ISSAI 5450

Die Internationalen Richtlinien der Obersten Rechnungskontrollbehörden, ISSAI, werden von der Internationalen Organisation der Obersten Rechnungskontrollbehörde, INTOSAI, herausgegeben. Weitere Information finden Sie unter *www.issai.org*

INTOSAI

Leitfadens zur Prüfung von Informationssystemen zur Verwaltung von Staatsschulden

Dezember 2016

PSC-Sekretariat
Rigsrevisionen • Store Kongensgade 45 • P.O. Box 9009 • 1022 Copenhagen K • Denmark
Tel.:+45 3392 8400 • Fax:+45 3311 0415 • E-mail: info@rigsrevisionen.dk

I N T O S A I

INTOSAI General Secretariat - RECHNUNGSHOF
(Austrian Court of Audit)
DAMPFSCHIFFSTRASSE 2
A-1033 VIENNA
AUSTRIA
Tel.: ++43 (1) 711 71 • Fax: ++43 (1) 718 09 69

E-MAIL: intosai@rechnungshof.gv.at
WORLD WIDE WEB: http://www.intosai.org

INTOSAI

Arbeitsgruppe für Staatsschulden

LEITFADEN ZUR PRÜFUNG VON INFORMATIONSSYSTEMEN ZUR VERWALTUNG VON STAATSSCHULDEN

Dezember 2016

INHALTSVERZEICHNIS

VORWORT

Sobald wir über die Verwaltung von Staatsfinanzen sprechen stehen die Staatsschulden im Zentrum der Diskussion. Die Stärkung der Wirtschaft und die Verbesserung der Sozialleistungen in ihren jeweiligen Ländern bringen die meisten Regierungen in große finanzielle Bedrängnis. Theoretisch sind Staatsschulden ein wirksames Instrument für wirtschaftliches Wachstum und für die gerechte Verteilung der Steuerlast auf die heutige und die zukünftigen Generationen von Steuerzahlern. Aufgrund ihrer Bedeutung für das wirtschaftliche Gleichgewicht ist es wesentlich die Staatsschulden mit großer Vorsicht zu messen und zu verwalten.

Hauptziel der Verwaltung der Staatsverschuldung ist es, die Aktivitäten der Regierung mit einer stabilen Finanzierung zu unterstützen, die so kostengünstig wie möglich und mit einem vernünftigen Maß an Risiko erhalten werden soll. Die Richtlinien des Internationalen Währungsfonds-Weltbank zur Verwaltung von Staatsschulden enthalten eine Reihe solider Praktiken in Bezug auf die internen Kontrollen des Schuldenmanagements. Unter anderen finden wir die Aussage, dass „Aktivitäten zum Management von Schulden von einem genauen und umfassenden Informationssystem mit sachgemäßen Schutzmaßnahmen unterstützt werden sollen.“ Länder, die sich um eine wirksame Verwaltung ihrer Staatsschulden bemühen, müssen der Entwicklung von vertrauenswürdigen Systemen zur Erfassung und Berichterstattung von Schuldeninformation hohe Priorität geben. Dies ist notwendig, nicht nur um Verschuldungsdaten zu erstellen und eine pünktliche Bezahlung zur Abtragung der Schulden zu sichern, sondern auch, um die Qualität der Haushaltsberichterstattung und die Transparenz des staatlichen Rechnungswesens zu verbessern, was es Politikern und Verwaltungsstellen für Staatsschulden ermöglicht, die Ziele bezüglich der Staatsschulden zu erreichen.

Wie man sieht, ist es das Ziel der Prüfung von Informationssystemen zur Verwaltung der Staatsschulden die Leistungsfähigkeit, Effektivität und Wirksamkeit der Verwaltung von Staatsschulden zu erhöhen. Aus diesem Grund soll die Prüfung als Wirtschaftlichkeitsprüfung eingestuft werden. Dennoch kann diese Arbeit auch im Zusammenhang mit Finanzprüfung von großer Bedeutung sein; diese konzentriert sich darauf festzustellen, ob die Finanzinformationen, die die Regierung erhält, den Richtlinien für die Präsentation von Finanzberichten entsprechen und ob sie vertrauenswürdig, frei von Betrug und fehlerlos sind. Diese Arbeit ist von großer Bedeutung, denn sie trägt dazu bei ein Informationssystem aufzubauen, das genaue und verlässliche Information zu einem der wichtigsten Elemente der Staatsfinanzen sammelt und produziert: den Staatsschulden.

