لأي موظف سابق أو شخص غير موظف في مكتب إدارة الدين أو أي مستخدم "افتراضي". يجب مراجعة حقوق الولوج إلى أنظمة المعلومات بشكل دوري. ضمان عمل البرامج المحدثة لمكافحة الفيروسات، وجدران الحماية، وكشف البرمجيات الخبيثة ومكافحة التسلل. يجب القيام بتحديثات منتظمة لأنظمة التشغيل في أجهزة الحواسيب والخوادم. يجب أن تضع المؤسسة إجراءاتها الخاصة بها لإعطاء الإذن بالولوج وإلغائه وتعديله عندما تتغير الظروف (التعيينات الجديدة، وإنهاء العقود، وتغيير المهام.. الخ)	تقييم ما إذا كانت أوضاع الوصول الخاصة بالموظفين ملائمة لأدوارهم. التحقق مما إذا كان أي موظف سابق أو أي شخص غير موظف في مكتب إدارة الدين يزال يتمتع بوضع وصول سار دخول النظام. التحقق من وجود جدران الحماية، برامج محدثة لمكافحة الفيروسات وكشف البرمجيات الخبيثة ومكافحة التسلل. التحقق مما إذا كان يتم تحديث أنظمة تشغيل الحواسب والخوادم بصورة منتظمة. التحقق مما إذا كان يتم تنفيذ سياسة كلمات السر بطريقة ملائمة. التحقق مما إذا كانت الإجراءات معرفة وموثقة بشكل مناسب.

الضوابط المنطقية	يجب أن تعلن المؤسسة سياستها أو توجيهاتها بشأن كلمات السر وضوابط الأمن الأخرى (بطاقات الدخول. الخ) على جميع مستخدمي نظام إدارة الدّين.	
ضوابط بيئة العمل	يجب أن توجد أنابيب (للماء، ونظام التدفئة، والكهرباء، الخ...) في غرفة المخدم. يجب أن توجد كواشف للماء والحرارة والرطوبة. يجب أن يوجد نظام مضاد للفيضان في غرفة المخدم. يجب وجود أجهزة كشف للدخان/الحريق. يجب أن تكون الأرض مرتفعة أو أن يكون الجهاز مرفوعة على رفوف تعلو بقدر 20-15 سم عن الأرض. يجب وجود مصدر كهربائي غير قابل للانقطاع (UPS) للمحافظة على استمرارية تشغيل الحاسوب الرئيسي والخوادم.	زيارة غرفة خوادم قاعدة البيانات لفحص وتقييم الشروط البيئية - وينطبق هذا على غرف مكتب إدارة الدّين الأخرى. التأكد من وجود وفعالية صيانة الأجهزة المستخدمة في الوقاية من الحريق والطوفان والرطوبة. التحقق من وجود وفعالية مصادر الكهرباء الاحتياطية وعملها بشكل جيد لتجنب الانقطاع في خدمات تقنية المعلومات.

ضوابط تغيير البرامج	يجب أن تحتفظ إدارة تقنية المعلومات بسجل تدقيق لمشاكل التشغيل والحوادث والأخطاء. يجب على السجل أن يتتبع الواقعة ابتداء من سببها وحتى حلها. يجب ألا تتبقى بدون حل في مكتب المساعدة أية طلبات مهمة ذات علاقة بنظام معلومات إدارة الدين العام .PDMIS يجب أن يكون هناك نظام التصعيد المشاكل بالنسبة للأحداث ذات الطبيعة الحساسة، ويجب أن توجد طريقة لتحديد المستوى المناسب للاستجابة بناء على أولوية الحدث. يجب إعداد تقرير عن الحوادث الأمنية ويجب توجيهه إلى مدراء مكتب إدارة الدين . DMO إن التغييرات السابقة يجب أن تتبع الإجراءات الموحدة. في حال استخدام نظام إدارة دين غير معياري، فيجب على المؤسسة أن توثق إجراءات ضوابط التغيير وتحدد صفات الشخص المخول بإجراء التغييرات على النظام	تقييم الوقت اللازم لحل متطلبات مكتب إدارة الدين المتعلقة بتعليمات الاستخدام أو الفشل في وظائف نظام معلومات إدارة الدّين العام. تحديد حالات فشل نظام معلومات إدارة الدّين العام المتكررة وأسبابها المحتملة. مقارنة التغيرات السابقة مع الإجراءات الموحدة.

ضوابط تغيير البرامج	يجب على المؤسسة أن تتعقب وتراقب كل التغييرات في نظام الدين (سجّل تعقّب التدقيق).	
تخطيط استمرارية الأعمال BCP وخطة التعافي من الكوارث DRP.	يجب أن يضع مكتب إدارة الدين خطة لاستمرارية الأعمال وأخرى للتعافي من الكوارث. يجب أن يعلم الموظفون المسؤولون عن استمرارية التشغيل أدوارهم ومسؤولياتهم. يجب تقديم تقارير عن نقاط الضعف التي لوحظت في الاختبارات السابقة لخطط استمرارية الأعمال والتعافي من الكوارث، أو في الحوادث الحقيقية، ويجب رفع تقرير بالأعمال التي يقوم بها مكتب إدارة الدين لحل نقاط الضعف هذه. يجب الحفاظ على وثائق القروض في مكان آمن حيث يتم حماية الوثائق من السرقة أو الحريق أو الفيضان أو أي حادث آخر قد يتلفها أو يدمرها.	تقييم تناسق وشمول خطة استمرارية الأعمال وخطة التعافي من الكوارث ومعرفة ما إذا كان يتم تحديثهما. تقييم التقارير المقدمة عن الاختبارات السابقة لخطة استمرارية الأعمال وخطة التعافي من الكوارث وخطة النسخ الاحتياطي. التحقق من أن خطة استمرارية الأعمال وخطة التعافي من الكوارث قد تم توزيعهما على جميع أفراد طاقم العمل بشكل مناسب. التحقق من أن النسخ الاحتياطية الموجودة في موقع آخر في وضع جيد ويمكن استخدامها لإعادة تشغيل النظام في حال حصول أعطال.

