GUID 5259

Systèmes d'information sur la dette publique

Les Normes internationales des institutions supérieures de contrôle des finances publiques (ISSAI) sont publiées par l'Organisation internationale des institutions supérieures de contrôle des finances publiques (INTOSAI). Pour plus de renseignements visitez le site www.issai.org

INTOSAI

Document pré-IFPP - ce document a été élaboré avant la création du Cadre des prises de position professionnelles de l'INTOSAI (IFPP) en 2016. Il peut être différent dans son objectif formel des lignes directrices d'audit de l'INTOSAI plus récentes

INTOSAI

INTOSAI, 2019

1) Approuvé comme ISSAI 5450 - Orientations sur l'audit des systèmes d'information sur la gestion de la dette publique en 2016

2) Avec la réalisation du Cadre de prises de position professionnelles de l´INTOSAI (IFPP), renommé en tant que GUID 5259 - Système d'information de la dette publique avec des changements d´édition en 2019.

GUID 5259 est disponible dans toutes les langues officielles de l´INTOSAI : Arabe, Anglais, Français, Allemand et Espagnol.

TABLE DE MATIÈRES

PRÉFACE 5

LISTE D'ABRÉVIATIONS 7

1. INTRODUCTION 8

1. PLANIFICATION 9

2. CONTRÔLES GÉNÉRAUX 13

Contrôles organisationnels 14

Contrôles d'accès physique 14

Contrôles d'accès logique 14

Contrôles environnementaux 15

Contrôles de modifications des programmes 15

Plans de continuité des activités et de reprise après sinistre 15

3. CONTRÔLES DES APPLICATIONS 16

3.1. Normes de Documentation 17

3.2. Contrôles D'entrée 18

Écrans de saisie de données 19

Routines de préparation des données 20

Autorisation de saisie de données 20

Rétention de Documents d'entrée 21

Validation des données d'entrée 21

Erreurs de saisie de données 22

Mécanismes d'appui à l'entrée de données 23

3.3. Contrôles de Traitement **23**

Intégralité 23

3.4. Contrôles de Sortie **25**

3.5. Tests des Contrôles des Applications **26**

3.6. Rapports des Résultats de L'audit **28**

ANNEXE I : Tableau de planification **29**

ANNEXE II: Matrice de test pour les contrôles généraux **34**

ANNEXE III : Matrice de tests pour les contrôles des applications **41**

FIGURE 1 : Audit de la dette publique par les ISC : Le cas du Brésil **62**

FIGURE 2 : Audit de la dette publique par les ISC : Le cas de la Moldavie **67**

BIBLIOGRAPHIE **69**

PRÉFACE

Lorsque nous parlons de la gestion des finances publiques, la dette publique est au centre du jeu. En cherchant à développer leurs économies et á améliorer les services publics, la plupart des gouvernements font face à des besoins financiers importants. Dans la théorie économique, la dette publique est un outil efficace pour la croissance économique et pour distribuer équitablement la charge fiscale entre les générations actuelles et futures de contribuables. En raison de son importance pour l'équilibre économique, il est essentiel de mesurer et gérer la dette publique attentivement.

L'objectif principal de gestion de la dette est d'obtenir un financement stable, au coût le plus bas possible et à des niveaux prudentiels de risque, afin de soutenir l'activité du gouvernement. Les Directives pour la gestion de la dette publique du Fonds monétaire international (FMI) - Banque mondiale fournissent un ensemble desbonnes pratiques de contrôles interne pour la gestion de la dette. Parmi celles-ci, se trouve le principe suivant: «La gestion de la dette doit s'appuyer sur un système informatique de gestion précis et complet, muni des dispositifs de sécurité requis.». Les pays qui souhaitent mettre en place une gestion efficace de la dette publique doivent accorder un haut degré de priorité au développement de systèmes fiables pour l'enregistrement et la communication des informations concernant la dette. Ceci est nécessaire non seulement pour développer les données sur la dette et assurer le paiement en temps utile du service de la dette, mais aussi pour améliorer la qualité des rapports budgétaires et la transparence des comptes publics, ce qui permettra aux décideurs et aux gestionnaires d'atteindre les objectifs de la dette publique.

Comme nous pouvons le constater, l'audit des systèmes d'information de gestion

de la dette publique vise à accroître l'efficience, l'efficacité et la performance de la gestion de la dette publique. Pour cette raison, il doit être classé comme un audit de performance. Néanmoins, ce travail peut également être d'une grande utilité dans le cadre des vérifications financières, dont l'objectif estde déterminer si l'information financière présentée au gouvernement est conforme au cadre de réglementation applicable à la présentation de rapports financiers et si l'information est fiable et exempte de fraudes ou d'erreurs. Dans ce contexte, ce travail acquiert une grande importance, car il contribue à réaliser un système d'information qui rassemble et produit des informations précises et fiables sur l'une des plus importantes données financièrespubliques : la dette publique.

Le but de ce GUID est de fournir aux auditeurs des lignes directrices descriptives sur l'audit des systèmes d'information de gestion de la dette publique. Étant donné que l'Organisation internationale des institutions supérieures de contrôle des finances publiques (INTOSAI) dispose déjà de quelques documents relatifs aux audits de Technologies de l'information (TI), développés par le Groupe de travail sur l'audit informatique (WGITA), ce GUID porte sur le contrôle des applications, qui doit être spécifique aux systèmes d' information de gestion de la dette publique.

LISTE D'ABRÉVIATIONS

BCP – Plan de continuité des opérations

CAAT – Techniques de vérification informatisée

CNUCED – Conférence des Nations Unies sur le commerce et le développement

CS-DRMS – Système de comptabilisation et de gestion de la dette du Secrétariat du Commonwealth

DMO – Service de gestion de la dette

DRP – Plan anti sinistre

FMI – Fonds monétaire international

FMIS – Système d'information sur la gestion financière

INTOSAI – Organisation internationale des institutions supérieures de contrôle des finances publiques

ISC – Institution supérieure de contrôle

MF – Ministère des finances

PDMIS – Système d'information de gestion de la dette publique

SYGADE – Système de gestion et d'analyse de la dette

TI – Technologies de l'information

WGITA – Groupe de travail sur l'audit informatique

WGPD – Groupe de travail sur la dette publique

INTRODUCTION

Conformément aux directives fixées par le Conseil d'administration de l'INTOSAI, le Groupe de travail sur la dette publique (WGPD) a été chargé de publier des lignes directrices et autres documents d'information destinés à être utilisés par les Institutions supérieures de contrôle (ISC) pour promouvoir le suivi correct et la bonne gestion de la dette publique.

Ce GUID doit permettre d'accroître la capacité d'action du WGPD en fournissant un cadre général qui puisse être utilisé, lors des vérifications des ISC, pour évaluer les contrôles généraux et ceux des applications du Système d'information de gestion de la dette publique (PDMIS). Il est important de considérer que, dans les références, le PDMIS comprend un ou plusieurs systèmes d'information utilisés dans la gestion de la dette publique.

Avec l'avancée des technologies de l'information, les organismes gouvernementaux sont devenus de plus en plus tributaires de leur utilisation pour effectuer leurs opérations et fournitures de services et pour traiter, entretenir et communiquer les informations essentielles. Selon un document de travail du FMI, « un FMIS (système d'Information de la gestion financière) désigne généralement l'informatisation des processus de gestion des dépenses publiques y compris la définition du budget, son exécution et sa comptabilité, à l'aide d'un système entièrement intégré de gestion financière des ministères sectoriels et autres organismes gérant des fonds publics.»

L'Institut des ingénieurs électriciens et électroniciens (IEEE 1471) définit les systèmes comme « un ensemble de composants organisés pour accomplir une fonction spécifique ou un ensemble de fonctions.» En particulier, la principale activité d'un système dans un service de gestion de la dette est de maintenir

la base de données des emprunts publics à l'aide d'un logiciel qui permette à la fois d'enregistrer et d'exercer les fonctions analytiques du Service de gestion de la dette (DMO).

Un audit informatique peut être classé, par approches prédominantes, comme suit :

» Gouvernance des TI

» Audit des données

» Audit des systèmes d'information Passation de contrats de TI, et

» Sécurité de l'information.

En général, un auditeur TI travaille avec plusieurs approches, cependant il peut choisir une approche prédominante. Dans ce guide, l'approche prédominante est l'*audit de systèmes d'informations.*

Ce GUID est structuré en plusieurs parties : planification, évaluation des contrôles généraux et évaluation des contrôles des applications.

1. PLANIFICATION

Le Système d'information de gestion de la dette publique peut être considéré comme un ensemble de parties interdépendantes (structures physiques, personnel, outils informatiques) qui interagissent afin d'enregistrer, de contrôler, d'évaluer et de gérer les transactions qui sont générées par la levée, l'entretien et le règlement de la dette publique.

Cette phase permet à l'auditeur d'acquérir une compréhension des opérations, contrôles et risques liés au système, compte tenu des risques inhérents aux flux opérationssur la dette publique. Sur cette base, le vérificateur évalue l'environnement de contrôle global, identifie les systèmes utilisés dans la gestion de la dette publique, examine l'ensemble de la documentation sur ces systèmes et procède à une évaluation préliminaire des risques. Le résultat de cetteévaluation guidera l'étendue des procédures à employer dans la phase de tests.

L'ISC doit aussi procéder à un examen de toutes les structures liées au Service de la dette publique, telles que le personnel, les processus, les type de dettes, la sécurité des données, les outils informatiques,entre autres.

Dans cette phase, le vérificateur doit réaliser une évaluation préliminaire de la structure du Bureau de la dette publique et des flux d'opérations de la Dette publique, couvrant les questions suivantes :

» le fonctionnement de l'audit interne;

» les résultats des audits précédents (internes ou externes) sur le Système d'information de gestion de la dette publique;

» le stockage physique des documents liés aux opérations;

» l'utilisation de matériel informatique, de logiciels et la responsabilité de leur maintenance ;

» les opérations traitées par les systèmes d'information et leur importance relative;

» comment a lieu la relation entre les divers composants d'informations de la dette publique;

» les méthodes et procédures prévues pour la mise en œuvre des nouvelles opérations ou larévision des opérations existantes;

» les évaluations précédente du contrôle interne du DMO.Si le contrôle interne du DMO n'a pas été précédemment évalué, l'ISC devray procéder. Cette procédure est très importante pour évaluer le degré de risque existant et delà, déterminer les tests 'd'audit à conduire.

Le niveau de sophistication du système n'influe pas sur l'évaluation des contrôles généraux, qui doit toujours être réalisée. Cependant, il détermine les procédures d'audit à effectuer et le nombre d'experts en TI nécessaires pour effectuer le travail d'audit. Il est suggéré d'avoir au moins un expert en informatique dans l'équipe pour tous les travaux impliquant les systèmes. Pour les auditeurs de l'équipe qui débutent dans les audits informatiques, il est important d'acquérir des connaissances sur la

terminologie usuelle. Dans ce cas, un bon dictionnaire technique d'informatique est un bon investissement pour l'ISC. Le document Audits des systèmes d'information– Glossaire des termes, par le groupe de travail de l'INTOSAI sur l'audit informatique, est très utile dans ce cadre. Certains glossaires web peuvent être très utiles : http://www.webopedia.com ou http://whatis.techtarget.com.