Dieser Leitfaden will Rechnungsprüfern eine anschauliche Anleitung zur Prüfung von Informationssystemen zur Verwaltung von Staatsschulden geben. In Anbetracht der Tatsache, dass die Internationale Organisation der Obersten Rechnungskontrollbehörden (INTOSAI) schon über einige Dokumente verfügt, die sich auf die Prüfung von Informationstechnologien beziehen und von der Arbeitsgruppe für IT-Prüfung (WGITA) entwickelt wurden, konzentriert sich dieser Leitfaden auf

Anwendungskontrollen, die spezifisch für das Informationssystem zur Verwaltung von Staatsschulden konzipiert sein müssen.

LISTE DER ABKÜRZUNGEN

BCP (Englisch) – Planung von Geschäftskontinuität
CAAT (Englisch) - Computergestützte Prüfungstechnik
CS-DRMS (Englisch) – Schuldenerfassungs- und Managementsystem des Commonwealth-Sekretariats
DMFAS (Englisch) – Schuldenmanagement- und Finanzanalysesystem
DMO (Englisch) – Schuldenmanagementbehörde
DRP (Englisch) – Katastrophensanierungsplan
FMIS (Englisch) - Informationssystem zur Finanzverwaltung
IMF (Englisch) – Internationaler Währungsfond
INTOSAI – Internationale Organisation der Obersten Rechnungskontrollbehörden
IT (Englisch) – Informationstechnologien
ORKB– Oberste Rechnungskontrollbehörde(n)
PDMIS (Englisch) – Informationssystem zur Verwaltung von Staatsschulden
UNCTAD (Englisch) – Konferenz der Vereinten Nationen für Handel und Entwicklung
WGITA (Englisch) – Arbeitsgruppe für IT Prüfung
WGPD (Englisch) – Arbeitsgruppe für Staatsschulden

EINLEITUNG

Mit dem Mandat des Präsidiums der INTOSAI erhielt die Arbeitsgruppe für Staatsschulden (WGPD) die Aufgabe, Richtlinien und anderweitiges Informationsmaterial zu veröffentlichen, das von den Obersten Rechnungskontrollbehörden (ORKB) verwendet werden soll, um eine korrekte Berichterstattung und eine solide Verwaltung der Staatsschulden zu fördern.

Dieser Leitfaden ist bestrebt die Leistungsfähigkeit der Arbeitsgruppe für Staatsschulden (WGPD) durch Bereitstellung allgemeiner Rahmenbedingungen zu erhöhen, die bei Rechnungsprüfungen der ORKB verwendet werden können, um die allgemeinen Kontrollen und die Anwendungskontrollen des Informationssystems zur Verwaltung von Staatsschulden (PDMIS) zu bewerten. Es ist wichtig zu beachten, dass im Rahmen dieses Mandats unter PDMIS eines oder mehrere Informationssysteme zu verstehen sind, die beim Staatsschuldenmanagement verwendet werden.

Mit der stetigen Entwicklung von Informationstechnologien haben sich Regierungsorganisationen zunehmend dem Gebrauch von IT verschrieben, um ihre Geschäfte abzuwickeln und Dienstleistungen zu erbringen sowie um wesentliche Information zu verarbeiten, zu speichern und weiterzugeben. Nach einem IMF-Arbeitspapier, „bezieht sich FMIS (Informationssystem für Finanzmanagement) normalerweise auf die Computerisierung des Verwaltungsverfahrens für öffentliche Ausgaben mit der Aufgabe den Haushaltsplan zu erstellen, zu vollziehen und zu bilanzieren, und zwar mit Hilfe eines voll integrierten Finanzmanagementsystem der angeschlossenen Ministerien und anderer ausgabentätigenden Agenturen."

Das Institute of Electrical and Electronics Engineers (IEEE 1471) definiert Systeme als „eine Zusammenstellung von Komponenten, die auf eine Weise angeordnet sind, um eine bestimmte Funktion oder eine Reihe von Funktionen zu erfüllen." Die Hauptaufgabe eines Schuldenverwaltungssystems ist insbesondere, die Darlehensdatenbank für Staatskredite mit einer Software zu unterstützen, die es erlaubt Berichte abzufassen und analytische Funktionen der Schuldenmanagementbehörde (DMO) zu übernehmen.

Eine IT-Prüfung kann je nach vorherrschender Methode folgendermaßen eingestuft werden:

- IT-Governance;
- Datenprüfung;
- Prüfung des Informationssystems;
- IT-Vertragswesen; und
- Informationssicherheit.