الملحق 3: مصفوفة اختبار ضوابط التطبيقات

معايير التوثيق		
تهدف معايير التوثيق المناسبة إلى ضمان عمل الضوابط باستمرار والتقليل من خطر الأخطاء.		
المتطلبات/ الوظائف	**ضوابط التطبيقات**	**اقتراحات من أجل إجراءات الاختبار**
ظوابط التوثيق	يجب أن يكون توثيق التطبيقات شاملا بما فيه الكفاية (بكل وظائف التطبيق والأداء المتعلق بها).	تفحص الوثائق.
	يجب أن يكون التوثيق محدثا لتعكس التعديلات الجارية على التطبيق.	تفحص الوثائق.
	إن ضوابط التطبيق المذكورة في الوثائق يجب أن تكون موضع التنفيذ وتعمل بشكل فعال.	صنع عينة من ضوابط التطبيق مما ذكر في ضوابط التوثيق والتأكد من أنها تنفذ حسب الوثائق وتعمل بفعالية.
النسخ الاحتياطي للوثائق	يجب الاحتفاظ بنسخة احتياطية عن الوثائق.	تفحص النسخة الاحتياطية من الوثائق.

ضوابط الإدخال		
تهدف ضوابط الإدخال إلى ضمان صحة توقيت البيانات المدخلة في التطبيقات، وتمامها، ودقتها ووجود الإذن بإدخالها .		
المتطلبات/ الوظائف	**ضوابط التطبيقات**	**اقتراحات من أجل إجراءات الاختبار**
حقول الإدخال الإجبارية	لا يسمح التطبيق بتأكيد العملية في حال لم يتم تعبئة جميع حقول الإدخال الإجبارية.	محاولة تأكيد العملية بعدم إدخال البيانات اللازمة والتثبت من عدم قبول البرنامج لهذه العملية. يجب تطبيق هذا الاختبار على العمليات التالية: تسجيل العقود، تفعيل العقود، تسجيل إصدار الضمانات ... الخ.
إدخال صحيح ومناسب للبيانات	لا يقبل التطبيق أي إدخال غير صحيح أو غير مناسب للبيانات.	تفحص تنسيق البيانات في قاعدة البيانات. مراجعة مواصفات موانع الإدخال والتأكد من بعضها في التطبيق محاولة القيام بإدخال بيانات غير صحيحة أو غير مناسبة والتأكد من وجود موانع إدخال ورسالة خطأ يجب أن يتم تطبيق هذا الاختبار على العمليات التالية: تسجيل العقود، تفعيل العقود، تسجيل إصدار الضمانات، تحديث القوائم، استرداد قيمة الضمانات ... الخ.

إدخال صحيح ومناسب للبيانات	لا يسمح التطبيق بتكرار إدخال البيانات نفسها.	محاولة تسجيل عقد أو ضمانات بنفس الاسم الذي سجل به عقد موجود سابقة، والتحقق من وجود موانع إدخال ومن إظهار رسالة عن تكرار البينات.
	لا يجب وجود فترات تداخل أو فترات غير مغطاة تتعلق بتطبيق معدلات الفائدة على العقود.	فحص قاعدة البيانات للتأكد مما إذا كانت هناك فترات فيها معدلات فائدة متداخلة أو غير مغطاة.
	في حالة عقود المنح، يجب على التطبيق أن يسمح بإدخال عملية الصرف لأنه في هذه الحالة ليس هناك استهلاك للدين ولا عمليات ذات علاقة بالفوائد.	محاولة إدخال عمليات صرف لعقود المنح والتحقق من أن التطبيق لا يتطلب استهلاكا للدين أو عمليات فائدة
	في شاشة إدخال بيانات الصرف، عندما يبحث المستخدم عن العقود من أجل تسجيل عملية الصرف، يجب أن يظهر التطبيق فقط العقود التي في حالة "نشاط في حقل "الصرف" أو في مرحلة "الصرف واستهلاك الدين".	محاولة إدخال عملية الصرف والتحقق من أن التطبيق يظهر العقود التي هي في المرحلة الصحيحة.
	إذا كان نظام معدلات الفائدة في حالة تعويم، التطبيق يجب ان يطلب تضمين المؤشر.	فإن التحقق مما إذا كان التطبيق يتطلب تضمين المؤشر عندما يتم اختيار نظام معدلات الفائدة المعول به.
	يجب ألا يسمح التطبيق بإدخال الكسور العشرية في سندات الضمان الصادرة.	محاولة إدخال الكسور العشرية في سندات الضمان الصادرة والتحقق من إعاقة التطبيق للعملية.
	يجب أن يسمح التطبيق بإنشاء سند الضمان قبل إصداره.	محاكاة إنشاء سند ضمان مالي بدون إصداره.

إكمال المعلومات	يجب إدخال كل المعلومات المتعلقة بالدّين في التطبيق.	التحقق من إدخال جميع بيانات الدّين الهامة في التطبيق مثل عملية الائتمان والضمانات والقروض ومعدلات الفائدة و معدلات صرف العملات...الخ.
التنسيق بين التواريخ	يجب أن يكون تاريخ بداية حساب معدل الالتزام سابقا لتاريخ انتهاء المشروع.	محاولة إدخال تاريخ بداية حساب معدل الالتزام متأخرا عن تاريخ انتهاء المشروع والتحقق من وجود إعاقة ورسالة عن الخطأ.
	يجب أن يكون تاريخ فعالية العقد قبل انتهاء المشروع.	محاولة إدخال تاريخ فعالية متأخرا عن تاريخ انتهاء المشروع والتحقق من وجود اعاقة ورسالة عن الخطأ.
	يجب أن يكون تاريخ الفعالية قبل تاريخ موعد انتهاء الصرف.	محاولة إدخال تاريخ فعالية متأخرا عن تاريخ انتهاء الصرف والتحقق من وجود الموانع ورسالة عن الخطأ.
	يجب أن يكون الموعد النهائي للصرف سابقا لتاريخ انتهاء المشروع.	محاولة إدخال موعد نهائي للصرف متأخرا عن تاريخ انتهاء المشروع والتحقق من وجود موانع ورسالة عن الخطأ.
	للحصول على تقرير استحقاق الدّين، يجب أن يكون تاريخ استحقاق الضمانات المالية متأخرا عن تاريخ بدنه.	محاولة إدخال موعد البدء متأخرا عن تاريخ انتهاء استحقاق الضمانات المالية والتحقق من وجود أي إشارة إلى رسالة خطأ.
	لا يقبل التطبيق تواريخ مستقبلية للعمليات.	محاولة إنجاز بعض العمليات عم طريق ادخال تاريخ مستقبلي والتحقق من وجود موانع ورسالة خطأ.