Les auditeurs qui sont déjà familiarisés avec les expressions informatiques doivent connaître la terminologie utilisée dans le DMO, surtout les sigles et abréviations (types de rubriques, secteurs du DMO, créanciers, nom des systèmes, logiciel utilisé par le DMO, etc.) Il est indispensable d'avoir ces connaissances avant de procéder à des entretiens. Un glossaire très utile, mis au point par la Conférence des Nations Unies sur le commerce et le développement (CNUCED) peut être trouvé sur les liens suivants:

» http://UNCTAD.org/en/docs/pogiddmfasm3r3.en.pdf – Debt and DMFAS Glossary (version anglaise)

» http://unctad.org/fr/docs/pogiddmfasm3r3.fr.pdf – Glossaire de la dette et du SYGADE (version française)

Comprendre en détail un système d'Information de gestion de la dette publique signifie de connaître les données inhérentes et les flux des informations. Ainsi, il est très important, à l'étape de planification, de dresser une cartographie des processus-clés de la dette publique (enregistrement, traitement, contrôle, sécurité, reportinget analyse) et de comprendre comment ces processus sont effectués par le système d'information. Après cela, il est nécessaire d'effectuer une analyse de risque afin d'identifier les risques les plus élevés associés aux processus-clés relatifs aux opérations et àla gestion de la dette publique, compte tenu de leur impact et leur probabilité d'occurrence. L'évaluation des risques joue un rôle important pour déterminer le champ des procédures nécessaires pour gérer les niveaux de risque associés. L'ancienne ISSAI 5410 *Orientations pour la planification et la conduite d'un audit de contrôles internes sur la dette publique*[1] fournit des lignes directrices pour effectuer cette évaluation des risques. En outre, l'évaluation des risques pourrait être placée dans le cadre des audits financiers.

Les flux du PDMIS sont presque toujours fixéspar le Service de gestion de la dette

1 Cette prises de position a été retirée du cadre en septembre 2019

(DMO). D'autres services peuvent également être responsables de la saisie des données de la dette, par exemple, dans le cas de la dette contractuelle. Lorsque le DMO est divisé en Back, Middle et FrontOffice, chaque fonction a ses propres flux de données et d'informations. Le FrontOffice est généralement responsable de l'exécution des opérations sur les marchés financiers, y compris de la gestion des enchères et des autres formes d'emprunts, ainsi que de toutes autres opérations de financement. Le BackOffice gère le règlement des opérations et la maintenance des données financières. Un MiddleOffice indépendant, ou gestionnaire des risques, effectue généralement l'analyse des risques, surveille et signale les risques liés au portefeuille et évalue la performance des gestionnaires de la dette par rapport aux cibles stratégiques. La majorité des flux de données associés à la dette publique, y compris les données externes, sont logés dans le BackOffice, chargé de contrôler et d'enregistrer la saisie de données.

Étant donné que beaucoup de pays utilisent un logiciel commercial développé et mis à jour par des organisations internationales tierces pour la gestion de la dette publique (p. ex. SYGADE, CS-DRMS), l'utilisation de rapports relatifs à la performance, tels qu'avènement d'évolutions, demandes de maintenance du système et dossiers d'incidents, est très importante.

Le Programme SYGADE, mis au point par la Conférence des Nations Unies sur le commerce et le développement (CNUCED), se concentre sur les activités « aval». Il s'agit de maintenance des bases de données de la dette, validation de données de la dette, *reporting* interne et externe sur la dette, statistiques de la dette et analyse de base de la dette, et d'établir des liens entre le système de gestion de la dette et d'autres logiciels financiers. Elles complètent d'autres activités plus « en amont » telles que l'analyse de soutenabilité de la dette proposée par d'autres fournisseurs tels que la Banque mondiale. En outre, le Programme aide de plus en plus les pays à établir des liens entre le système SYGADE pour la gestion de la dette et d'autres logiciels gouvernementaux (qui sont utilisés, par exemple, pour l'établissement du budget, la gestion de trésorerie, la gestion de l'aide au développement) ou au sein de systèmes complexes intégrés de gestion financière, dans le cadre de l'ensemble des efforts de gestion des finances publiques du pays. Pour plus d'informations, accéder à http://unctad.org/dmfas.

L'application CS-DRMS, fournie par le Secrétariat du Commonwealth, permet d'enregistrer, gérer et analyser la dette dans une perspective holistique. Elle fournit

un référentiel central pour plusieurs catégories de dette sécurisée publique et privée, extérieure et intérieure, y compris la dette à court terme. Le système gère également les subventions, les prêts du gouvernement et la rétrocession. Pour plus d'informations accéder à http://www.csdrms.org.

Dans le cas de pays qui utilisent le SYGADE ou le CS-DRMS pour la gestion de la dette publique, les rapports d'audit du PDMIS réalisés par d'autres pays (ISC) pourraient être d'une grande utilité pour l'identification des lacunes qui sont les plus fréquentes et/ou ont le plus d'impact.

Un tableau sur les informations requises, les procédures et les questions auxquelles doit répondre l'ISC et qui peut être utilisé par l'équipe de vérification au cours de la phase de planification, est joint à l'annexeI.

2. CONTRÔLES GÉNÉRAUX

Les contrôles généraux constituent le cadre de contrôles d'ensemble pour les fonctions informatiques1. Ces contrôles sont conçus pour résoudre les problèmes dans le développement, les opérations et l'entretien de l'environnement. Les objectifs des contrôles généraux sont de sauvegarder les données, protéger les programmes desapplications et assurer la continuité des opérations informatiques en cas d'interruptions imprévues.

Bien qu'un audit du système de la dette publique exige la vérification des contrôles généraux, le présent document n'entend pas épuiser cette question, étant donné qu'il existe des documents, préparés par l'INTOSAI, sur l'audit informatique, qui traitent des contrôles généraux en détail.

Il est suggéré, lors de l'audit d'un système, l'équipe d'audit prenne en compte le contenu de l'ancienne ISSAI 5310[2] : *Directives concernant les contrôles de sécurité des systèmes d'informations* (ISec), un guide pour l'examen de la sécurité des systèmes d'information (SSI) dans les organisations gouvernementales.

Un autre document pouvant s'avérer utile pour la planification des contrôles généraux est WGITA - IDI Manuel d'audit informatique pour les Institutions

2 Cette prises de position a été retirée du cadre en septembre 2019. Le nouveau prononcé GUID 5110 GUID relatif à l'audit de la sécurité des systèmes d'information peut être renvoyé.

supérieures, qui fournit aux utilisateurs les informations essentielles et les questions-clés utiles pour une planification efficace des audits informatiques.

À l'annexe II est présentée une matrice de tests avec quelques contrôles généraux et suggestions de procédures qui peut aider l'auditeur à tester les contrôles généraux.

L'ensemble complet des différentes catégories de contrôles généraux comprend les éléments décrits ci-dessous :

» CONTRÔLES ORGANISATIONNELS

Les contrôles organisationnels sont les politiques, les procédures et le cadre organisationnel établis pour garantir des politiques de ressources humaines et des pratiques de management saines, la séparation des fonctions, les stratégies de sécurité d'information, mises en œuvre afin de fournir des méthodes pour évaluer l'efficacité et assurer l'efficience des contrôles opérationnels.

» CONTRÔLES D'ACCÈS PHYSIQUE

Les contrôles d'accès physique comprennent les règles et pratiques pour empêcher l'accès non autorisé, et les interférences avec les services informatiques, y compris des procédures administratives comme les badges d'identité pour le personnel, le contrôle des visiteurs, les mesures physiques telles que les serrures à clé mécaniques et les serrures électroniques, les caméras et les autres moyens de limiter l'accès physique aux serveurs et aux autres infrastructures essentielles.

» CONTRÔLES D'ACCÈS LOGIQUE

Les contrôles d'accès logique utilisent la sécurité intégrée aux systèmes informatiques pour empêcher tout accès non autorisé aux données et aux fichiers sensibles et pour s'assurer que tous les utilisateurs disposent de droits d'accès limités aux besoins de leurs fonctions. Ceci comprend des pare-feux, antivirus, logiciels de détection d'intrusions et de programmes malveillants.

Dans les systèmes modernes, ces contrôles sont obtenus de manières diverses

et variées. Ils sont mis en œuvre par le biais de logiciels d'application, système d'exploitation, système de gestion de base de données, logiciel de contrôle d'accès, moniteurs de traitement transactionnel en ligne (OLTP), serveurs, réseau, LAN et éventuellement d'autres logiciels.[3]

» CONTRÔLES ENVIRONNEMENTAUX

Les contrôles environnementaux sont les règles, les pratiques et les conditions établies pour éviter tout dommage causé par l'instabilité électrique, l'incendie, la poussière, l'eau, la nourriture, les températures extrêmes ou l'humidité, et l'électricité statique.

Bien que l'objectif de ces contrôles soit le datacenter (centre de traitement de données) ou l(espace dédié à l'équipement informatique, qui exige un milieu spécifique ou du moins la protection contre le vol, ils s'appliquent également à tous les environnements de bureau.

» CONTRÔLES DE MODIFICATIONS DES PROGRAMMES

Les contrôles de modifications des programmes sont les règles visant à garantir que toutes les modifications apportées à la configuration du système sont gérées correctement, entièrement et en temps utile.

Les mises à niveau et les modifications devraient être dotées d'un processus officiel pour assurer la journalisation de tous les changements et pour permettre la possibilité de faire marche arrière si des problèmes apparaissent avec la nouvelle version.

Une validation officielle devrait être requise avant que des programmes ne soient transférés du test à la production, et toute la documentation liée au système, opérations et programmes doit être complète, tenue à jour et dans le respect des normes, politiques et procédures.

» PLANS DE CONTINUITÉ DES ACTIVITÉS ET DE REPRISE APRÈS SINISTRE

Le plan de continuité des activités (BCP) et le plan anti sinistre (DRP) connexe visent à

3 Audits des Technologiques de l'information, Xenia Ley Parker

assurer la disponibilité. Les plans de contingence et de récupération après sinistre, la viabilité des plans, les tests, le monitorage et la nécessité d'une mise à jour continue des plans sont des facteurs cruciaux.[4]

Le BCP est une approche globale définissant des voies alternatives pour le maintien des processus opérationnels critiques en cas d'urgence, de catastrophe ou autre

perturbation. L'accent est mis sur la survie de l'entreprise dans son ensemble et non seulement sur les TI. Toutefois, le plan global doit tenir compte des exigences en matière de systèmes d'information et de réseaux de télécommunications. Cette partie du BCP est un DRP.

Les plans BCP et les DRP connexes peuvent être établis en même temps, afin de considérer simultanément tous les aspects. Au minimum, le plan doit comprendre des procédures et des critères pour déterminer quand une situation est une sinistre, la personne responsable de le déterminer ;et comment déclarer un événement comme étant officiellement un sinistre et lancer la mise en œuvre du plan en.

3. CONTRÔLES DES APPLICATIONS

Les contrôles des applications sont automatisés dans les applications du système d'information afin de contribuer à garantir l'autorisation, l'intégrité, l'exactitude et la validité des transactions. Ils sont intégrés dans la programmation de l'application et sont fréquents dans les opérations d'entrée, de traitement et de sortie de l'application. Leur objectif est de garantir l'intégralité, la fiabilité et l'exactitude du traitement des données.

Exemples de contrôles des applications: contrôles effectués par l'application sur le format des données saisies afin d'éviter des données non valides, contrôles de traitement qui empêchent les utilisateurs de comptabiliser des transactions non autorisées, création de rapports détaillés et de contrôles sur la totalité des transactions pour s'assurer que ces dernières soient enregistrées de façon complète et exacte.

Les contrôles des applications peuvent être classés comme suit :

4 Audits des Technologiques de l'information, Xenia Ley Parker

» Entrée,

» Traitement,

» sortie.

3.1. NORMES DE DOCUMENTATION

Les normes de documentation assurent le maintien adéquat et à jour de la documentation des applications. La mise à jour soignée de la documentation est importante.[5]

Une documentation adéquate est importante pour améliorer la compréhension des contrôles qui sont, ou devraient être, mis en place.