Normalerweise arbeitet ein IT-Rechnungsprüfer mit mehr als einer Methode, doch er kann auch eine dominierende Methode wählen. In diesem Leitfaden ist die dominierende Methode die Prüfung des Informationssystems.

Die Struktur dieses Leitfadens umfasst die Planung und Bewertung allgemeiner Kontrollen und Anwendungskontrollen.

1. PLANUNG

Das Informationssystem zur Verwaltung von Staatsschulden kann als ein Satz voneinander abhängiger Teile (Physischer Strukturen, Personal, Technologien) angesehen werden, die interagieren, um Arbeitsvorgänge, die bei der Aufnahme, Erhaltung und Tilgung von Staatsschulden umgesetzt werden, aufzuzeichnen, zu kontrollieren, zu beurteilen und zu verwalten.

Diese Phase hilft dem Rechnungsprüfer die mit dem System verbundenen Arbeitsgänge, Kontrollen und Risiken zu verstehen, die sich aus den charakteristischen mit den Arbeitsabläufen zu Staatsschulden verbundenen Risiken ergeben. Mit diesem Verständnis bewertet der Rechnungsprüfer das gesamte Kontrollumfeld, identifiziert die in der Verwaltung der Staatsschulden verwendeten Systeme, inspiziert die gesamte Dokumentation dieser Systeme und erarbeitet eine vorläufige Risikobewertung. Das Ergebnis dieser Bewertung bestimmt das Ausmaß der Verfahren, die in der Testphase angewendet werden.

Die ORKB muss ebenso alle der Staatsschuldenbehörde unterliegenden Strukturen wie Personal, Prozess, Schuldenart, Datensicherheit, Technologien und anderes, untersuchen.

In dieser Phase sollte der Rechnungsprüfer eine vorläufige Bewertung der Struktur und des Arbeitsablaufes der Staatsschuldenbehörde vornehmen, die Folgendes beurteilt:

- wie das Informationssystem zur Verwaltung von Staatsschulden organisiert ist: welche Systeme zur Aufzeichnung, Verarbeitung, Berichterstattung, Kontrolle und Verwaltung der Staatsschulden verwendet werden und was die wesentlichen Prozesse und Funktionen sind, die jedes System ausübt;
- die interne Prüfungsfunktionalität;
- die Ergebnisse früherer Prüfungen (intern oder extern) des Informationssystems zur Verwaltung von Staatsschulden ;
- die physische Lagerung der Arbeitsdokumentation ;
- die Verwendung von Computer Hard- und Software und die Verantwortung für deren Instandhaltung;
- Tätigkeiten, die von Informationssystemen ausgeführt wurden und deren relative Bedeutung;
- wie sich die Beziehung zwischen den jeweiligen Informationskomponenten zu den Staatsschulden ergibt;
- Methoden und Verfahren zur Umsetzung neuer Tätigkeiten oder zur Revidierung existierender Tätigkeiten; ebenso
- vorherige Bewertungen der internen Kontrollen der DMO, Falls die internen Kontrollen früher nicht bewertet wurden, soll die ORKB diese Bewertung

durchführen. Dies ist sehr wichtig, um den Grad existierender Risiken beurteilen zu können und so die Prüfungen festzulegen, die umgesetzt werden müssen.

Die Ausgereiftheit des Systems hat keinen Einfluss auf die Bewertung der allgemeinen Kontrollen, die in jedem Fall durchgeführt werden soll. Allerdings bestimmt sie die zu realisierenden Prüfungsverfahren und gibt an, wie viele IT-Spezialisten nötig sind, um die Prüfungen umzusetzen. Es wird mindestens ein IT-Spezialist pro Team für alle Arbeiten mit Systembezug empfohlen. Jene Prüfer des Teams, die noch keine Erfahrung mit IT-Prüfungen haben, sollten in jedem Fall die üblichen technischen Begriffe erlernen. In diesem Falle ist ein fundiertes technisches IT-Wörterbuch eine sinnvolle Investition für die ORKB. *Information Systems Auditing – Glossary of Terms* der INTOSAI-Arbeitsgruppe für IT-Prüfung ist für diesen Zweck sehr nützlich. Folgende Online-Glossare können auch sehr hilfreich sein: http://www.webopedia.com oder http://whatis.techtarget.com.