التنسيق بين التواريخ	لا يقبل التطبيق تواريخ مستقبلية للعمليات.	يجب أن يتم تطبيق هذا الاختبار على العمليات التالية: تسجيل العقود، تفعيل العقود، تسجيل إصدار الضمانات المالية، تحديث المؤشرات، استرداد الضمانات، تسجيل الصرف والإضافة على العقود... الخ.
	يجب أن يكون تاريخ إصدار الضمان المالي قبل تاريخ استحقاق الدّين.	محاولة إدخال تاريخ الإصدار متأخرة عن تاريخ استحقاق الدين والتحقق من وجود موانع ورسالة خطأ.
	عند تسجيل دفعة استهلاك الدين، في الحالات التي يختلف فيها المبلغ أو التاريخ المدخل عن الموجود في التطبيق، يجب على التطبيق أن يعرض رسالة يخبر فيها المستخدم بهذا الوضع قبل تأكيد إكمال العملية.	تسجيل دفعة بتاريخ أو قيمة مختلفين عن الموجودين في التطبيق والتحقق من أن التطبيق يعرض رسالة.
	إذا كان تاريخ سداد الدين مختلفة عن تاريخ استحقاقه، يجب على التطبيق أن يطلب تعبئة حقول "تبرير" أو"موافقة الدائن".	إدخال تواريخ مختلفة لاستحقاق الدين وسداده والتحقق مما إذا كان التطبيق يطلب تبريرة أوموافقة.
	لا يمكن أن يكون العمليات الصرف المستحقة فترات متداخلة. فمثلا لا يمكن أن يكون تاريخ بداية عملية الصرف الثانية قبل تاريخ نهاية عملية الصرف الأولى.	محاولة إدخال تاريخ الصرف الثاني قبل التاريخ الأول والتحقق من وجود موانع ورسالة خطأ.

أمن إدخال البيانات والعمليات	بالنسبة للأشخاص غير المصرح لهم، يجب ألا يسمح التطبيق لهم بإدخال بعض البيانات والقيام ببعض العمليات.	التأكد من وجود رمز الولوج Tokenومتطلبات وضع الوصول المحدد. محاولة إدخال البيانات وإنجاز بعض العمليات بدون وجود ملف مستخدم مناسب وتفحص موانع الإدخال. يجب تطبيق هذا الاختبار على العمليات التالية: تسجيل العقود، تفعيل العقود، تسجيل إصدار الضمانات المالية، تغيير المؤشرات، استرداد الضمانات المالية، تسجيل الدفعات... الخ.
	يجب أن يقوم التطبيق بحفظ سجل الدخول في حال إدخال البيانات بطريقة يدوية.	التأكد من وجود سجلات دخول مقيدة وما إذا لا يمكن الاطلاع على هذه السجلات أو تعديلها من طرف أفراد غير مسموح لهم بذلك.
	يجب ألا يسمح التطبيق بتغيير قيمة عقد بعد تفعيله.	محاولة تغيير قيمة عقد مفعل والتأكد من وجود موانع.
	يجب أن يمنع التطبيق تعديل البيانات وحذف العقود التي تشير حالتها إلى "ملغي" أو "منتهي".	محاولة تعديل وحذف بعض البيانات من عينة عقد مصنف تحت حالة "ملغي" أو "منتهي" والتحقق من أن نظام معلومات إدارة الدين العام يمنع مثل هذه المحاولات.
	لا يجب أن يسمح التطبيق باستثناء أي عقد نشط إلا إذا كان العقد قيد التفاوض أو كان غير مفعّل.	محاولة حذف عقد مفعل والتحقق من وجود ما يمنع ذلك.

أمن إدخال البيانات والعمليات	لا يجب أن يسمح التطبيق بالاستبعاد الخاطئ لأي سند ضمان صادر إلا في حال عدم وجود أي عملية مرتبطة بهذا السند.	محاولة حذف سند ضمان صادر مع وجود عملية مرتبطة به والتأكد من وجود ما يمنع ذلك.
	يجب أن يطلب التطبيق موافقتين لإنجاز عمليات حساسة.	التأكد من أن إنجاز العمليات الحساسة يحتاج إلى موافقتين. يجب أن يتم تنفيذ هذا اختبار على العمليات التالية: تفعيل العقود، إصدار سندات الضمان، دفع المال المخصص للسداد، استرداد سندات الضمان، تغيير قيمة العقود، دفعات القسائم، إبطال الدفعات، تغيير معدلات الفائدة... الخ.
	يجب أن يقبل التطبيق إدخال البيانات من مصادر معترف بها حصرا. يجب أن يتم إدخال القروض وفق الاتفاقية والمعايير المتفق عليها.	التأكد من أنه قد تم إدخال البيانات الرئيسة مرتين وبأن رسالة الخطأ تظهر عندما تكون البيانات مختلفة.
	يجب أن يسمح التطبيق بتخفيض القيمة التعاقدية طالما أن قيمتها لا تتجاوز قيمة "الميزانية التي يجب صرفها".	محاولة تخفيض قيمة العقود بمقدار أكثر من القيمة التي سيتم صرفها والتأكد من وجود موانع وظهور رسالة خطأ.
	يجب أن يسجل التطبيق جميع العمليات مرة واحدة فقط.	إنجاز بعض العمليات المتطابقة (مثل: دفع المال المخصص للسداد) والتأكد من وجود موانع ومن عدم تكرار العمليات نفسها في قاعدة البيانات.

أمن إدخال البيانات والعمليات	عند تسجيل الدفعات، إذا كان إذن المستخدم ملغى، فيجب أن يقوم التطبيق برفع تقرير فقط عندما يقوم المستخدم بإعطاء أمر "الإدخال" وهكذا يسمح التطبيق بتسجيل المحاولة الفاشلة وكذلك البيانات التي أراد المستخدم إدخالها.	محاولة تسجيل دفعة بإذن ملغى والتحقق من وجود موانع وسجلات لهذه العملية.
	في حالة نقل الملفات آليا بين التطبيقات، يجب أن يحافظ نظام معلومات إدارة الدين العام PDMIS على البيانات الأصلية المستلمة من تطبيقات أخرى لفترة يحددها مسبقا مكتب إدارة الدين.	تفحص البيانات المحتفظ بها والمنقولة من تطبيقات أخرى للتأكد من أن البيانات مشفرة أو محمية من الضرر والضياع والاختراق.
	يجب ألا يسمح التطبيق بتعديل معدلات الفائدة لأي قسط تم دفعه سابقا. كما يحتاج أي تعديل لمعدلات الفائدة إلى موافقة ثانية من أجل إكماله.	محاولة تعديل معدل الفائدة لقسط تم دفعه سابقا والتأكد من وجود موانع. راجع ما إذا كان التطبيق بحاجة إلى موافقة ثانية لتغيير معدل الفائدة.
التوافق بين القيم	يجب أن تكون قيمة الشريحة الائتمانية أقل من قيمة العقد.	محاولة إدخال قيمة للشريحة أكبر من قيمة العقد والتأكد من وجود موانع ورسالة خطأ.
	يجب أن تكون قيمة الاسترداد أقل من قيمة سند الضمان الصادر.	محاولة القيام باسترداد سند ضمان بقيمة أعلى من قيمة السند الصادر والتأكد من وجود موانع ورسالة خطأ.
	يعرض التطبيق تنبيها عن الدفعات الناقصة أو الزائدة قبل المعالجة.	محاكاة القيام بدفعة ناقصة أو زائدة والتأكد من وجود التنبيه.
وثائق المصدر	يجب وجود تتبع لوثائق المصدر الخاصة بالبيانات المدخلة لضمان صحة إدخال البيانات.	اختيار بعض البيانات المدخلة والتأكد من أن لها وثيقة مصدر خاصة بها (مثل عقود القروض، البريد الإلكتروني، المعلومات الإلكترونية. الخ).