Une bonne documentation des applications réduit également le risque que les utilisateurs ne suivent pas les procédures de contrôleprévues par la direction. L'examen d'une documentation complète et à jour aide l'auditeur à comprendre le fonctionnement de chaque application et peut aider à identifier certains risques d'audit particuliers.

» Documentation des applications : aide les programmeurs de maintenance à comprendre l'application, corriger les problèmes et apporter des améliorations. La documentation augmente à chaque phase du processus de développement et peut être élaborée sous différents formats : organigrammes, graphiques, tableaux ou texte. La documentation peut inclure des détails sur les éléments suivants : source des données, attributs de données, écrans de saisie, validations de données, procédures de sécurité, description des calculs, conception du programme, interfaces avec d'autres applications, procédures de contrôle, gestion d'erreurs, instructions d'exploitation, archives, sauvegarde, stockage et procédures de récupération. La documentation de l'application doit être mise à jour au fur et à mesure que l'application est modifiée.

5 Audit Informatique – Principes généraux (Audit Informatique Séries Monographiques # 1) – Bureau du Contrôleur et Vérificateur General des comptes de l'Inde

» La documentation de l'utilisateur doit inclure les descriptions des processus automatisés et manuels afin d'aider à la formation de départ sur l'application et comme référence pour la suite. Dans les deux cas, la documentation de l'utilisateur doit être mise à jour au fur et a mesure que l'application est modifiée.

La documentation doit inclure les éléments suivants :

» un aperçu de l'application;

» la spécification des prérequis de l'utilisateur;

» la description et le listing des programmes;

» la description des entrées/sorties;

» la description du contenu des fichiers;

» les manuels de l'utilisateur ;

» les instructions de bureau;

» la description des contrôles de sécurité des applications;

» un résumé récent des évaluations de sécurité ;

» les décisions récentessur la sécurité et actions recommandées ; et

» la situation de mise en œuvre des actions recommandées.

3.2. CONTRÔLES D'ENTRÉE

Les contrôles d'entrée sont extrêmement importants pour réduire le risque d'erreur ou de fraude dans les applications informatiques. Les contrôles d'entrée sont essentiels à l'intégrité des données.

Les contrôles d'entrée garantissent l'autorisation, la précision, l'intégralité et la ponctualité des données entrées dans une application. L'autorisation est assurée

en exigeant des approbations de deuxième niveau pour les transactions dépassant un seuil défini. La précision est assurée par les contrôles qui valident les données saisies avant d'accepter la transaction et d'engager le traitement. L'intégralité est assurée par le biais de procédures de gestion d'erreurs qui offrent la journalisation, le signalement et la correction des erreurs. La ponctualité est assurée par la surveillance du flux de transaction, la journalisation et le reporting des exceptions.

Les contrôles d'entrée peuvent se trouver dans:

- les écrans d'entrée de données;
- les routines de préparation de données;
- l'autorisation de données;
- la rétention des documents d'entrée;
- la validation des données;
- les procédures d'erreur dans la saisie de données ;
- les mécanismes d'appui à l'entrée de données.

Les contrôles susmentionnés peuvent être contournéss'il est possible de saisir ou de modifier les données en dehors de l'application. Il devrait y avoir des contrôles automatiques d'intégrité de l'application capables de détecter et de signaler toute modification externe des données. Par exemple, un contrôle devrait être en place pour détecter et signaler les modifications non autorisées effectuées sur la base de données de transactions sous-jacente.

» ÉCRANS DE SAISIE DE DONNÉES

Les écrans de saisie de données normalisés peuvent permettre d'assurer l'entrée de données cohérentes.

Le PDMIS peut inclure les fonctionnalités suivantes :

- les écrans de saisie sont structurés sous une forme et une disposition normalisées;

- les champs de saisie de données restreignent ce que les utilisateurs sont autorisés à saisir;
- entrée obligatoire pour certains champs;
- une fonction d'aide (par exemple F1) aide l'utilisateur à compléter les champs de données d'entrée.

ROUTINES DE PRÉPARATION DES DONNÉES

Les routines de préparation de données visent à éviter les défaillances au cours des procédures d'entrée des données.

Le PDMIS peut inclure les fonctionnalités suivantes :

- environnements intégrés pour procédures de partage de données et transferts vers d'autres applications.

AUTORISATION DE SAISIE DE DONNÉES

L'autorisation de saisie de données vise à garantir que toute saisie a été enregistrée et autorisée par la personne adaptée.

Le PDMIS peut inclure les fonctionnalités suivantes :

- Le PDMIS requiert un mot de passe d'accès;
- enregistrement de l'historique des accès lorsqu'il y a saisie manuelle de données ;
- obligation de deux approbations pour certaines opérations sensibles (par exemple activation de contrat, modification de taux d'intérêt, modification de valeurs de contrat).

» RÉTENTION DE DOCUMENTS D'ENTRÉE

Cette dimension des contrôles d'entrée de données se réfère à la maintenance et le contrôle des documents originaux qui accompagnent les enregistrements de données de la dette. Dans le cas de transferts de fichiers automatique entre les applications, le PDMIS doit conserver les données originales provenant d'une autre application,pendant une période prédéfinie par le DMO.

» VALIDATION DES DONNÉES D'ENTRÉE

Les contrôles de validation de données visent à assurer que les données d'entrée soient valides et exactes.

Le PDMIS peut inclure les fonctionnalités suivantes :

- listes de contrôles automatiques pour vérifier l'absence de valeurs (par exemple en téléchargeant une série historique d'indices, le PDMIS vérifie si une valeur quotidienne, mensuelle ou annuelle est manquante);
- tous les écrans de saisie de données identifient clairement les champs obligatoires et l'application permet la confirmation de l'opération uniquement si toutes les informations obligatoires ont été saisies;
- chaque table de base de données doit contenir une règle spécifique concernant les champs pour lesquels la duplication de données n'est pas autorisée;
- si l'application estime que des données dupliquées sont saisies, elle n'acceptera pas l'entrée jusqu'à ce que la duplication soit résolue;
- l'application ne permet pas la modification de certaines données après leur saisie (par exemple, taux de change à la date de l'opération). En ce qui concerne les autres données, l'application peut permettre la modification si certaines conditions sont remplies (par exemple lorsqu'un contrat est «bloqué» ou «terminé», aucune donnée ne peut être modifiée);
- certains champs, une fois qu'ils sont remplis, requièrent que d'autres champs le soient également (par exemple si l'utilisateur saisit la commission

d'engagement de contrat, l'utilisateur doit entrer également la taxe d'engagement);

» les champs de «date» sont essentiels pour le contrôle général d'un contrat de dette. Ils sont particulièrement utiles dans les calculs des versements, pour éviter les retards de paiements, pour appliquer des pénalités, etc... Ainsi, l'application doit comporter des règles de base pour les détails de saisie des champs de «date»;

» à l'exception des opérations simulées, l'application du système ne permet pas l'enregistrement de certaines données pour une date ultérieure, associée à des opérations réelles. Par exemple : décaissement, inversion de décaissement, annulation de contrat, addition de contrat.

» ERREURS DE SAISIE DE DONNÉES

Une piste d'audit ou journal d'audit est un registre, ensemble de registres ou d'enregistrements de destination et de source chronologiques,lié à la sécurité, qui fournissent les pièces justificatives de la séquence des activités qui ayant affecté à un

moment une opération, procédure ou événement spécifique. Les pistes d'audit ou les fichiers de journalisation doivent être restreints au personnel approprié.

Le PDMIS peut inclure les fonctionnalités suivantes :

» le DMO doit définir la responsabilité pour les dossiers en attente;

» des programmes pour la journalisation d'activité des erreurs, le reportingdes erreurs en suspens et la correction d'erreurs devraient être intégrées dans l'application;

» dans un processus de téléchargement automatique de données, lorsque l'application identifie des lacunes dans les séries, un e-mail automatique devrait être envoyé aux utilisateurs appropriés pour le suivi;

» l'application doit envoyer des rapports périodiques des erreurs non résolues et de leur vieillissement et leur donner la priorité auprès du personnel approprié.

» MÉCANISMES D'APPUI À L'ENTRÉE DE DONNÉES

Ces contrôles sont liés à l'appui des procédures du DMO qui aident les utilisateurs à saisir les données dans l'application informatique, à réinitialiser les applications et à surveiller les activités de l'utilisateur afin d'éviter toute déviation possible des règles établies.

Ces mécanismes sont souvent inclus dans les contrôles généraux.

3.3. CONTRÔLES DE TRAITEMENT

Les contrôles de traitement garantissent l'exactitude, l'intégralité et la ponctualité des données au cours de traitements par lots ou en ligne. Ces contrôles permettent d'assurer que les données soient traitées avec précision sur toute l'application et qu'aucune donnée ne soit ajoutée, perdue ou altérée au cours du traitement.[6]

» INTÉGRALITÉ

L'intégralité peut être assurée, dans le traitement par lots, en équilibrant les transactions reçues par un système avec les transactions transmises par un système subsidiaire.

L'équilibrage doit survenir entre les applications qui partagent des données communes, en créant un rapport de conciliation qui présente les données issues des deux applications et signale toute différence à un groupe d'utilisateurs.[7]

L'équilibrage doit inclure un décompte de transactions ainsi que les totaux pour tous les champs de montant, pour chaque type de transaction, et le croisement des totaux des champs de détail avec ceux des champs de totaux.[8]

Dans les fichiers qui n'ont aucun total significatif, les totaux de contrôle peuvent être créés en ajoutant tous les chiffres d'une colonne pour vérifier que le même total soit accepté par le processus suivant. Par exemple, totaliser les numéros d'accord de

6 Contrôle et Audit Informatique – Deuxième édition, Frederick Gallegos
7 Contrôle et Audit Informatique – Deuxième édition, Frederick Gallegos
8 Contrôle et Audit Informatique – Deuxième édition, Frederick Gallegos

dette n'a aucune signification, mais ce total peut être utilisé pour vérifier que tous les numéros d'accord de dette corrects aient figuré dans le traitement.[9]

Le PDMIS peut inclure les fonctionnalités suivantes :

» dans l'interface avec d'autres systèmes entre applications, s'il y a une erreur dans le traitement des fichiers, un fichier d'erreur est généré et enregistré dans l'application du système. Développer une approche de l'interopérabilité de profondeur pour les profils techniques et pour la formation en général;

» l'application contient des traitements par lots programmés pour réaliser de nombreuses tâches. Par exemple, mise à jour du stock de dette, planification financière, indices, versements futurs, etc... Évaluer les sorties de systèmes en temps réel souple en se concentrant sur les journaux axés sur le traitement par lots ainsi que sur les capacités de temps réel «dur» pour mesurer le traitement actualisé d'informations;

» en cas d'erreur dans le traitement par lots, l'application envoie un message à l'utilisateur avec les informations sur l'erreur. Vérifier si les capacités de consolidation, au sein du système, se conforment aux politiques de correction d'erreurs et estimer ainsi les procédures de contrôle;

» à l'issue d'une opération, l'application affiche un message confirmant que le traitement a été réussi et présente un sommaire des données saisies;

» après toute modification de données préalablement enregistrées, l'application affiche un message indiquant le succès de la modification et présente un résumé des données modifiées ;

» après la suppression de données déjà saisies, l'application affiche un message indiquant le succès de la suppression et présente un résumé des données supprimées;

» si la suppression d'un enregistrement affecte l'intégrité relationnelle de la base de données, l'application n'autorise pas la suppression et affiche un message indiquant que l'enregistrement ne peut pas être supprimé. Par exemple, les données d'une banque créancière ne peuvent pas être supprimées de la table

9 Contrôle et Audit Informatique – Deuxième édition, Frederick Gallegos

des créanciers si ce créancier a des contrats en cours dans l'application; e

» l'application effectue des vérifications entre les données du FrontOffice et celles du BackOffice. Par exemple, en exigeant que le BackOffice valide les données d'entrée des enchères. Vérifier, dans les communications, les interrelations d'architecture de données entre les composants et les systèmes pour valider les flux de données selon le schéma de l'interopérabilité.