Prüfer, denen die IT-Ausdrücke geläufig sind, müssen die Terminologie kennen, die die DMO verwendet, insbesondere Akronyme und Abkürzungen (Arten von Überschriften, Sektoren der DMO, Gläubiger, Namen der Systeme, der von der DMO verwendeten Software usw.). Es ist wesentlich, diese Kenntnisse zu haben bevor die Interviews durchgeführt werden. Ein sehr nützliches Glossar der Konferenz der Vereinten Nationen für Handel und Entwicklung (UNCTAD) kann unter folgenden Links gefunden werden:

- http://unctad.org/en/Docs/pogiddmfasm3r3.en.pdf – Debt and DMFAS Glossary (Englische Version)
- http://www.unctad.org/sp/docs//pogiddmfasm3r3.sp.pdf – Glosario de la deuda y del SIGADE (Spanische Version)

Um ein PDMIS im Detail zu verstehen, muss man den inhärenten Daten- und den Informationsfluss kennen. Deshalb ist es wesentlich, bei der Planung die Schlüsselprozesse in Bezug auf die Staatsschulden (Aufzeichnung, Verarbeitung, Kontrolle, Sicherheit, Berichterstattung und Analyse) abzubilden und zu verstehen, wie diese im Informationssystem umgesetzt werden. Anschließend muss eine Risikobewertung erfolgen, um höhere Risiken zu identifizieren, die im Zusammenhang mit Schüsselprozessen im Arbeitsablauf und bei der Verwaltung der Staatsschulden auftreten; dabei müssen deren Auswirkungen und Eintrittswahrscheinlichkeit berücksichtigt werden. Die Risikobewertung ist wichtig, um das Ausmaß der notwendigen Verfahren zu bestimmen und die damit verbundenen Risikoniveaus zu verwalten. Die *ISSAI 5410 Richtlinien zur Planung und Durchführung von Prüfungen der internen Revision der Staatsschuld* gibt Richtlinien zur Erstellung einer Risikobewertung. Zusätzlich könnte die Risikobewertung im Zusammenhang mit Finanzprüfungen gemacht werden.

Die Abläufe von PDMIS finden fast immer in der DMO statt. Andere Behörden können auch für die Eintragung von Verschuldungsdaten verantwortlich sein, grundsätzlich im Fall von Vertragsschulden. Falls die DMO in ein Back-, Middle- und Front-Office unterteilt ist, hat jede Kernfunktion ihre eigenen Daten- und Informationsflüsse. Das Front-Office ist typischerweise verantwortlich für die Umsetzung von Transaktionen auf Finanzmärkten, einschließlich der Verwaltung von Versteigerungen und anderen Formen von Anleihen, sowie von allen anderen Finanzierungsmitteln. Das Back-Office

befasst sich mit der Abwicklung von Transaktionen und mit der Überprüfung der Finanzberichte. Ein getrenntes, mittleres Büro für Risikomanagement macht normalerweise Risikoanalysen, überwacht und erstellt Berichte zu Portfoliorisiken und bewertet die Leistung von Schuldenmanagern in Bezug auf strategische Ziele und Maßtäbe. Das Back-Office verwaltet den Hauptdatenfluss in Bezug auf Staatsschulden, einschließlich externer Daten, und hat die Aufgabe den Dateneingang aufzuzeichnen und zu kontrollieren..

Da viele Länder für die Verwaltung von Staatsschulden ein Standardsystem verwenden, das drittseitig von internationalen Organisationen (z.B. DMFAS, CS-DRMS) entwickelt wurde und aktualisiert wird, ist die Verwendung von Berichten in Bezug auf Leistung, etwaige Entwicklungen, Anträge zur Systeminstandhaltung und Aufzeichnung von Vorfällen sehr wichtig.

Das von der UNCTAD entwickelte DMFAS-Programm konzentriert sich auf nachgeschaltete Aktivitäten. Hierzu gehören die Instandhaltung von Datenbanken, die Bestätigung von Verschuldungsdaten, die interne und externe Berichterstattung zu Schulden, Statistiken und grundlegende Analyse zu Schulden und der Aufbau von Systemverbindungen zwischen Schuldenmanagement und anderer Finanzsoftware. Diese Operationen werden ergänzt durch vorgelagerte Aktivitäten wie Analysen der Schuldentragfähigkeit, die von anderen Instanzen wie von der Weltbank geliefert werden. Zusätzlich hilft das Programm Ländern zunehmend Verbindungen zwischen dem DMFAS-System für Schuldenmanagement und anderer staatlicher Software herzustellen (z.B. für die Erstellung des Budgets, die Bargeldverwaltung und Verwaltung von Förderungen) oder innerhalb komplexer, integrierter Finanzmanagementsysteme als Teil der allgemeinen Bemühungen der öffentlichen Finanzverwaltung der Länder. Weitere Information finden Sie unter: http://unctad.org/dmfas.