ضوابط المعالجة		
تهدف ضوابط المعالجة إلى ضمان معالجة البيانات بدقة من خلال التطبيق وبضمان عدم إضافة أو ضياع أو تبديل أي بيانات خلال المعالجة..		
المتطلبات/ الوظائف	**ضوابط التطبيق**	**اقتراحات من أجل إجراءات الاختبار**
المؤشر المناسب للحالة	يجب أن يغير التطبيق مؤشر حالة العقد بعد تمام الصرف الكلي.	محاكاة حالة إنهاء الصرف والتحقق من تغير حالة العقد من "جاري الصرف" إلى تم الصرف بشكل كلي".
	يجب أن يغير التطبيق حالة سند الضمان المالي عند تأكيد إصداره.	محاكاة تأكيد إصدار سند ضمان والتحقق من تغير حالة السند من حالة "غير نشط" إلى حالة "نشط".
	يجب أن يغير التطبيق حالة العقد أو سند الضمان بعد الدفع بشكل كامل.	محاكاة الدفعة الأخيرة والتحقق من تغير حالة العقد أو سند الضمان.
	على الأقل يجب أن تكون المراحل التالية ممكنة الاختيار في التطبيق: • جاري الصرف: يمكن إنشاء دفعات الصرف في هذه المرحلة. • اكتمل الصرف: لا يسمح بإجراء عمليات الصرف في هذه المرحلة. • انتهى: في هذه المرحلة، لا يمكن القيام بأية عمليات مالية لها علاقة بالصرف ولا يسمح بتعديل أي بيانات.	قم بإنشاء عقد، وحاول إنجاز عملية صرف في كل مرحلة وتأكد من وجود موانع ورسالة خطأ.

المؤشر المناسب للحالة	يجب أن يتضمن التطبيق قوانين لجعل حالة العقود (مفعلة، غير مفعلة) متوافقة مع المراحل (جاري الصرف، اكتمل الصرف، جاري سداد الدين، جاري الصرف والتسديد، انتهى) من أجل منع التناقض في المعلومات. مثلا العقد الذي يكون في حالة "غير مفعل" لا يمكن أن يكون في مرحلة "جاري الصرف" أو الجاري سداد الدّين".	محاكاة بعض التغييرات في حالة العقد ومراحل العقد والتأكد من توافقها.
	يجب أن يتضمن التطبيق برنامج لتحديث مراحل العقد. مثلا عندما يكون باقي الميزانية التي ستنفق صفرة، يقوم التطبيق بتعديل المرحلة من "جاري الصرف" إلى "اكتمل الصرف".	محاكاة الشروط الضرورية لتغيير مراحل العقود والتأكد من تغيرها.
الحساب الصحيح	يجب على التطبيق أن ينجز الحسابات بشكل صحيح.	التحقق من الحساب وإعادة الأداء. يجب القيام بهذا الاختبار على المعلومات التالية: أصل الدّين (التعاقدي والمسنّد) واستحقاق الدّين والجدول الزمني الاستهلاك الدّين (التواريخ والقيم)، قيمة عمولة الوكلاء، تدفق دفع سندات الضمان، القيمة المالية لاسترداد السند...الخ).

الحساب الصحيح	بعد تغير بعض البيانات المدخلة، يجب على التطبيق أن يجري الحسابات ويحدث البيانات.	إدخال بعض التغييرات والتحقق من تحديث البيانات والنتائج على سبيل المثال: • محاكاة تسديد دفعة والتحقق من أن باقي الرصيد المستحق وتدفق السداد قد تم تحديثهما • تغيير بعض المؤشرات والتحقّق من تحديث قيمة أصل الدّين.
	يجب أن يتضمن التطبيق في برمجته الطرق التالية على الأقل لحساب الأقساط: التوزيع المنظم، الفائدة البسيطة، القسط، تطبيق السعر، تطبيق السداد الثابت، سلة العملات الموحدة (البنك الدولي للإنشاء والتعمير)، وسلة عملات UAC (IDB)	التحقق من الطرق التي يستخدمها النظام لحساب الأقساط. يمكن تفحص صحة هذه الطرق بتجربتها على عينة من البيانات.
	كلما تغير حقل "القيمة التعاقدية " فيجب على التطبيق أن يعيد حساب حقل "رصيد العقد الذي سيتم صرفه" بصورة تلقائية".	تغيير القيمة التعاقدية والتحقق من أن حقل رصيد العقد الذي سيتم صرفه" قد تم تحديثه بشكل صحيح.
	يجب أن يولّد التطبيق تواريخ الأقساط بشكل آلي حسب الطرق الممكنة التالية: تاريخ البداية والعدد الثابت للأقساط. تاريخ البداية وتاريخ النهاية والعدد المتناقص للأقساط. تاريخ البداية والنهاية والعدد الثابت للأقساط. تاريخ البداية وعدد الفترات.	إدخال البيانات المطلوبة في كل طريقة ممكنة والتحقق مما إذا كانت تواريخ الأقساط صحيحة.