3.4. CONTRÔLES DE SORTIE

Les contrôles de sortie assurent l'intégrité des sorties ainsi que la distribution correcte et ponctuelle des sorties produites. Les faiblesses dans le traitement peuvent parfois être compensées par de stricts contrôles sur les sorties.[10] Une application bien contrôlée à la saisie et pendant le traitement est susceptible d'être entièrement fragilisée si la sortie n'est pas contrôlée.[11]

L'exhaustivité et l'intégrité des rapports de sorties dépendent desrestrictions portées à la possibilité de modifier les sorties et de l'intégration des contrôles d'exhaustivité tels que les numéros de page et les sommes de contrôle.[12]

Les fichiers de sortie doivent être protégés afin de réduire le risque de modification non autorisée. Les raisons possibles de modifier la sortie de l'ordinateur peuvent être la dissimulation de traitements non autorisés ou la manipulation des résultats financiers nondésirés.[13]

La sortie d'une application informatique peutêtre l'entrée vers une autre application. Si tel est le cas, le vérificateur doit rechercher les contrôles qui garantissent que les sorties sont transférées avec précision d'une étape de traitement à l'autre.[14]

Dans le PDMIS, les contrôles de sortie peuvent également être programmés de manière à identifier les informations critiques qui requièrent la mise en œuvre

10 Contrôle et Audit Informatique – Deuxième édition, Frederick Gallegos
11 Directives d'audit informatique, ASOSAI
12 Audit Informatique – Principes généraux (Audit Informatique Séries Monographiques # 1) – Bureau du Contrôleur et Vérificateur General des comptes de l'Inde
13 Audit Informatique – Principes généraux (Audit Informatique Séries Monographiques # 1) – Bureau du Contrôleur et Vérificateur General des comptes de l'Inde
14 Audit Informatique – Principes généraux (Audit Informatique Séries Monographiques # 1) – Bureau du Contrôleur et Vérificateur General des comptes de l'Inde

d'actions prioritaires par les responsables de la gestion de la dette publique. Par exemple, parmi les contrats signés dont l'échéance correspond au mois en cours, l'application peut afficher des alertes quotidiennes sur le premier écran du système concernant les contrats dont la date de paiement limite est dans les cinq prochains jours.

L'application peut permettre également à certains profils d'utilisateurs de générer des rapports en mode de priorité, permettant ainsi que l'application priorise les rapports à générer.

Le PDMIS peut inclure les fonctionnalités suivantes :

- comparaison automatique de la somme des données d'origine avec la somme des données traitées;
- l'application doit informer les utilisateurs sur le statut de génération des demandes de rapports, par exemple, «non commencé », «en cours» et «terminé» ;
- à la fin d'un processus de génération de rapports, l'application envoie un message à l'utilisateur ayant effectué la demande, l'informant que cette tâche a été menée à bien.

3.5. TESTS DES CONTRÔLES DES APPLICATIONS

Une fois que les contrôles ont été identifiés, l'étape suivante d'un audit est de vérifier leur efficacité.

Ceci peut être accompli en :

- soumettant un ensemble de données de test lesquelles, si l'application fonctionne correctement, produiront des résultats connus;
- développer des programmes indépendants pour ré-exécuter la logique de l'application;
- évaluer les résultats de l'application.

Les procédures ci-dessus testent l'intégrité d'un programme intégré à la PDMIS et non l'intégrité des données.

Si l'application possède un environnement de test, celui-ci peut être utilisé pour tester les contrôles, dans la mesure où il s'agit d'une copie confirmée de l'environnement de production.

Afin de tester les règles de calcul, comme celles qui se rapportent à la mise à jour du stock ou du service de la dette, l'auditeur peut faire usage de Techniques de vérification informatisée (CAAT), qui comprennent une multitude d'outils et de techniques généralisés notamment des logiciels, des logiciels utilitaires, des données de test, de suivi et de modélisation de logiciels d'application et d'applications spécialisées d'audit. Elles peuvent inclure des outils qui analysent la logique et les calculs de feuilles de calcul pour en apprécier la précision. Certains outils peuvent également être utilisés pour analyser les applications de base de données et en tirer un diagramme logique. Les logiciels d'audit généralisé peuvent être utilisés pour l'analyse de données produites par la plupart des applications.

L'auditeur devrait évaluer la nécessité d'utiliser un CAAT. Leur utilisation doit être déterminée en fonction de la sophistication de l'application de gestion de la dette publique.

Ce document contient une suggestion de matrice de tests (annexe III), qui peut servir de référence pour effectuer les tests sur les contrôles des applications. Cette matrice identifie certaines exigences et fonctionnalités que les systèmes de la dette publique devraient fournir, certaines requêtes qu'ils devraient être en mesure de remplir, ainsi que les exigences minimales de capacités de ces systèmes.

Il est important de noter que, de même que la dette de chaque pays possède une composition et des caractéristiques différentes, les systèmes de gestion de la dette présentent sans doute des caractéristiques différentes. C'est donc la responsabilité de l'équipe d'audit d'identifier, d'ajuster si nécessaire et d'utiliser, les éléments applicables aux systèmes de la dette de leur pays.

3.6. RAPPORTS DES RÉSULTATS DE L'AUDIT

En plus de se conformer à l'INTOSAI-P 1 - Déclaration de Lima, le cas échéant, des rapports d'audit du PDMIS pourraient prendre en compte le contenu de l'ancienne ISSAI 5440[15] - Orientations pour la conduite d'un audit de la dette publique - Utilisation de tests de corroboration dans les audits financiers, section 2.6 Résultats de l'audit.

Comme indiqué précédemment, cet audit est une vérification de performance. Il est donc important que le rapport suive les normes des rapports d'audit de performance,

telles qu'indiquées par ISSAI 3000 - Normes et lignes directrices pour l'audit de performance ayant pour base les Normes d'audit de l'INTOSAI ainsi que l'expérience pratique, ISSAI 300 – Principes fondamentaux des audits de performance.

15 Cette prises de position a été retirée du cadre en septembre 2019. Une nouvelle prises de position sur l'audit de la dette publique est en cours d'élaboration.

ANNEXE I : TABLEAU DE PLANIFICATION

Informations, documents et rapports requis

- Inventaire des systèmes d'information utilisés par le DMO et de la documentation liée ;

- Inventaire des ordinateurs et des systèmes d'exploitation de réseau utilisés par le DMO;

- Cartographie à jour des flux de processus du DMO;

- Rapports d'audits précédents sur le DMO;

- Rapports d'audits précédents liés aux systèmes informatiques de la dette;

- Lois et règlements liés au cadre du DMO et à la gestion de la dette publique ;

- Liste des gestionnaires du DMO et des services informatiques, responsables de la continuité d'activité, gestionnaires des ressources humaines, responsables des risques, audit interne, autres, avec leurs fonctions, adresses, courriels et numéros de téléphone;

- Documents montrant le fonctionnement du DMO et/ou de ses systèmes, comme les procédures écrites et les manuels de procédures du DMO ou du Ministère des finances:

- Gestion du personnel
- Sécurité de l'information.
- Gestion du changement

- Accès physique
- Exigences d'environnement/emplacement des TI
- Accès logique
- Plan de continuité des opérations (BCP)
- Plan anti sinistre (DRP)
- Plan de sauvegarde
- Services tiers (services informatiques)
- Rapports préalables d'évaluation des risques
- Résumé récent des évaluations de sécurité
- Décision récente de la sécurité et actions recommandées
- Statut de mise en œuvre des actions recommandées.
- Approbation de l'encadrement supérieur pour déployer le système

- Rapports diffusés par les entités externalisées chargées de fournir la maintenance du système;

- Autres documents liés au service de gestion de la dette publique et/ou son système (diapositives, textes, cibles et rapports annuels de gestion de la dette);

- Nombre d'employés du DMO qui sont utilisateurs du système et ont un profil d'accès;

- Nombre d'employés des services informatiques et spécification des fonctions (définition de rôle) pour le personnel du DMO et des TI;

- Liste des employés qui ont accès à la salle des serveurs;

- Description du profil d'accès au PDMIS;

- Spécification formelle de la manière et la périodicité de la mise à jour du système d'exploitation, pare-feu et antivirus;

- Liste des obstacles physiques et outils automatiques utilisés pour empêcher l'accès non autorisé au mainframe, stations de travail, serveurs et autres équipements du DMO;

- Emplacement de chaque salle à l'intérieur et à l'extérieur du DMO;

- Liste des quantités suivantes : personnel, postes de travail, serveurs;

- Montants du budgetpour les 5 dernières années;

- Liste de formation préalable, sur l'utilisation du PDMIS (personnel du DMO) et sur la mise à jour des connaissances informatiques (personnel informatique);

- Règles, pratiques et descriptions inhérentes énoncées pour éviter tout dommage causé par instabilité électrique, incendie, poussière, eau, nourriture, températures ou humidité extrêmes, électricité statique;

- Spécifications sur le fonctionnement de l'alimentation sans coupure (s'il y en a);

- Journaux des incidents aux demandes du DMO sur les erreurs ou les rapports de consignes d'utilisation du PDMIS ;

- Rapports des journaux d'incidents de sécurité;

- Liste des changements au système PDMIS au cours des 12 derniers mois;

- Journaux et rapports de test préalables des BCP et DRP et des événements qui ont eu lieu;

- Documentation des applications et manuel de l'utilisateur;

- Termes d'utilisation de chaque application;

- Manuel de procédures pour traiter les erreurs de traitement;

- Échantillon de données pour ré-exécuter des opérations afin de vérifier les contrôles et les calculs des applications.

Procédures

- Étudier la documentation du système (les manuels et les conditions d'utilisation) pour connaître les principaux processus de la dette réalisés par les systèmes d'information. Si la documentation sur les processus du DMO est insuffisante, l'équipe de vérification devra examiner et modéliser les processus;

- Vérifier l'existence de règles juridiques liées à l'utilisation, la maintenance et la gestion du Système d'information de gestion de la dette publique;

- Identifier, dans les audits précédents, les constatations ayant trait à des points faibles sur les flux d'opération de la dette publique et/ou sur les systèmes de gestion de la dette publique;

- Identifier les principaux contrôles généraux en s'appuyant sur la documentation du système;

- Identifier les principaux contrôles des applications en s'appuyant sur la documentation du système: contrôles d'entrée, traitement et sortie;

- Effectuer une évaluation des risques sur les contrôles généraux principaux et les applications afin d'évaluer les risques qui ont une incidence sur ces systèmes et la sévérité de leur impact sur la gestion de la dette publique;

- Déterminer les systèmes qui ont un impact sur les fonctions critiques et les données, telles que la saisie, le traitement et la sortie de données, la liste des créanciers, les calculs de la dette publique, le reporting, la prise de décisions;

- Identifier les contrôles internes mis en place pour atténuer ou réduire les risques constatés

- Classer les systèmes et les processus d'après l'évaluation des risques et déterminer le champ de l'audit;

- Estimer les ressources et le calendrier;

- Organiser des entretiens avec le chef du service informatique, les gestionnaires et l'organe technique chargés de travailler sur les aspects de développement/ maintenance/fonctionnement du système;

- Élaborer une matrice de vérification des contrôles généraux et des applications et déterminer les tests à réaliser. (Voir la matrice proposée à l'annexe III).