Die CS-DRMS-Applikation, die vom Commonwealth-Sekretariat zur Verfügung gestellt wird, hilft bei der Aufgabe Schulden aus ganzheitlicher Perspektive zu erfassen, zu verwalten und zu analysieren. Sie bietet eine zentrale Sammelstelle für mehrere Kategorien staatlicher und privat gesicherter Auslands- und Inlandsschulden, einschließlich kurzfristiger Schulden. Das System handhabt auch Fördergelder, staatliche Kredite und On-Lending. Weitere Information finden Sie unter: http://www.csdrms.org.

Im Falle von Ländern, die das DMFAS oder CS-DRMS zur Verwaltung von Staatsschulden verwenden, können Prüfungsberichte des PDMIS, die von anderen Ländern (ORKB) erstellt wurden, zur Identifizierung der häufigsten und/oder folgenschwersten Mängel sehr nützlich sein.

Eine Tabelle der erforderlichen Informationen, Verfahren und Fragen, die von der ORKB zu beantworten sind und die vom Prüfungsteam bei der Planung der Prüfung des staatlichen Schuldensystems verwendet werden kann, ist in Anhang 1 zu finden.

2. ALLGEMEINE KONTROLLEN

Allgemeine Kontrollen bilden den Rahmen für umfassende Kontrollen von IT-Funktionen.[1] Diese Kontrollen sind darauf ausgelegt, Themen der Entwicklung, des Betriebs und der Instandhaltung des Umfelds anzusprechen. Ziele der allgemeinen Kontrollen sind die Datensicherung, der Schutz der Applikationsprogramme und die Gewährleistung, dass Computer auch im Falle von unerwarteten Unterbrechungen weiter betrieben werden können.

Obwohl eine Prüfung des Systems zur Verwaltung von Staatsschulden die Verifizierung der allgemeinen IT-Kontrollen erfordert, wird hier nicht weiter auf dieses Thema eingegangen, da Dokumente der INTOSAI zu IT-Prüfungen vorliegen, die allgemeine IT-Kontrollen im Einzelnen beschreiben.

Bei einer Systemprüfung wird empfohlen die *ISSAI 5310: Richtlinie für die Prüfung der Sicherheit der Informationsverarbeitung (ISec)* zu verwenden, einen Leitfaden zur Überprüfung der Sicherheit von Informationssystemen (ISS) in staatlichen Organisationen.

Ein anderes Dokument, das bei der Planung allgemeiner Kontrollen hilfreich sein kann, ist das WGITA-IDI Handbuch IT-Prüfung für ORKB, das wesentliche Information und Schlüsselthemen zur Verfügung stellt, die für eine wirksame Planung von IT-Prüfungen notwendig sind.

In Anhang II befindet sich eine Testmatrize mit einigen allgemeinen Kontrollen und Vorschlägen zu Prüfungsverfahren, die für die Rechnungsprüfer bei der Durchführung von allgemeinen Kontrollen nützlich sein können.

Ein umfassende Anzahl Aufzählung der verschiedener verschiedenen Kategorien der allgemeiner Kontrollen schließt die im Folgenden beschriebenen Posten mit ein:

Organisatorische Kontrollen

Organisatorische Kontrollen enthalten Praktiken, Verfahren und organisatorische Rahmenbedingungen, die eine solide Personalpolitik und Managementpraxis gewährleisten, sowie Aufgabentrennung und Regeln der Informationssicherheit, um Methoden zur Bewertung der Effektivität zur Verfügung zu stellen und operationelle Kontrollen und Leistungsfähigkeit gewährleisten.

Physische Zugangskontrollen

Physische Zugangskontrollen enthalten Regeln und Praktiken zur Verhinderung von unerlaubtem Zugriff auf und Störung von IT-Diensten; dazu gehören Verwaltungspraktiken, wie Identitätsabzeichen für das Personal, Besucherkontrollen, physische Maßnahmen, wie mechanische und elektronische Schlösser und Sperren,

[1] IDI-e-Learning-Kurs zur Prüfung der Verwaltung von Staatschulden, 6. Einheit: Prüfung von Informationssystemen zur Verwaltung von Staatschulden.