الحساب الصحيح	عندما يتصادف تاريخ القسط مع يوم عطلة، يجب على التطبيق أن يتيح خيارين: تأخير التاريخ إلى اليوم التالي (يوم عمل) أو تقديمه إلى يوم العمل السابق للعطلة.	إنشاء قسط بتاريخ يوم عطلة والتحقق من أن التطبيق يسمح بتغيير التاريخ إلى يوم العمل السابق أو التالي.
	يجب أن يقوم التطبيق بتحديث القيمة الاسمية لسندات الضمان بشكل آلي عند حصول تغيير في المؤشر المعني.	تغيير مؤشر أحد سندات الضمان والتحقق من تحديث القيمة الاسمية المعنية.
	في حالة دفع مبلغ أقل قام التطبيق بحسابه، تظهر رسالة تخبر بذلك في لحظة إدخال الدفعة. يجب أن يتكرر عرض هذه الرسالة حتى حلول موعد القسط التالي.	محاكاة دفعة أقل من المبلغ الذي تم حسابه من قبل التطبيق والتحقق من عرض رسالة وتكرارها حتى موعد القسط التالي.
	يجب أن يقوم النظام في قاعدة بياناته بتمييز سندات الضمان المصدرة بغرض المحاكاة.	التحقق في قاعدة البيانات من التمييز بين سندات المحاكاة والتأكد من إهمالها أثناء حسابات أصول الدين واستحقاقه.
	عندما يقوم المستخدم بحذف سند ضمان، يجب على التطبيق أن يحذف القيم المتعلقة به في قاعدة البيانات.	حذف سند ضمان والتحقق من أنه قد تم حذف قيمته من قاعدة البيانات.
	لا يجب اعتبار السندات التي تكون في حالة "ملغي" في حسابات سندات الدّين (مثل معدل العائد الداخلي واستحقاق الدين ...الخ) أي أنه بعد إلغاء السندات، يجب استبعاد القيم المتعلقة بها بشكل دائم من قاعدة البيانات.	تغيير حالة السند إلى "ملغي" والتحقق من أن قيمته قد تم إهمالها في الحسابات (الأصل، استحقاق الدين.. الخ).
	يجب أن يعالج التطبيق الأقساط المتأخرة بشكل مختلف.	التحقق من أن التطبيق يقوم بحساب الرسوم بشكل صحيح على الأقساط المتأخرة.

الضبط الصحيح الأخطاء المعالجة	يجب ألا تبقى أخطاء المعالجة بدون أحل الأيام أو لأسابيع.	التحقق من وجود معيار يتعلق بعدد الأيام التي تستغرقها معالجة الأخطاء في النظام. التحقق من وجود رسائل خطأ، والتحدث مع مدراء النظام/مدراء الدين لمناقشة الإجراءات المتخذة لتصحيح الأخطاء.
	في حال حدوث خطأ في المعالجة، يجب على التطبيق أن يلغي المعالجة ويحفظ في قاعدة البيانات كلا من التاريخ والوقت والسبب التقني للمشكلة.	محاكاة معالجة خطأ والتأكد من أن التطبيق قام بتخزين المشكلة الحاصلة في قاعدة البيانات.
التسجيل الصحيح	يجب أن يخول التطبيق مدراء الدين تسجيل التدفق النقدي (المرتبط بالعملة الأجنبية واقتراض العملة المحلية، ونشاطات التعامل التجاري والتحوط، والضمانات والإقراض) بشكل دقيق الجميع المعاملات.	تنفيذ عملية ما والتحقق من صحة ودقة سجلها.
	يجب على التطبيق أن يحتفظ بسجل للمعاملات المنفذة خلال فترة العقد كما يجب أن يتضمن تفاصيل عن الدائن، والقيمة التعاقدية، وتاريخ إغلاق المشروع، والتواريخ المحددة لحقول الصرف.	اختيار بعض العقود والتحقق من وجود سجل الجميع المعاملات المنفذة خلال فترتها مع وجود جميع التفاصيل الضرورية.
	يجب أن يكون للتطبيق سجل للدين لكل أداة دين.	التحقق من أن العمليات التاريخية المرتبطة بالسند أو العقد توافق مع سجل التنين الخاص به.
المهام المجدولة الصحيحة	يجب على التطبيق أن يبدأ وبشكل آلي المهام المجدولة الموضوعة من قبل مكتب إدارة الدين لتحديث المؤشرات وأصول الدين ... الخ.	التحقق من وجود البدء الآلي وعمله بشكل صحيح.

المهام المجدولة الصحيحة	في حال كان سداد الدين لسند ما بنفس تواتر الفائدة (السعر على سبيل المثال) فيجب على النظام أن يتأكد من أن الفائدة والسداد جدول الدفع نفسه.	إنشاء سند ضمان بسداد وفائدة لهما نفس التواتر والتحقق من أن لهما نفس جدول الدفع.
تتبع التدقيق	يجب أن يتم الحفاظ على سجل تتبع التدقيق لنظام معلومات إدارة الدين العام للتمكن من متابعة عقد الدين أو سند الضمان منذ لحظة التوقيع أو الإصدار إلى السداد.	التحقق من وجود سجل تتبع التدقيق لعينة من العقود والسندات منذ لحظة التسجيل إلى السداد.

ضوابط المخرجات		
تهدف ضوابط المخرجات إلى ضمان سلامة المخرجات والتوزيع الصحيح للمخرجات الناتجة في الوقت المناسب.		
المتطلبات/ الوظائف	**ضوابط التطبيق**	**اقتراحات من أجل إجراءات الاختبار**
ضوابط على مستخدمي المعلومات	يجب أن يحوي التطبيق على سجل للتقارير للحفاظ على اسم المستخدم الذي طلب التقرير وتاريخ وساعة الطلب أيضا.	طلب بعض التقارير والتحقق من أن التطبيق يسجل البيانات.
	يجب أن يطلب التطبيق تفويض خاص لتحميل بعض التقارير الخاصة (خاصة إذا كانت تشير إلى معلومات حساسة).	محاولة إعداد بعض التقارير المصممة مسبقا.
إعداد تقارير موثوقة وفي الوقت الصحيح	يجب على التطبيق أن يخرج تقارير مصممة مسبقة (صكوك، وتصنيف التقارير قروض وشرائح ائتمانية، مثل استحقاق الدين، والحالة، ومصادر التمويل، ونمط التمويل، ونوع الرصيد الدائن للسند، والشروط، والفواتير غير المدفوعة...الخ.	محاولة إعداد هذه التقارير.