L'ISC devrait répondre aux questions suivantes

- Quels sont les systèmes d'information de gestion de la dette publique et quel est le rôle de chaque système dans la gestion de la dette publique ?

- Le PDMIS a-t-il été développé par le MDO exclusivement ou provient-il d'un tiers? Dans ce dernier cas, une personnalisation a-t-elle été réalisée afin de répondre aux besoins spécifiques du DMO?

- Qui doit être interrogé sur les questions de contrôles généraux informatiques au sein du DMO?

- Qui doit être interrogé pour clarifier les contrôles des applications du PDMIS?

- Qui sont les principaux utilisateurs du PDMIS?

- Quels sont les contrôles généraux et des applications du PDMIS ?

- Les contrôles internes sont-ils en mesure de réduire les risques des systèmes d'information susceptibles d'affecter la gestion de la dette publique?

- Quels sont les risques les plus élevés liés à la saisie, au traitement et à la sortie des données du PDMIS?

- Quels tests relatifs aux contrôles des applications et aux contrôles généraux devraient être mis en œuvre?

ANNEXE II: MATRICE DE TEST POUR LES CONTRÔLES GÉNÉRAUX

CONTRÔLES GÉNÉRAUX		
Les objectifs des contrôles généraux sont de protéger les données, protéger les programmes d'application et assurer la continuité des opérations informatiques en cas d'interruptions imprévues.		
BESOINS / FONCTIONNALITÉS	**CONTRÔLES GÉNÉRAUX**	**SUGGESTION DE PROCÉDURES DE TEST**
Questions d'ordre général	Les actions du service informa-tique doivent être cohérentes avec la mission du DMO Le monitoring de la performance du PDMIS doit exister et tenir compte des objectifs du DMO Un audit interne doit être effectué périodiquement sur les opérations du DMO et du PDMIS	Examiner des échantillons de décisions ou de mémos des gestionnaires, liés aux actions informatiques, pour s'assurer qu'ils sont clairs, bien étayés et cohérents avec la mission du DMO Évaluer les mesures de performance du PDMIS vis-à-vis des cibles attendues et s'assurer que l'encadrement supérieur reconnaisse ces mesures. Évaluer les rapports des audits internes précédents sur les contrôles généraux informatiques, afin d'identifier toute déficience grave Évaluer la quantité relative et la capacité des postes de travail et autres équipements informatiques, ainsi que du personnel, tout en veillant à ce que cedernier possède les compétences requises

Questions d'ordre général		Évaluer la taille des budgets, en la comparant aux périodes précédentes et aux secteurs informatiques d'autres entités gouvernementales
Contrôles organisationnels	La direction du DMO ou du MF doit s'engager à développer et maintenir un bon environnement informatique général Le personnel informatique etcelui du DMO doivent recevoir une formation périodique adéquate, incluant la sensibilisation à la sécurité Il doit y avoir un programme de formation Il doit y avoir des politiques et des procédures normalisées écrites pour: • la sécurité de l'information. • les ressources humaines • les services tiers informa-tiques • la gestion du changement • les accès physiques et logiques • les plans de continuité des opérations et de reprise après sinistre	Interroger la direction du DMO sur leur intérêt pour les questions informatiques afin d'évaluer leur engagement à développer et maintenir un bon environnement informatique général Examiner les éléments de preuve indiquant que les formations ont bien eu lieu Interroger les utilisateurs du DMO et du personnel informatique sur: • la fréquence de la formation • la nécessité de connais-sances/ formation • la connaissance des politiques Évaluer le caractère adéquat des politiques écrites et procédures standard pour les services informatiques Observer si le personnel du DMO travaille conformément aux procédures standard (établies dans le manuel)

Contrôles organisationnels	Les politiques et procédures standard doivent être actuali-sées périodiquement Les procédures doivent être diffusées correctement par la direction du DMO Les employés DMO doivent connaitre ces politiques Il doit y avoir une documentation de procédures couvrant toutes les activités de gestion de la dette L'organisation doit mettre en place une séparation appropriée des fonctions pour faire en sorte que les utilisateurs n'aient pas plus de pouvoir que ne l'exige leur poste	
Contrôles d'accès physique	L'accès physique au mainframe et serveurs doit être bien protégé (portes, serrures, etc.) Il devrait y avoir une surveillance vidéo Les fenêtres de la salle où se trouvent mainframes et serveurs doivent être protégées contre l'accès forcé	Vérifier l'existence réelle et le fonctionnement des obstacles physiques qui empêchent l'accès non autorisé au mainframe, aux serveurs et aux postes de travail du DMO Vérifier si les procédures administratives du personnel pour empêcher l'accès non autorisé à, l'ingérence dans les services informatiques fonctionnent conformément au cadre établi et de manière satisfaisante

Contrôles d'accès physique	Seules les personnes autorisées doivent avoir accès à la salle des serveurs	Afin d'identifier toute faiblesse des contrôles automatisés, observer comment fonctionnent les outils électroniques, tels que les serrures électroniques, les systèmes de verrouillage du clavier, les caméras et autres moyens de limiter l'accès physique aux serveurs et aux autres infrastructures essentielles Dans le cas de systèmes de verrouillage du clavier, vérifier s'il y a partage de mots de passe entre les employés
Contrôles d'accès logique	Si les services informatiques de la dette publique sont externalisés, le contrat de service doit préciser les mesures de contrôle adéquates pour s'assurer du non-accès par une tierce partie aux secrets d'affaires, aux données importantes ou aux stratégies liées à la dette publique Il ne doit y avoir aucun ancien employé, personne non employée par le DMO ou utilisateur «virtuel» disposant d'un profil d'accès actif Les droits d'accès doivent être révisés périodiquement Lesantivirus, pare-feu, les intrusions et les systèmes de détection des codes malveillants devraient être à jour et fonctionner	Évaluer si les profils d'accès sont cohérents avec le rôle de l'employé Vérifier si un ancien employé, personne non employée par le DMO dispose encore d'un profil d'accès actif Vérifier l'existence de pare-feu, antivirus actualisé, détecteurs de logiciels mal- veillants et d'intrusions Vérifier si les systèmes d'exploitation sont systéma-tiquement mis à jour sur les postes de travail et les serveurs Déterminer si la politique relative aux mots de passe est correctement appliquée Vérifier si les procédures sont définies et documentées

Contrôles d'accès logique	Il devrait y avoir une mise à jour systématique du système d'exploitation sur les postes de travail et les serveurs L'organisation doit définir des procédures pour autoriser, révoquer ou modifier le contrôle d'accès du personnel lorsque les conditions changent (embauches, licenciements, changement de fonctions, etc.) L'organisation doit faire connaître ses politiques ou lignes directrices concernant les mots de passe de sécurité et les autres contrôles de sécurité (cartes-clés, etc.) à tous les utilisateurs du système de gestion de la dette	
Contrôles environnementaux	Il devrait y avoir des tuyaux (eau, chauffage, électricité, etc.) tout au long de la salle des serveurs Il devrait y avoir des détecteurs d'eau, de chaleur et d'humidité Il devrait y avoir un système anti-inondation dans la salle des serveurs	Visiter la salle des serveurs pour inspecter et évaluer les conditions environnementales - ceci vaut pour les autres salles du DMO Vérifier l'existence et le maintien effectif des dispositifs de prévention de l'incendie, des inondations,de l'humidité Vérifier l'existence et le fonctionnement effectif d'alimentations électriques alternatives pour éviter toute interruption des services informatiques

Contrôles environnementaux	Il devrait y avoir des dispositifs de détection de fumée/incendie Il devrait y avoir un plancher surélevé ou alors l'équipement devrait être situé 15 à 20 cm au-dessus du sol sur des supports Il devrait y avoir une alimentation électrique sans coupure (UPS) pour soutenir l'opération du mainframe et des serveurs	
Contrôles de modifications aux programmes	L'équipe de gestion informatique doit conserver un journal des dysfonctionnements, incidents et erreurs Le journal doit tracer l'incident depuis la cause sous-jacente jusqu'à la résolution Il ne doit y avoir, au service d'assistance, aucune demande importante d'instruction du PDMIS non résolue Il doit y avoir escalade du problème pour les événements critiques et un niveau de réponse fonction du degré de priorité de l'événement Il doit y avoir un rapport d'incidents de sécurité communiqué à l'encadrement du DMO	Évaluer le temps passé pour résoudre les demandes du DMO concernant les instructions d'utilisation ou les défaillances dans le fonctionnement du PDMIS Identifier les défaillances du PDMIS les plus fréquentes et leurs causes probables Comparer les changements antérieurs avec des procédures standard

Contrôles de modifications aux programmes	Les changements préalables devraient suivre les procédures standards Si un système de gestion de la dette non standard est utilisé, l'organisation doit avoir des procédures documentées pour le contrôle des modifications et signaler les personnes autorisées à effectuer des changements au système L'organisation doit suivre et surveiller toutes les modifications apportées au système de la dette (pistes d'audit)	
BCP et DRP	Il doit y avoir des plans BCP et DRP établis par le DMO Le personnel chargé d'assurer la continuité opérationnelle doit connaître ses rôles et responsabilités Les défaillances dans les tests préalables aux BCP et DRP ou les événements qui ont effectivement eu lieu et les mesures prises par le DMO pour résoudre ces défaillances doivent être signalées La documentation de prêts doit être conservée dans un endroit sûr où les documents sont protégés contrele vol, l'incendie, les inondations ou d'autres incidents pouvant l'endommager ou la détruire	Évaluer la cohérence et l'exhaustivité des BCP et DRP et si ils sont actualisés Évaluer les rapports sur les tests préalables effectués sur les BCP, DRP et sur le plan de sauvegarde Vérifier si les plans BCP et DRP sont diffusés à tout le personnel de manière adéquate ; Vérifier si les « back-ups » hors-site sont en bon état et peuvent être utilisés pour redémarrer le système en cas de défaillance;

ANNEXE III : MATRICE DE TESTS POUR LES CONTRÔLES DES APPLICATIONS

NORMES DE DOCUMENTATION		
Les objectifs des normes de documentation sont d'assurer que les contrôles s'exerceront de manière continue et réduiront les risques d'erreur.		
Sauvegarde de la documentation	**Une copie de sauvegarde de la documentation devrait être**	**Vérifier la documentation**
CONTRÔLES D'ENTRÉE		
L'objectif des contrôles d'entrée est de garantir l'autorisation, la précision, l'intégralité et la ponctualité des données entrées dans une application.		
BESOINS / FONCTION-NALITÉS	**CONTRÔLES DES APPLICATIONS**	**PROCÉDURES DE TEST POSSIBLES**
Contrôles de la documentation	La documentation de l'application doit être suffisamment complète (avec toutes les fonctionnalités des applications et fonctionnements connexes) La documentation doit être actualisée pour refléter les modifications apportées à l'application	Vérifier la documentation Vérifier la documentation Faire un échantillon de contrôles des applications spécifiés dans les contrôles de documentation et vérifier s'ils sont mis en œuvre conformé- ment à la documentation et fonctionnent efficace-ment