Kameras sowie andere Mittel zur Begrenzung des physischen Zugangs zu Servern und anderer kritischer Infrastruktur.

Logische Zugriffskontrollen

Logische Zugriffskontrollen verwenden die in Rechnersystemen eingebauten Sicherheitsmaßnahmen zur Vermeidung von unerlaubtem Zugriff auf sensible Dateien und Daten und, um zu gewährleisten, dass die Zugriffsrechte aller Benutzer auf ihre Arbeitsanforderungen beschränkt bleiben. Die Firewall, Antiviren- sowie Intrusion- und Malware-Detection-Programme gehören zu diesen Kontrollen.

In modernen Systemen stehen diese Kontrollen in allen möglichen Formen zu Verfügung. Sie werden mit der Applikationssoftware, dem Betriebssystem, dem Datenbankmanagementsystem, der Software für Zugriffkontrolle, mit Monitoren zur Online-Transaktionsverarbeitung (OLTP), mit Servern, dem Netzwerk, dem LAN und möglicherweise mit anderer Software [2] implementiert.

Umweltkontrollen

Umweltkontrollen sind Regeln, Praktiken und Konstruktionen zur Schadensvorbeugung durch Stromschwankungen, Feuer, Staub, Wasser, Lebensmittel, extreme Temperaturen oder Feuchtigkeit und statischer Elektrizität.

Obwohl sich diese Kontrollen auf die Datenbank konzentrieren (oder auf den Bereich für IT-Technologien, die eine spezifische Umgebung oder zumindest Schutz vor Diebstahl benötigen), sind sie auch auf alle anderen Büroräume anwendbar.

Kontrollen zur Programmänderung

Kontrollen zur Programmänderung enthalten Regeln, die gewährleisten, dass alle Änderungen der Systemkonfiguration präzise, umfassend und rechtzeitig gemacht werden.

Aktualisierungen und Änderungen sollten nach einem formalen Prozess durchgeführt werden, um die Protokollierung aller Änderungen zu gewährleisten und die Möglichkeit zu geben, den Prozess rückgängig zu machen, falls Probleme mit der neuen Version auftreten.

Bevor Programme aus der Testphase in die Produktionsbibliothek übergehen, soll eine formale Genehmigung eingeholt werden; das gesamte System, die Operationen und die Programmdokumentation sollen vollständig und auf dem neuesten Stand sein sowie den geltenden Normen, Richtlinien und Verfahren entsprechen.

Planung von Geschäftskontinuität und Katastrophensanierungsplan

Das Ziel bei der Planung von Geschäftskontinuität (BCP) und dem Katastrophensanierungsplan (DRP) ist Verfügbarkeit. Notfall- und

[2] Information Technology Audits , Xenia Ley Parker

Katastrophensanierungsplanung, Realisierbarkeit, Erprobung, Überwachung und die Notwendigkeit kontinuierlicher Aktualisierung der Pläne sind dabei kritische Faktoren.[3]

BCP ist ein Gesamtkonzept von Alternativen um bei Notfällen, Katastrophen oder anderen Störungen entscheidente Geschäftsprozesse aufrecht zu erhalten. Hierbei geht es um das Überleben des gesamten Betriebes und nicht nur um das der IT. Der Gesamtplan muss jedoch auch den Anforderungen des Informationssystems und des Telekommunikationsnetzes gerecht werden. Dieser Teil des BCP ist ein DRP.

Der BCP und der damit zusammenhängende DRP können gleichzeitig entwickelt werden, damit alle Aspekte gleichzeitig beachtet werden. Der Plan muss mindestens Verfahren und Kriterien enthalten, die festlegen, wann eine Situation eine Katastrophe ist; wer berechtigt ist solch eine Entscheidung zu treffen; und wie ein Ereignis formal zum Katastrophenfall zu erklären und der Plan in die Praxis umzusetzen ist.

[2] Information Technology Audit, Xenia Ley Parker

[3] Information Technology Audit, Xenia Ley Parker

3. APPLIKATIONSKONTROLLEN

Applikationskontrollen sind in Applikationen für Informationssysteme automatisch integriert, um die Autorisierung, Integrität, Genauigkeit und Gültigkeit der Arbeitsvorgänge zu gewährleisten. Sie sind in das Applikationsprogramm integriert und bestimmen die Eingabe, Verarbeitung und Ausgabe durch die Applikation. Ihr Ziel ist es die Vollständigkeit, Verlässlichkeit und Genauigkeit der Datenverarbeitung zu garantieren.