إعداد تقارير موثوقة وفي الوقت الصحيح	يجب على التطبيق أن يخرج بعض التقارير بشكل مناسب مع ضمان شمولية وسلامة المعلومات.	التحقق من أن تتوافق مع شروط الاستخدام. التحقق من أن التقارير تعرض أرقام الصفحات وتتحقق من حواصل الجمع. يجب أن يطبق هذا الاختبار على التقارير التالية: تقرير استحقاق الدّين اللحين التعاقدي) وتقرير الرصيد المستحق، وتقرير الاستلام... الخ)
	يجب أن يسمح التطبيق بإعداد التقارير سواء منها الشاملة (جميع ديون سندات الضمان) أو الخاصة مثل: • بناء على حالة سندات الضمان الصادرة، الملغاة، المستردة...الخ) • بناء على الأحداث الجارية ضمن نطاق زمني محدد (إصدارات، استردادات... الخ). • بناء على الأصول قصيرة الأمد وطويلة الأمد. • بناء على وضع المحفظة. • بناء على نوع سند الضمان. • بناء على فاصل استحقاق السند. الخ.	محاولة توليد التقارير الشاملة والخاصة باستخدام البيانات التالية كمعيار: • حالة سندات الضمان (الصادرة، الملغاة، المستردة... الخ) • بناء على الأحداث الجارية ضمن نطاق زمني محدد إصدارات، استردادات... الخ) • بناء على الأصول قصيرة الأمد وطويلة الأمد. • بناء على وضع المحفظة. • بناء على نوع سند الضمان • بناء على فاصل استحقاق السند...الخ.

إعداد تقارير موثوقة وفي الوقت الصحيح	يجب أن تقدم التقارير معلومات كاملة وصحيحة.	توليد التقارير وإعادة إجراء الحسابات. يجب تطبيق هذا الاختبار على التقارير التالية: تقرير استحقاق الدين للدين التعاقدي والمستدل)، تقرير الرصيد القائم، تقرير الاستلام.. الخ).
	يجب أن تظهر التقارير نفس المعلومات الموجودة في التطبيق.	مقارنة التقارير من حيث تطابقها مع المعلومات المعروضة على شاشات التطبيق. يجب تطبيق هذا الاختبار على التقارير التالية: تقرير استحقاق الدين للحين التعاقدي والمستدل) وتقرير الرصيد القائم، وتقرير الاستلام... الخ.
	يجب أن تتطابق القيم المعروضة في تقرير استحقاق الدين وتقرير الرصيد القائم وتقرير الأصول.	مقارنة التقارير للتأكد من اتساقها.
	يجب أن يكون النظام قادرة على إعداد التقارير عن مجموع الديون على أساس فردي وكلي مع توقع خدمة الدين على القروض وسندات الضمان الحالية والمستقبلية.	محاولة إعداد مثل هذه التقارير. التحقق من أن التقارير تغطي عمليات الدين الموجودة والمتوقعة.
	يجب أن يولد التطبيق بشكل آلي التقارير المالية اليومية على العقود النشطة". كما يجب أن يسمح بالتوليد البدوي للتقارير من أجل عقود محددة.	التحقق من وجود التقارير الآلية لجميع العقود النشطة ومحاولة توليد التقارير اليدوية لعقود محددة.

النقل الصحيح للبيانات	يجب أن يكون نقل البيانات بين التطبيقات و/أو مراحل المعالجة دقيقة وكاملا.	محاكاة نقل للبيانات بين التطبيقات والتحقق من دقة وشمولية البيانات.
الرسائل المفيدة عن المخرجات	عند الدخول إلى التطبيق، يجب أن يعرض رسالة تتضمن المعلومات التالية: • العقود المستحقة في الأيام الخمسة التالية. • العقود ذات الدفعات المتأخرة للأقساط. • العقود ذات الأقساط المدفوعة جزئيا. • العقود ذات تواريخ الصرف المتأخرة. • العقود التي يكون تاريخ الصرف النهائي لها بعد خمسة أيام، يجب أن يرسل التطبيق رسالة يومية حتى يتم الصرف، أو حتى إلغاء قيمة الصرف، أو تعديل الموعد النهائي.	الدخول إلى التطبيق والتحقق من عرضه لجميع هذه الرسائل.
	يجب أن يقوم التطبيق بالإبلاغ عن حالة عملية الحساب الجاري الحساب" أو "تم إكمال عملية الحساب".	طلب القيام بالحساب والتأكد من أن التطبيق يقوم بالإبلاغ عن حالة العملية.
	في نهاية توليد التقرير، يجب أن يقوم التطبيق بعرض رسالة للإبلاغ عن اكتمال توليد التقرير أو يقوم بعرض التقرير المطلوب.	طلب تقرير والتحقق من أن التطبيق يعرض رسالة تعلن إكمال العملية أو يعرض التقرير المطلوب.
	يجب أن يبلغ التطبيق عن حالة التقارير المعدة، مثل: "قيد التنفيذ" أو "تم التنفيذ".	إعداد تقرير والتحقق من أن التطبيق يبلغ عن حالة العملية.

الرسائل المفيدة عن المخرجات	في حال وجود أي تعديلات على نسب الفائدة، يجب أن يعرض التطبيق رسالة تنبيه.	تغيير نسب الفائدة والتأكد من وجود رسالة تنبيه.
	قبل معالجة إلغاء أو استرداد سند ما، يجب على التطبيق أن يعرض شاشة بمعلومات السند التي تم حذفها او استعادتها كي يستطيع المستخدم تأكيد العملية.	محاولة استعادة أو حذف سند والتأكد من أن التطبيق يعرض رسالة تنبيه، وأنه يطلب تأكيد العملية.

الشكل 1: تدقيقات الدين العام التي تقوم بها الأجهزة العليا للرقابة والمحاسبة: حالة البرازيل

التدقيق الذي أجرته المحكمة البرازيلية للرقابة والمحاسبة على نظام الدين المدمج *SID*حكومة البرازيل الفدرالية عام *2014*.

باعتبار أنه يتم اختبار نظام الدين المدمج DS إلى الدين المسند (الموق) المحلي، فقد اختار فريق التدقيق التركيز فقط على اختبار العمليات المتعلقة بإدارة الدين الخارجي (المورق والتعاقدي). كانت ملاحظات ونتائج التحقيقات كالتالي:

إستراتيجية نظام تقنية المعلومات والإدارة العامة

بحسب دليل التشغيل، ما أن ينتهي إعداد نظام الدين المدمج SIDبشكل كامل، فإنه سيوفر الوظائف التالية:

أ) عدد متنوع من الحسابات، مثل القيمة الاسمية المحدثة، سعر الوحدة، الأصول (للديون التعاقدية وديون السندات)، التخطيط المالي للعقود، استحقاق وتسعير العقود والصكوك.