Contrôles de la documentation	Les contrôles des applications compris dans la documentation devraient être mis en place et fonctionner correctement	
Champs à saisie obligatoire	L'application n'autorise pas la confirmation de l'opération si les champs de saisie obligatoire ne sont pas remplis	Essayer de confirmer l'opération en omettant des données obligatoires et vérifier que la transaction n'est pas traitée Ce test devrait être appliqué aux processus suivants : enregistrement de contrat, activation de contrat, enregistrement émission de titres, etc.
Entrée de données correctes et adéquates	L'application n'accepte pas les données incorrectes ou non valides	Vérifier le format des données au niveau de la base de données Examiner les spécifications de blocage d'entrées et en vérifier quelques unes dans l'capplication Essayer d'introduire des données incorrectes ou non valides et vérifier message d'erreur et blocage. Ce test devrait être appliqué aux processus suivants: enregistrement de contrat, activation de contrat, enregistrement émission de titres, mise à jour d'index, rachat de titres, etc.
	L'application ne permet pas la duplication des données	Essayer d'enregistrer un contrat ou un titre portant le même nom qu'un autre déjà existant et vérifier l'existence d'un blocage et d'unmessage de duplication

Entrée de données correctes et adéquates	Pour les taux d'intérêt d'un contrat, il ne doit pas y avoir de période de chevauchement ou de découvert s'agissant de l'applicabilité des taux d'intérêt	Vérifier dans la base de données s'il y a des périodes avec des taux d'intérêt qui se chevauchent ou des périodes sans intérêt
	En cas de contrat de donation, l'application doit permettre l'entrée des décaissements puisque, dans ce cas, il n'y a aucun amortissement et aucune opération sur les intérêts	Essayer d'entrer un décaissement à l'un des contrats de donation et vérifier si l'application ne requiert pas d'amortis- sement ni d'opération sur les intérêts
	Dans l'écran de saisie des versements, lorsque l'utilisateur effectue une recherche de contrats afin d'enregistrer un décaissement, l'application doit montrer seulement les contrats ayant un statut «actif» dans la phase de «décaissement» ou de «décaissement et amortissement»	Essayer d'entrer un décaissement et vérifier les phases de contrats montrés par l'application
	Si le régime de taux d'intérêt est flottant, l'application doit exiger l'inclusion de l'index	Vérifier si l'application requiert l'inclusion de l'index lorsque le régime de taux d'intérêt flottant est sélectionné
	L'application ne doit pas permettre l'entrée de nombres décimaux pour la quantité de titres émis	Essayer d'introduire des nombres décimaux pour la quantité de titres émis et vérifier le blocage de l'application

Entrée de données correctes et adéquates	L'application doit permettre la création d'un titre avant son émission	Simuler la création d'un titre sans effectuer son émission
Intégralité de l'information	Toutes les informations pertinentes sur la dette doivent être saisies dans l'application	Vérifier si toutes les données importantes de la dette sont entrées dans l'application, telles que les opérations de crédit, les garanties, les prêts, les taux d'intérêt, les taux d'échange, etc.
Compatibilité entre les dates	La date initiale pour le calcul du taux d'engagement doit être antérieure à la date de conclusion du projet	Essayer d'introduire une date initiale pour le calcul du taux d'engagement postérieure à la date de conclusion du projet et vérifier l'existence d'un blocage et d'un message d'erreur
	La date d'entrée en vigueur doit être antérieure à la date de conclusion du projet	Essayer d'introduire une d'entrée en vigueur postérieure à la date de conclusion du projet et vérifier l'existence d'un blocage et d'un message d'erreur
	La date d'entrée en vigueur doit être antérieure à la date limite de décaissement	Essayer d'introduire une d'entrée en vigueur postérieure à la date limite de décaissement et vérifier l'existence d'un blocage et d'un message d'erreur
	La date limite pour le déboursement doit être antérieure à la date de conclusion du projet	Essayer d'introduire une date limite pour le déboursement posté- rieure à la date de conclusion du projet et vérifier l'existence d'un blocage et d'un message d'erreur
	Pour obtenir le rapport d'échéances, la date finale d'échéance des titres doit être postérieure à la date initiale	Essayer d'introduire une date initiale postérieure à la date limite d'échéance d'un titre et vérifier l'existence d'un message indicatif de l'erreur

Compatibilité entre les dates	L'application n'accepte pas de dates futures pour les opérations	Essayer d'exécuter certaines opérations en introduisant une date ultérieure et vérifier l'existence d'un blocage et d'un message d'erreur Ce test devrait être appliqué aux processus suivants: enregistrement de contrat, activation de contrat, enregistrement émission de titres, mise à jour d'index, rachat de titres, enregistrement de décaissements, compléments de contrat, etc.
	La date d'émission d'un titre doit être antérieure à sa date d'échéance	Essayer d'introduire une date d'émission postérieure à la date d'échéance et vérifier l'existence d'un blocage et d'un message d'erreur
	En cas d'enregistrement d'un paiement d'amortissement, si le montant ou la date d'entrée diffèrent de ceux de l'application, l'application doit afficher un message informant l'utilisateur d'une telle situation, avant que la confirmation de l'opération ne puisse être effectuée	Enregistrer un paiement avec une date ou une valeur différente de celle de l'application et vérifier si l'application affiche un message
	Si la date de liquidation est différente de la date d'échéance, l'application doit requérir que les champs de «justification» ou d'«aval du créancier» soient remplis	Introduire des dates différentes pour l'échéance et la liquidation et vérifier si l'application requiert une justification ou un aval

Compatibilité entre les dates	Les versements réguliers ne peuvent pas avoir de périodes se chevauchant. Par exemple, la date initiale du deuxième versement ne peut être antérieure à la date limite du premier déboursement	Essayer d'introduire une date du deuxième versement antérieure à la date du premier et vérifier l'existence d'un blocage et d'un message d'erreur
Sécurité de l'entrée de données et des opérations	L'application ne doit pas permettre que des personnes non autorisées saisissent certaines données et effectuent certaines opérations	Vérifier l'existence de «jetons» ou dispositifs de sécurité et de prérequis de profils spécifiques. Essayer de saisir des données et d'effectuer certaines opérations sans avoir le bon profil et vérifier l'existence d'un blocage. Ces tests devraient être appliqués aux processus suivants: enregistrement de contrat, activation de contrat, enregistrement émission de titres, mise à jour d'index, rachat de titres, enregistrement de décaissements, etc.
	L'application devrait enregistrer l'historique des accès en cas de saisie manuelle de données	Vérifier l'existence de journaux d'accès restreint et déterminer si ces journaux peuvent être lus ou modifiés par des personnes qui n'en ont pas l'autorisation
	L'application ne doit pas permettre une modification de la valeur d'un contrat actif	Essayer de changer la valeur d'un contrat actif et vérifier s'il y a blocage
	L'application doit empêcher la modification de données et la suppression des contrats ayant un statut «annulé» ou «terminé»	Essayer de modifier et de supprimer certaines données sur un échantillon de contrats ayant le statut «annulé» ou «terminé» et vérifier si le PDMIS bloque de telles tentatives

Sécurité de l'entrée de données et des opérations	L'application ne doit pas permettre l'exclusion d'un contrat actif, sauf si le contrat est en négociation ou inactif	Essayer de supprimer un contrat actif et vérifier s'il y a blocage
	L'application ne doit pas autoriser l'exclusion incorrecte d'un titre émis, à moins qu'il n'y ait aucune opération liée à ce titre	Essayer de supprimer un titre émis, ayant une opération liée, et vérifier s'il y a blocage
	L'application devrait exiger une double autorisation pour exécuter des opérations critiques	Vérifier si les opérations critiques nécessitent une double autorisation pour être finalisées Ce test devrait être appliqué aux processus suivants: activation de contrat, émission de titres, paiement d'amortis- sements, rachat de titres, changements de valeurs de contrats, paiement de coupons, contrepassation des paiements, changements de taux d'intérêt, etc.
	L'application devrait accepter uniquement les données provenant de sources reconnues. Le prêt entré doit être conforme aux accords et normes acceptées	Vérifier que les données clés sont saisies deux fois et qu'un message d'erreur est affiché lorsque les données sont différentes.
	L'application doit permettre la réduction d'une valeur contractuelle, tant que celle-ci ne soit pas supérieure à la valeur du «solde à décaisser»	Essayer de réduire la valeur d'un contrat en dessous de la valeur à décaisser et vérifier l'existence d'un blocage et d'un message d'erreur

Sécurité de l'entrée de données et des opérations	L'application ne doit enregistrer toutes les opérations qu'une seule fois	Effectuer certaines transactions identiques (par exemple : paiement d'un amortissement) et vérifier s'il y a blocage et si celles-ci ne sont pas dupliqués dans la base de données
	Lors de l'enregistrement d'un paiement, si l'autorisation de l'utilisateur est révoquée, l'application ne devrait signaler la révocation qu'une fois que l'utilisateur ait activé la commande «Enter», permettant ainsi de journaliser à la fois l'intention manquée et les données que l'utilisateur voulait introduire	Essayer d'enregistrer un paiement avec une autorisation révoquée et vérifier l'existence d'un blocage et la journalisation
	Dans le cas de transferts de fichiers automatique entre applications, le PDMIS doit conserver les données originales provenant de l'autre application pour une période prédéfinie par le DMO.	Vérifier les données conservées transférées à partir d'autres applications pour s'assurer qu'elles sont chiffrées ou protégées contre les dommages, pertes ou violation
	L'application ne doit pas permettre la modification des taux d'intérêt d'un versement déjà payé, et toute modification du taux d'intérêt devrait nécessiter d'une deuxième autorisation pour être complétée	Essayer de modifier le taux d'intérêt d'un versement payé et vérifier le blocage. Vérifier également si l'application requiert une deuxième autorisation pour modifier un taux d'intérêt

Compatibilité entre les valeurs	La valeur de la tranche doit être inférieure à la valeur du contrat	Essayer d'introduire une valeur de tranche supérieure à celle du contrat et vérifier l'existence d'un blocage et d'un message d'erreur
	La valeur de rachat doit être inférieure à la valeur du titre émis	Essayer de faire un rachat de titre pour une valeur supérieure à celle du titre émis et vérifier l'existence d'un blocage et d'un message d'erreur
	L'application affiche une alerte en cas de paiement insuffisant ou excédentaire avant traitement	Simuler un paiement insuffisant ou excédentaire et vérifier l'existence de l'alerte
Documents source	Une piste quant à la source des documents des entrées devrait exister pour garantir l'authenticité des données d'entrée	Sélectionner quelques données d'entrée et de vérifier si le document source existe (par exemple contrat de prêt, courriel, information électronique, etc.)