Beispiele von Applikationskontrollen sind Kontrollen des eingegebenen Datenformats, um möglichen ungültigen Daten vorzubeugen, Verarbeitungskontrollen, die verhindern, dass Benutzer Arbeitsvorgänge durchführen, für die keine Autorisierung vorliegt, und umfassen außerdem die Erstellung ausführlicher Berichte und Kontrollen zu den gesamten Arbeitsvorgängen, um zu gewährleisten, dass alle Arbeitsvorgänge in ihrer Gesamtheit und im Einzelnen registriert werden.

Anwendungskontrollen können folgendermaßen eingestuft werden:

- Eingabe
- Verarbeitung; und
- Ausgabe.

3.1. DOKUMENTATIONSNORMEN

Dokumentationsnormen gewährleisten eine angemessene und aktuelle Applikationsdokumentation. Wichtig ist es, die Dokumentation sorgfältig zu aktualisieren.[4]

Eine ordnungsgemäße Dokumentation ist wesentlich, um besser zu verstehen, welche Kontrollen durchgeführt werden oder werden sollten.

Eine gute Applikationsdokumentation reduziert das Risiko, dass Nutzer gegen die vom Management bestimmten Kontrollverfahren verstoßen. Die Überprüfung einer umfassenden und aktuellen Dokumentation hilft dem Prüfer zu begreifen, wie jede Applikation funktioniert und kann dazu beitragen bestimmte Prüfungsrisiken zu identifizieren.

– Applikationsdokumentation: hilft Wartungsprogrammierern die Applikation zu verstehen, Probleme zu korrigieren und Verbesserungen vorzunehmen. Die Dokumentation optimiert jede Phase des Entwicklungsprozesses und kann in verschiedenen Formaten, wie in Flussdiagrammen, Grafiken, Tabellen oder mittels Text gestaltet werden. Die Dokumentation folgendes enthalten: Datenherkunft, Datenattribute, Bildschirme zur Dateneingabe, Datenvalidierung, Sicherheitsverfahren, Berechnungsbeschreibung, Programmdesign, Schnittstellen zu anderen Applikationen, Kontrollverfahren, Fehlerbehandlung, Bedienungsanleitungen, Archiv, Sicherungskopie, und Speicherungs- und

[4] IT Prüfung – Allgemeine Richtlinien (IT-Prüfung Monografie Serie # 1) – Office of the Comptroller und Auditor General, Indien

Wiederherstellungsverfahren. Die Applikationsdokumentation soll aktualisiert werden sobald die Applikation modifiziert wird.

– Benutzerdokumentation: soll sowohl den automatischen wie den manuellen Arbeitsablauf beschreiben, um die Einarbeitung in die Applikation zu unterstützen und als fortlaufende Referenz zu dienen. In beiden Fällen soll die Nutzerdokumentation aktualisiert werden, sobald die Applikation modifiziert wird.

Die Dokumentation soll enthalten:

- Applikationsübersicht;

- Beschreibung der Benutzeranforderungen;

- Liste und Programmbeschreibung;

- Beschreibung von Eingabe/Ausgabe;

- Beschreibung des Dateieninhalts;

- Bedienungsanleitung;

- Instruktionen zum Arbeitsplatz;

- Beschreibung der Sicherheitskontrollen der Applikation;

-aktuelle Zusammenfassung der Sicherheitsbewertung ;

- letzte Entscheidung bzgl. Sicherheit und empfohlene Maßnahmen; und

- Status in Bezug auf die empfohlenen Maßnahmen.

3.2. EINGABEKONTROLLE

Eingabekontrolle ist extrem wichtig zur Reduzierung von Fehlern und Betrugsrisiken in computerisierten Applikationen. Die Eingabekontrolle ist wesentlich für die Datenintegrität.

Eingabekontrolle gewährleistet die Autorisierung, Genauigkeit, Vollständigkeit und Aktualität der in eine Applikation eingegebenen Daten. Autorisierung wird gewährleistet, da ab einer definierten Schwelle eine zweite Genehmigung des Arbeitsvorgangs erforderlich ist. Genauigkeit wird durch Bearbeitungskontrollen gewährleistet, die eingegebene Daten validieren bevor der Arbeitsvorgang zur Verarbeitung freigegeben wird. Vollständigkeit wird mittels Fehlerbehandlungsverfahren gewährleistet, die Protokollierung, Berichterstattung und Fehlerberichtigung ermöglichen. Aktualität ist gewährleistet durch Überwachung der Arbeitsabläufe, Protokollierung und Berichterstattung von Ausnahmen.