ب) مجموعة متنوعة من عمليات البحث والتقارير لتسجيل البيانات ونتائج الحسابات.

ج) العمليات المالية مثل إصدار الصكوك وسداد العقود والاسترداد والتحويل وعمليات أخرى.

د) سجل المعلومات المستخدم إلى أقصى حد في وحدات الأعمال المختلفة.

أما فيما يتعلق بإستراتيجية نظام تقنية المعلومات والإدارة العامة فإن الملاحظات الرئيسة ونتائج التدقيق كانت كالتالي:

- ليس هناك برنامج تدريب على أكثر أنظمة إدارة الدين العام استخدامة، وهي أنظمة Seorfi ونظام الدين المدمج .SID
- ليس هناك تاريخ متوقع للتنفيذ الكامل لنظام الدين المدمج SID بما في ذلك الدين المورق المحلي.
- بعض العمليات الهامة مثل تفعيل العقود، والسداد، وإبطال السداد، وتغيير معدلات الفائدة، أو تغيير قيمة العقود، تعالج من قبل شخص واحد فقط ليس هناك حاجة للموافقة أو المشورة ثانية في النظام. تعتمد سلامة العمليات فقط على كفاية صاحب الصلاحيات، وهو الأمر الذي يثير قضية الفصل بين واجبات المسؤولين.
- وهناك مشكلة أخرى بخصوص الفصل بين الواجبات، وهي أنه بسبب نقص عدد العاملين على تطوير برنامج نظام الدين المدمج SID، فإن موظفي مكتب إدارة الدّين أنفسهم يعملون على تطوير البرنامج، بالإضافة إلى وظائفهم الاعتيادية.
- لقد اكتمل تقييم قابلية تعرض العمليات للمخاطر الملازمة لعمليات تقنية المعلومات، لكن تقييم الحد من هذه المخاطر لم يتم بعد.

ضوابط الأمن وبيئة العمل

بما يتعلق بضوابط الأمن وبيئة العمل، فإن الملاحظات الرئيسة ونتائج التحقيق كانت كالتالي:

- لم يقم مكتب إدارة الدين بتعيين مدير الأمن المعلومات والاتصالات، كما أن لجنة أمن المعلومات المسؤولة عن تعيين مدير أمن المعلومات IS لم تبدأ بالعمل بشكل فعال بعد.
- لم يتم الانتهاء من إعداد تخطيط استمرارية الأعمال (BCP)، بينما يتم حالية مراجعة إجراءات العمل في إدارة الدين العام للتحضير لذلك التخطيط.

- لوحظ من نتائج تحليلات فريق التدقيق وجود ثلاث حسابات نشطة لمستخدمين غير محددين، مما يضر بممارسات تقنية المعلومات الجيدة، خاصة البند ISO/IEC- 11.2.1 227002: 2005 الذي ينصح بتحديد شخصية المستخدمين لضمان مسؤولية كل مستخدم للنظام عن تصرفاته.

- على الرغم من أنه يجب تحديد الدخول إلى نظام الدين المدمج SID من خلال الشهادة الرقمية A3 فقط، وعلى الرغم من أن إمكانية الدخول باستخدام رقم التعريف الوطني وكلمة السر هي إجراء استثنائي، فإن تحليل قاعدة البيانات لمستخدمي نظام الدين المدمج SIDيشير إلى عدم تحديد موعد نهائي للتوقف عن استخدام لذلك الإجراء الاستثنائي.

- يشير تحليل قاعدة بيانات مستخدمي نظام الدين المدمج SID إلى إخفاق عملية مراجعة دخول المستخدمين إلى النظام.

- اكتشف فريق التدقيق أيضاً وجود إخفاقات في الصيانة اليومية الروتينية الآلية لقاعدة بيانات مستخدمي نظام الدين المدمج SID.

- لا يقوم نظام الدين المدمج SID بتدوين سجل يتتبع تدقيق معظم عملياته، ونتيجة لذلك لا يقوم مكتب إدارة الدين بمراجعة دورية لنتائج التحقيق التي يولدها النظام، كما أنه لا يراقب العمليات في نظام الدين المدمج .SID

- لا يتمتع نظام الدين المدمج SID بوظيفة تدقيق لإنشاء وتخزين وتحليل سجل النظام بشكل روتيني.

- لاحظ فريق التدقيق عدم وجود خطة الاختبارات وبالتالي نتائجها المرتبطة بمعظم الأنظمة المستخدمة من قبل مكتب إدارة الدين ونظام Seorfi ونظام الدين المدمج SID.

- لم يتلق فريق التدقيق تأكيدا على الإنشاء الفعلي لفريق عمل يتحمل مسؤولية الاستجابة للأحداث الواقعة في شبكات الحاسوب، بحيث يتمتع بمسؤولية استلام ومراجعة والرد على الإشعارات المتعلقة بالحوادث الأمنية في نشاطات شبكات الحاسوب.

- لاحظ فريق التدقيق عدم وجود خطة لاستمرارية خدمات تقنية المعلومات، والتي تعتبر وثيقة رسمية تصف، بصورة مركزية، مبادرات ضمان استمرارية جميع خدمات تقنية المعلومات التي تديرها الوكالة أو الوحدة.

الضوابط التشغيلية والتوثيق

فيما يتعلق بالضوابط التشغيلية والتوثيق، كانت الملاحظات الرئيسة ونتائج التدقيق كالتالي:

- واجهة التواصل ليست ودودة، لذلك فإن نظام الدين المدمج SID يتطلب وجود معرفة سابقة كبيرة لدى المستخدم عن النظام.
- ليس هناك دليل لمستخدمي نظام الدين المدمج . SID
- إن سرعة معالجة الحسابات المطلوبة متدنية، مما يمنع إعداد الحسابات والتقارير بشكل متزامن. وبما أنه يوجد عدة مستخدمين للنظام في نفس الوقت، فيمكن أن تضعف هذه القضية كفاءة النظام. اقترح فريق التدقيق على مكتب إدارة الدين ضرورة النظر في إجراء تحسينات لزيادة طاقة المعالجة لدى النظام.