CONTRÔLES DE TRAITEMENT		
Les contrôles de traitement visent à s'assurer que les données sont traitées avec précision tout au long de l'application et qu'aucune donnée n'est ajoutée, perdue ou altérée en cours de traitement.		
BESOINS / FONCTION-NALITÉS	**CONTRÔLES DES APPLICATIONS**	**SUGGESTION DE PROCÉDURES DE TEST**
Indication correcte de statut	L'application doit changer le statut d'un contrat après son déboursement total	Simuler une finalisation de déboursement et vérifier si le statut de contrat passe d' «en décaissement» à « totalement déboursé»
	L'application doit changer l'indication du statut d'un titre lorsque son émission est confirmée	Simuler une confirmation d'émission de titre et vérifier si le statut du titre passe d'«inactif» à «actif»
	L'application doit changer le statut d'un contrat ou d'un titre après le déboursement total	Simuler le dernier paiement et vérifier si le statut du contrat ou du titre est modifié
	L'application doit prévoir au moins les phases suivantes: • en décaissement: les versements sont créés lors de cette phase • déboursée entièrement : les versements lors de cette phase ne sont pas autorisés • terminé: lors de cette phase, les versements ne subissent plus aucune	Créer un contrat, essayer d'effectuer un versement pour chacune des phases et vérifier l'existence d'un blocage et d'un message d'erreur

Indication correcte de statut	opération financière et la modification des données n'est plus permise	
	L'application doit contenir des règles pour que le statut du contrat (actif, inactif) soit compatible avec les phases (en décaissement, entièrement déboursé, en amortissement, en décaissement et amortissement, terminé) afin d'éviter des contradictions dans l'information. Par exemple, un contrat avec un statut «inactif» ne peut pas être dans la phase «en décaissement» ou «en amortis- sement»	Simuler quelques changements de statut de contrat et de phase et vérifier s'ils sont compatibles
	L'application doit comporter un programme de mise à jour des phases du contrat. Par exemple, lorsque le solde à décaisser est égal à zéro, modifier la phase d'«en décaissement» à «totalement déboursé»	Simuler les conditions nécessaires pour changer la phase du contrat et vérifier si ce changement à lieu

Calcul correct	L'application doit exécuter le calcul correctement	Vérifier calcul et ré- exécuter Ce test de calcul devrait s'appliquer aux informations suivantes: encours de la dette (contractuels et titrisés), échéances, programme d'amortis- sement (dates et valeurs), valeur des commissions des agents, flux de paiements, valeur financière de rachat, etc.
	Après certaines modifications aux données d'entrée, l'application doit effectuer le calcul et la mise à jour de données	Faire certains change-ments aux entrées et vérifier la mise à jour des données et les résultats. Par exemple : • simuler un paie- ment et vérifier si le solde impayé et les flux d'amortissement ont été mis à jour • changer certains indices et vérifier si la valeur de l'encours de la dette a été mise à jour
	L'application doit contenir, dans sa programmation, au moins les méthodes suivantes pour le calcul des versements: distribution uniforme, intérêt simple, versements, application de prix, application d'amortissement constant, panier de monnaies Pool Unit (BIRD - Banque internationale pour la reconstruction et le développement) et panier de monnaies UAC (BID - Banque interaméricaine de développement)	Vérifier les méthodes utilisées par le système pour calculer les versements. L'exactitude des méthodes peut être vérifiée sur des exemples de données méthodes peut être vérifiée sur des exemples de données

Calcul correct	Chaque fois que le champ «valeur de contrat» est modifié, l'application doit recalculer automatiquement le champ «solde à décaisser»	Changer la valeur de contrat et vérifier si le champ de solde à décaisser du contrat a étémis à jour correctement
	Les dates de versements doivent être générées automatiquement par l'application selon les méthodes possibles suivantes: • date initiale et nombre fixe de versements • date initiale, date limite et nombre décroissant de versements • date initiale, date limite et nombre décroissant de versements • date initiale et nombre de périodes • périodes	Introduire les données requises par chaque méthode possible et vérifier si les dates de versements sont correctes
	Lorsque la date du versement correspond à un jour non ouvrable, l'application doit offrir deux options: avancer la date au jour ouvrable suivant ou la ramener au précédent	Configurer un versement avec la date d'un jour non ouvrable et vérifier si l'application permet de changer la date au jour ouvrableprécédent ou suivant

Calcul correct	Le système devrait automatiquement mettre à jour la valeur nominale des titres chaque fois qu'il y ait un changement sur l'indexeur respectif	Changer un indexeur d'un titre et vérifier si la valeur nominale respective est mise à jour
	En cas de paiement d'une somme inférieure à celle calculée par l'application, un message est affiché au moment de l'entrée du paiement. Le message devrait être répété jusqu'à la date d'échéance du prochain versement	Simuler un paiement inférieur au montant calculé par l'application et vérifier l'existence d'un message et s'il se répète jusqu'à la date du prochain versement
	Le système doit différencier dans sa base les titres ayant une émission simulée	Vérifier dans la base de données si les titres simulés sont différenciés et vérifier s'ils sont ignorés dans le calcul de l'encours et l'échéance de la dette
	Lorsque l'utilisateur supprime un titre, l'application doit supprimer les valeurs respectives de la base de données	Supprimer un titre et vérifier si sa valeur est supprimée dans la base de données
	Les titres ayant le statut «annulé» ne doivent pas être considérés pour le calcul des titres de dette (p. ex. IRR, échéances, etc.), c'est-à-dire qu'une fois annulées, les valeurs respectives doivent être exclues définitivement de la base de données	Changer le statut d'un titre à «annulé» et vérifier si sa valeur est ignorée dans les calculs (encours, échéances, etc.)

Calcul correct	L'application doit traiter différemment les versements ayant des paiements en souffrance	Vérifier si l'application calcule correctement les frais sur les versements en souffrance
Contrôle adéquat des erreurs de traitement	Les erreurs de traitement datant de jours ou semaines ne doivent pas être laissées sans solution	Vérifier s'il existe un critère concernant le nombre de jours que doit prendre la correction d'erreurs dans le système. Vérifier l'existence de messages d'erreur et discuter, avec les gestionnaires du système et de la dette, les mesures prises pour corriger les erreurs affichées
	En cas d'erreur de traitement, l'application doit annuler ce dernier et enregistrer, dans la base de données, la date, l'heure et la raison technique du problème	Simuler une erreur de traitement et vérifier si l'application enregistre dans la base de données le problème qui s'est produit
Enregistrement correct	L'application devrait permettre aux gestionnaires de la dette d'enregistrer avec précision les flux de trésorerie (associés aux et emprunts en devises nationales et étrangères, aux activités de courtage et de couverture, aux garanties et aux rétrocessions) pour toutes les transactions	Effectuer une transaction et vérifier si son enregistrement est correct et précis

Enregistrement correct	L'application devrait conserver un historique des transactions effectuées pendant la durée du contrat et doit inclure des détails sur le créancier, la valeur du contrat, la date de clôture du projet, les dates limite des champs de versements	Sélectionner certains contrats et vérifier s'il existe un historique de toutes les transactions effectuées à date sur ceux-ci, avec tous les détails nécessaires
	L'application devrait avoir un journal de dette pour chaque titre de créance	Vérifier si les transactions historiques liées à un titre ou contrat coïncident avec le journal de dette
Tâches programmées correctes	L'application devrait avoir un démarrage automatique de tâches selon une planification fixée par le DMO pour mettre à jour les indexes, l'encours de la dette, etc.	Vérifier l'existence de démarrages automati- ques et s'ils fonctionnent correctement
Pistes d'audit	Une piste d'audit du PDMIS devrait être maintenue afin d'activer le suivi des contrats ou des titres de dette, de la signature ou émission jusqu'au remboursement	Vérifier l'existence d'une piste d'audit pour un échantillon de contrats et de titres, de l'enregistrement jusqu'au remboursement

CONTRÔLES DE SORTIE		
Le but des contrôles de sortie est d'assurer l'intégrité, ainsi que la distribution correcte et ponctuelle, des sorties produites.		
BESOINS / FONCTION-NALITÉS	**CONTRÔLES DES APPLICATIONS**	**SUGGESTION DE PROCÉDURES DE TEST**
Contrôle sur les utilisateurs de l'information	L'application devrait avoir un journal de rapports, qui conserve le nom de l'utilisateur qui a fait la demande du rapport ainsi que la date et l'heure de cette demande.	Exiger certains rapports et vérifier si l'application enregistre les données
	L'application devrait nécessiter une autorisation spéciale pour produire certains rapports spéciaux (surtout s'il s'agit d'informations sensibles)	Essayer de produire quelques rapports prédéfinis
Rapports en temps opportun et fiables	L'application doit produire des rapports prédéfinis (classifiés par bond, prêt et tranche, par exemple pour échéance, statut, type de financement, source de financement, type de crédit d'instrument, modalités, factures impayées, etc...)	Essayer de produire ces rapports
	L'application doit produire certains rapports correctement, en garantissant leur intégralité et l'intégrité de l'information	Vérifier si les rapports sont conformes aux conditions d'utilisation Vérifier si les rapports présentent des numéros de page et de sommes de contrôle

Rapports en temps opportun et fiables		Ce test devrait être appliqué aux rapports suivants: rapport d'échéances (pour dette contractuelle et titrisée), rapport de solde impayé, rapport de réception, etc.
	L'application doit produire des rapports, tant globaux (toutes les titres de dette) que spécifiques, tels que: • Par statut de titre (émis, annulé, racheté, etc..). • Pour les événements dans un intervalle de dates (émissions, rachats, etc...) • Pour les obligations à court et long terme • Par position de portefeuille • Par type de titre • Par intervalle d'échéance, etc.	Essayer de générer des rapports, globaux et spécifiques, en utilisant comme critère, les données suivantes: • Par statut de titre (émis, annulé, racheté, etc..). • Pour les événe-ments dans un intervalle de dates (émissions, rachats, etc...) • Pour les obligations à court et long terme • Par position de portefeuille • Par type de titre • Par intervalle d'échéance, etc.
	Les rapports doivent présenter des informations complètes et correctes	Générer les rapports et ré-effectuer les calculs Ce test devrait être appliqué aux rapports suivants: rapport d'échéances (pour dette contractuelle et titrisée), rapport de solde impayé, rapport de réception, etc.

Rapports en temps opportun et fiables	Les rapports devraient présenter exactement les mêmes informations que l'application	Comparer la cohérence des rapports avec l'information présentée sur les écrans de l'application Ce test devrait être appliqué aux rapports suivants: rapport d'échéances (pour dette contractuelle et titrisée), rapport de solde impayé, rapport de réception, etc.
	Les valeurs présentées dans les rapports d'échéances, de solde impayé et d'encours de la dette doivent correspondre	Comparer la cohérence des rapports
	Le système devrait être en mesure de produire des rapports sur les totaux de la dette, sur une base individuelle et agrégée, avec les prévisions du service de la dette sur les emprunts et titres actuels et futurs	Essayer de produire ces rapports Vérifier si les rapports couvrent les opérations d'emprunt existants et prévus
	L'application doit générer automatiquement des rapports quotidiens de planification financière pour tous les contrats «actifs». Elle devrait également permettre la génération manuelle de rapports pour des contrats spécifiques	Vérifier l'existence de rapports automatiques pour tous les contrats actifs et essayer de générer des rapports manuels pour des contrats spécifiques

Transmission correcte de données	Le transfert de données entre applications et/ou étapes de traitement doit être exact et complet	Simuler un transfert de données entre applications et vérifier l'exactitude des données et leur exhaustivité
Affichage de messages utiles	Lorsqu'on accède à une application, celle-ci devrait afficher un message contenant les informations suivantes: • Contrats arrivant à échéance dans les cinq prochains jours • Contrats ayant des paiements de versements en souffrance • Contrats ayant des versements payés partiellement • Contrats avec dates de versement expirées Pour les contrats ayant une date limite de décaissement de 5 jours, l'application devrait envoyer un message tous les jours jusqu'à ce que le paiement se fasse, ou la valeur à décaisser soit annulée, ou bien la date limite soit modifiée	Accéder à l'application et vérifier si elle affiche tous ces messages
	L'application doit indiquer le statut du calcul, tel que «calcul en cours d'exécution» ou «calcul terminé»	Requérir un calcul et vérifier si l'application indique le statut de l'opération

Affichage de messages utiles	À la fin d'un rapport, l'application devrait afficher un message indiquant que la génération du rapport a été achevée ou afficher le rapport demandé	Requérir un rapport et vérifier si l'application affiche un message indiquant que l'opération soit terminée ou bien affiche le rapport demandé
	L'application devrait informer sur le statut de la génération des rapports, comme «en cours» ou «terminé»	Générer un rapport et vérifier si l'application informe sur le statut de l'opération
	Si une modification du taux d'intérêt est faite, l'application doit afficher un message d'alerte	Changer les taux d'intérêt et vérifier l'existence d'un message d'alerte
	Avant de traiter l'exclusion ou le rachat d'un titre, l'application devrait afficher un écran avec les informations du titre qui est supprimé ou échangé pour que l'utilisateur confirme l'opération	Essayer de racheter ou de supprimer un titre et de vérifier si l'application affiche un message et une demande de confirmation

FIGURE 1 : AUDIT DE LA DETTE PUBLIQUE PAR LES ISC : LE CAS DU BRÉSIL

Vérification effectuée par la Cour des comptes brésilienne sur le Système intégré de la dette (SID) du gouvernement fédéral brésilien en 2014

Considérant que le système IDS est en phase de tests sur la dette financière domestique, l'équipe de vérification a choisi de se concentrer uniquement sur les tests de processus liés à la gestion de la dette externe (sous forme de titres et contractuelle). Voici les observations et conclusions de l'audit:

Stratégie informatique et gestion générale des systèmes;

Conformément à son manuel des opérations, une fois achevé, le SID offrira les fonctionnalités suivantes:

a) une gamme variée de calculs, tels que mise à jour de la valeur nominale, du prix unitaire, des encours (contractuels et de la dette), planification des financière des marchés, tarification et échéance des contrats et obligations;

b) une variété de recherches et de rapports de l'enregistrement de données et des résultats de calculs;

c) opérations financières, telles qu'émissions d'obligations, remboursements de contrats, rachats et transferts, entre autres;

d) registre d'informations utilisé dans sa pleine mesure par les différents modules de l'entreprise.