ضوابط التطبيق

بعد أن قام فريق التدقيق بإنجاز اختبارات ضوابط المدخلات والمعالجة والمخرجات على نظام الدين المدمج SID على الدين العام الخارجي، كانت نتائج التدقيق والملاحظات كالتالي:

- العديد من رسائل الخطأ غير واضحة وفي بعض الأحيان لا تظهر للمستخدم.
- خلال اختبارات ضوابط تطبيق المدخلات، وجد فريق التدقيق العديد من رسائل الخطأ التي لم تشرح سبب الخطأ.
- خلال اختبارات ضوابط تطبيق المعالجة في الدين التعاقدي الخارجي، وجد اختلاف في قيم التقرير المالي للتدفق النقدي بسبب عملية إبطال لم تؤخذ بعين الاعتبار عند إصدار ذلك التقرير بالذات.
- إذا كانت مدخلات البيانات غير صحيحة خلال اختبارات ضوابط تطبيق المخرجات، فإن التطبيق لا يقوم بإنشاء بعض تقارير الدين التعاقدية كما هو متوقع، لكن التطبيق لا يحدد للمستخدم ماهية الخطأ.

- خلال اختبارات ضوابط تطبيق المخرجات، تم تحديد الأخطاء في تقارير الدين التعاقدي بسبب استخدام النظام لمؤشرات قديمة.
- تم إصدار بعض تقارير الدين التعاقدية بمعلومات غير كاملة.

توصيات

مع أخذ نتائج التدقيق والملاحظات المسجلة بعين الاعتبار، قدم فريق التدقيق إلى أمانة الخزينة الوطنية بعض التوصيات لتطوير خطة عمل في تسعين يوما، تتضمن الجدول الزمني لتنفيذ التالي:

- وضع تاريخ متوقع للتنفيذ الكامل لنظام الدين المدمج SID تتضمن الدين المورق المحلي.
- تعيين مدير أمن المعلومات والاتصالات ولجنة أمن المعلومات.
- تشكيل خطة لاستمرارية الأعمال.
- تشكيل خطة لاستمرارية نشاطات تقنية المعلومات.
- تشكيل فريق لمعالجة الاستجابة للحوادث في شبكات الحاسوب.
- إنجاز التقييم والحد من المخاطر التشغيلية الخاصة بتقنية المعلومات.
- مراجعة الصيانة اليومية الروتينية لقاعدة بيانات مستخدمي نظام الدين المدمج SID فحص عملية مراجعة دخول مستخدمي نظام الدين المدمج SID.
- مراجعة عملية السماح بوجود حسابات مستخدمين غير محددين genericusers لنظام الدين المدمج SID.
- تحديد إجراءات للقيام بمراجعة الدورية لسجلات تتبع التدقيق التي يولدها نظام الدّين المدمج SID.
- أن يوفر نظام الدين المدمج SID عملية حفظ لسجل التطبيق.
- مراجعة رسائل الخطة التي يولدها نظام الدين المدمج. SID
- تطوير دليل مستخدمي نظام الدين المدمج SID.
- مراجعة منهج إصدار التقارير الخاصة بنظام الدين المدمج SID.

الشكل 2: تدقيقات الدين العام التي تقوم بها الأجهزة العليا للرقابة والمحاسبة: حالة مولدوفا

تقييم ضوابط التطبيق الذي أجرته محكمة الحسابات في جمهورية مولدوفا.

يتضمن تطبيق نظام إدارة الدين والتحليل المالي DMFASضوابط مدمجة كافية، والتي تقوم بالتحقق آلية من إدخال البيانات بشكل دقيق ليتم التصديق عليها، إلا أن هناك بعض المظاهر التي تدعو للقلق ويجب إزالتها: يملك المشغلون إمكانية إدخال البيانات في مصنفات النظام وفي جداول النظام الأخرى مما قد يؤثر على دقة البيانات وسلامتها من خلال تكرار التسجيلات أو حذفها:

التوصية رقم 15: النظر في إمكانية تقييد حق المشغلين في إدخال وتغيير وحذف البيانات في مصنف قاعدة البيانات لنظام إدارة الدين والتحليل المالي DMFAS، أو إضافة إمكانية التعرف على أمثال هذه العمليات لتجنب تكرار البيانات أو إدخالها بصورة خاطئة.

بالإضافة إلى التقارير المعيارية الموجودة في تطبيق نظام إدارة الدين والتحليل الماليDMFAS، تم تطوير عدد كبير من التقارير ذات صفة عامة في تطبيق "إكسل"، وتتضمن معظم الجوانب المطلوبة. ليست كل أنواع التقارير مستخدمة بانتظام. ومعظم التقارير المطلوبة يتم إعدادها باستخدام برنامج "إكسل".

إلا أن هناك تقارير معينة يتم توليدها بشكل يدوي من البيانات التي تؤخذ من تقارير أخرى. ما يثير القلق هو كيفية تجديد البيانات في تقارير "إكسل". إن إعداد التقارير هو إجراء معقد جدة يمكن أن يتأثر بشكل شديد بسبب العامل البشري. كما أن التقارير المعدة يمكن تعديلها دون إذن، وقد تحصل هذه الأخطاء في تقارير ملخصة هامة والتي يجب أن تتمتع بأعلى مستوى أمني وتمثل النتيجة الرئيسة النشاط قسم الدين العام. ونتيجة لذلك، فإن بعض العيوب الصغيرة يمكن أن تؤثر بشكل حساس على مصداقية ودقة البيانات في تقارير هامة متعلقة بنشاط قسم الدين العام.

التوصية رقم 16: النظر في إمكانية تحسين أو أتمتة عملية تعديل التقارير التي يتم توليدها. وتحديد إمكانية إعداد تقارير الملخصات بشكل آلي وبدون اللجوء إلى العامل البشري. كما يمكن انتهاز الفرصة للتفكير في إمكانية الانتقال إلى النسخة 6.0.

المصادر والمراجع

.ASOSAI Research Project. IT Audit Guidelines - 6th, September 2003

Gallegos, Frederick. Senft, Sandra. Manson, Daniel P. Gonzales, Carol. Information .Technology Control and Audit. Auerbach. USA 2004

India Office of the Comptroller and Auditor General. Information Technology Audit – .(General Principles (IT Audit Monograph Series # 1

International Monetary Fund and the Word Bank. Guidelines for Public Debt Management. April 1, 2014

International Organization of Supreme Audit Institution. ISSAI 300 Performance .Audit Principles. September 2019

International Organization of Supreme Audit Institution. ISSAI 3000 Performance Audit Standard. September 2019

INTOSAI Development Initiative. WGITA, IDI Handbook on IT Audit for Supreme .Audit Institutions. February 2014

.Parker, Xenia Ley. Information Technology Audits. CCH Incorporated. USA 2006

.United States Department of Homeland Security web site: http://www.dhs.gov

United States Government Accountability Office. Federal Information System Controls .Audit Manual (FISCAM). GAO-09-232G. February 2009