Au sujet de la stratégie informatique et de la gestion générale des systèmes, voici les principales observations et conclusions de l'audit:

- Il n'y a pas de programme de formation pour les systèmes de gestion de la dette publique les plus utilisés, Seorfi et SID;

- Il n'y a pas de date prévue pour la mise en œuvre intégrale du SID, y compris concernant la dette financière domestique ;

- Certaines opérations importantes telles que l'activation de contrats, les remboursements, les remboursements inverses, les modifications des taux d'intérêt ou de la valeur des contrats sont détenues par une seule personne. Il n'y a pas ni approbation et ni double conférence dans le système. La sécurité des opérations repose uniquement sur l'adéquation du profil, ce qui pose un problème de séparation de fonctions;

- Un autre problème de séparation de fonctions concerne le manque de personnel pour le développement du SID, ce qui fait que certains membres du personnel du DMO y travaillent en plus de leurs fonctions habituelles.

- L'évaluation de la vulnérabilité des risques opérationnels inhérente aux processus informatiques est prête, mais l'évaluation des mesures d'atténuation de ces risques n'a pas encore été effectuée.

Contrôles de sécurité et environnementaux

Au sujet des contrôles de sécurité et environnementaux, voici les principales observations et résultats de l'audit:

- Le DMO n'a pas nommé le Gérantresponsable de la sécurité de l'information et des communications et le Comité de sécurité de l'information, qui est responsable de la nomination du gérant de la SI, n'a pas commencé à travailler effectivement.

- Il n'y a aucun Plan de continuité (BCP) formalisé, et les processus de travail de gestion de la dette publique sont en cours de révision afin de préparer le BCP;

- Les analystes de l'équipe de vérification ont remarqué l'existence de trois profils d'utilisateurs génériques actifs, ce qui compromet les bonnes pratiques informatiques, en particulier l'article 11.2.1 de l'ISO/CEI 27002 : 2005, qui recommande l'utilisation de l'identification unique de l'utilisateur pour rendre compte des actions de chaque utilisateur du système;

- Bien que la définition de l'accès au SID doive se faire uniquement par le biais du certificat numérique A3, et que la possibilité d'accéder par numéro national d'identification et mot de passe soit une procédure exceptionnelle, l'analyse de la base de données des utilisateurs SID indique qu'il n'existe aucune date limite pour cette procédure exceptionnelle;

- L'analyse de la base de données des utilisateurs du SID indique une défaillance dans le processus de revue de l'accès des utilisateurs;

- L'équipe de vérification a aussi détecté des défaillances dans l'entretien automatique quotidien de routine de la base de données d'utilisateurs du SID;

- Le SID n'enregistre pas de pistes d'audit pour la plupart des transactions et, en conséquence, le DMO n'effectue pas un examen périodique des pistes d'audit générées par le système et ne surveille pas les transactions du SID;

- Le SID n'a pas une fonctionnalité d'audit pour générer, stocker et analyser régulièrement le journal du système.

- L'équipe de vérification a remarqué l'absence de plan de tests, et de ses résultats associés, pour les systèmes les plus utilisés par le DMO, le Seorfi et le SID

- L'équipe de vérification n'a pas reçu confirmation de la création effective d'une équipe pour répondre aux incidents des réseaux informatiques, et qui aurait la responsabilité de recevoir, examiner et répondre aux notifications relatives aux incidents de sécurité concernant les réseaux informatiques.

- L'équipe de vérification a remarqué l'absence d'un Plan de continuité des services informatiques. Il s'agit du document, correctement formalisé, qui décrit, de manière centralisée, les initiatives de continuité pour tous les services informatiques gérés par l'organisme ou entité.

Contrôles opérationnels et documentation;

Quant aux contrôles opérationnels et à la documentation, voici les principales observations et résultats de l'audit:

- L'interface n'est pas très conviviale et, de ce fait, le SID requiert une connaissance préalable importante de la part des utilisateurs sur le système;

- Il y a pas de manuel de l'utilisateur du SID;

- La vitesse de traitement des calculs demandés est faible. Cela empêche la génération de calculs et de rapports simultanément. Étant donné le nombre d'utilisateurs simultanés du système, ce problème pourrait réduire l'efficacité du système. L'équipe de vérification a suggéré au DMO d'évaluer les améliorations possibles afin d'augmenter la capacité de traitement du système.

CONTRÔLES DES APPLICATIONS

Les tests des contrôles de saisie, traitement et sortie sur le SID réalisés par l'équipe de vérification concernant la dette publique extérieure, ont conduit aux constatations et observations suivantes :

- Plusieurs messages d'erreur ne sont pas clairs et parfois n'apparaissent pas à l'utilisateur;

- Par le biais de tests de contrôles d'entrée de application, l'équipe de vérification a trouvé plusieurs messages d'erreur où la cause de l'erreur n'était pas expliquée;

- Par le biais de tests de contrôle de traitement de l'application sur la dette contractuelle, une différence de valeurs dans le rapport financier de flux de trésorerie, se référant à un remboursement qui n'était pas pris en compte dans ce rapport spécifique ;

- Quant aux tests de contrôle des sorties de l'application, si les données d'entrée ne sont pas correctes, l'application ne génère pas certains rapports de la dette contractuelle comme prévu, mais l'application n'identifie pas l'erreur de l'utilisateur;

- Par le biais de tests de contrôle de sortie de l'application, des erreurs ont été également identifiées dans les rapports de la dette contractuelle en raison de l'utilisation, par le système, d'indexes périmés;

- Certains rapports concernant la dette contractuelle ont été émis avec des informations incomplètes.

Recommandations

Compte tenu des constatations d'audit et des observations signalées, l'équipe de vérification a recommandé au Secrétariat de Trésor National d'élaborer, en 90 (quatre- vingt-dix) jours, un plan d'action contenant le calendrier pour la mise en œuvre de ce qui suit:

- Établir une échéance pour la mise en œuvre intégrale du SID, y compris la dette financière domestique ;
- Nommer le Gérant de la sécurité de l'information et des communications ainsi que le Comité de sécurité de l'information;
- Formaliser le Plan de continuité des opérations;
- Formaliser le Plan de continuité des services informatiques;
- Créer l'Équipe de réponse aux incidents des réseaux informatiques;
- Réaliser l'évaluation et l'atténuation des risques informatiques opérationnels;
- Réviser l'entretien automatique quotidien de routine de la base de données d'utilisateurs du SID;
- Réviser le processus d'évaluation de l'accès des utilisateurs au SID;
- Réviser le processus d'octroi d'accès aux utilisateurs du SID;
- Établir des procédures pour l'examen périodique des pistes d'audit générés par le SID;
- Fournir la journalisation des applications de la SID;
- Réviser les messages d'erreur SID;
- Développer le manuel de l'utilisateur du SID;
- Réviser la routine de rapports du SID.

FIGURE 2 : AUDIT DE LA DETTE PUBLIQUE PAR LES ISC : LE CAS DE LA MOLDAVIE

Évaluation des contrôles des applications réalisée par la Cour des comptes de la République de Moldavie

L'application SYGADE dispose de suffisamment de contrôles intégrés qui vérifient automatiquement si la saisie de données a été effectuée avec précision, pour être validée; cependant, il y a certains aspects qui posent des problèmes et doivent être résolus: les opérateurs ont la possibilité d'entrer des données dans les classificateurs du système et dans d'autres tables du système, ce qui peut affecter la précision et l'intégrité des données par duplication ou par suppression d'enregistrements.

Recommandation N° 15 : Réviser la possibilité de restreindre les droits des opérateurs pour saisir, modifier ou supprimer les données dans les classificateurs de base de données du SYGADE, ou inclure la possibilité d'identifier ces opérations afin d'exclure le risque de duplication de données ou d'entrée erronée.

Outre les rapports standards mis en place dans application du SYGADE, un grand nombre de rapports de nature générique ont été élaborés au moyen de l'application «Excel», y compris la plupart des aspects requis. Tous les types de rapports qui sont systématiquement utilisés. La plupart des rapports exigés sont développés en «Excel». Cependant, il y a certains rapports générés manuellement à partir de données obtenues d'autres rapports. La possibilité de renouveler les données dans les rapports d'«Excel» est préoccupante. La génération de rapports est une procédure assez compliquée, qui pourrait être considérablement affectée par le facteur humain. En outre, il se pourrait

que les rapports générés soient modifiés sans autorisation, et ces erreurs pourraient se produire dans d'autres rapports récapitulatifs importants, qui doivent avoir un maximum de sécurité car ils représentent le principal résultat de l'activité de la Division générale de la dette publique.

En conséquence, certaines lacunes mineures pourraient affecter gravement la fiabilité et l'exactitude des données des rapports importants sur l'activité de la Division générale de la dette publique.

Recommandation N° 16 : Envisager la possibilité d'optimiser ou d'automatiser le processus de modification des rapports à générer. Identifier la possibilité de générer automatiquement les rapports récapitulatifs, éliminant le facteur humain. Une occasion envisagée serait la possible migration vers la version 6.0.

BIBLIOGRAPHIE

Projet de recherche ASOSAI. Directives d'audit informatique, – 6 septembre 2003

Gallegos, Frederick. Senft, Sandra. Manson, Daniel P. Gonzales, Carol. Contrôle et Audit Informatique – Deuxième édition, Frederick Gallegos Auerbach. USA 2004

Bureau du Contrôleur et Vérificateur General des comptes de l'Inde, Audit Informatique – Principes généraux (Audit Informatique Séries Monographiques # 1)

Fonds monétaire international et Banque Mondiale. Lignes directrices pour la gestion de la dette publique. 1er avril 2014

Organisation internationale des institutions supérieures de contrôle. Principes de l'audit de performance ISSAI 300. Septembre 2019.

Organisation internationale des institutions supérieures de contrôle. Norme d'audit de performance ISSAI 3000. Septembre 2019

Initiative de développement de l'INTOSAI. WGTI – IDI Manuel d'audit informatique pour Institutions supérieures de contrôle des finances publiques, février 2014.

Parker, Xenia Ley. Audits des Technologiques de l'information. Parker, Xenia Ley. USA 2006

Département de la Sécurité intérieure des États Unis d'Amérique site web : http://www.dhs.gov.

« Accountability Office » États Unis d'Amérique. Manuel d'audit des contrôles des systèmes d'information du gouvernement fédéral, GAO-09-232 G. Février 2009.