Eingabekontrolle kann es geben bei:

- Bildschirme zur Dateneingabe;

- Datenvorbereitungsverfahren;

- Genehmigung von Dateneingabe;

- Speicherung von eingegebenen Dokumenten;

- Validierung von eingegebenen Daten;

- Verfahren zur Fehlererkennung bei der Dateneingabe; und

- Stützmechanismen bei der Dateneingabe.

Die oben genannten Kontrollen können umgangen werden, falls es möglich ist Daten außerhalb der Applikation einzugeben oder zu modifizieren. Es sollen automatische Integritätskontrollen der Applikation existieren, die jede extern vorgenommene externe Datenmodifizierung entdecken und melden. Beispielsweise sollten Kontrollen existieren, um unerlaubte Veränderungen der zu Grunde liegenden Datenbank festzustellen und zu melden.

Bildschirme zur Dateneingabe

Genormte Dateneingabebildschirme können eine stabile Dateneingabe gewährleisten.

Das PDMIS kann folgende Funktionen enthalten:

- Dateneingabebildschirme in Standardform und Standardlayout;

- Dateneingabefelder können beschränken, was Benutzer eingeben dürfen;

- Pflichteingabe für gewisse Felder; und

-eine Hilfsfunktion (z.B. F1), um Benutzer beim Ausfüllen von Dateneingabefeldern zu unterstützen

Datenvorbereitungsverfahren

Ziel der Datenvorbereitungsverfahren ist die Fehlervermeidung bei der Dateneingabe.

Das PDMIS kann folgende Funktionen enthalten:

-eingebaute Prozesse zur gemeinsamen Datennutzung, um Daten in andere Applikationen zu übertragen.

Genehmigung von Dateneingabe

Ziel der Genehmigung von Dateneingabe ist es, zu gewährleisten, dass alle Dateneingaben von der zuständigen Person aufgezeichnet und autorisiert wurden.

Das PDMIS kann folgende Funktionen enthalten:

-Der Zugang zum PDMIS erfordert ein Passwort;

-bei manueller Dateneingabe die Aufzeichnung des Zugangsprotokolls; und

-gewisse kritische Operationen erfordern zwei Genehmigungen (z.B. Vertragsaktivierung, Modifizierung des Zinssatzes oder des Vertragswerts).

Speicherung von eingegebenen Dokumenten

Dieser Teil der Eingabekontrolle bezieht sich auf die Instandhaltung und Kontrolle von Originaldokumenten, die Schuldendatenaufzeichnung unterstützen. Bei automatischer Übertragung von Dateien zwischen Applikationen muss das PDMIS die Originaldaten, die sie von der anderen Applikation erhalten hat, für einen vom DMO festgelegten Zeitraum speichern.

Validierung von eingegebenen Daten

Datenvalidationskontrollen gewährleisten, dass die Dateneingabe gültig und genau ist.

Das PDMIS kann folgende Funktionen enthalten:

-automatische Checklisten zur Überprüfung fehlender Werte (z.B. beim Herunterladen einer historischen Serie von Verzeichnissen prüft das PDMIS ob ein täglicher, monatlicher oder jährlicher Wert fehlt.)

-

-alle Bildschirme zur Dateneingabe identifizieren erst dann klar die Pflichtfelder und die Bestätigung der Applikationsgenehmigung der Operation, wenn alle Pflichtinformationen eingetragen sind;

-jede Datenbanktabelle muss eine spezifische Regel enthalten, die festlegt, auf welchen Feldern eine Datenduplikation nicht gestattet ist;

-wenn die Applikation merkt, dass doppelte Daten eingegeben werden, wird sie die Eingabe verweigern bis die Verdoppelung eliminiert worden ist.

-die Applikation erlaubt keine Modifizierung gewisser Daten nach ihrer Eingabe. (z.B. den Wechselkurs am Operationstag). In Bezug auf andere Daten könnte die Applikation unter gewissen Bedingungen eine Veränderung erlauben (z.B. sobald der Vertragszustand als „Gesperrt" oder „Abgeschlossen" definiert ist, können keine Daten mehr verändert werden.)

-einige Felder verlangen beim Ausfüllen, dass weitere Felder ausgefüllt werden. (z.B. wenn der Benutzer die Gebühr für die Vertragszusage einträgt muss er auch die entsprechende Steuer eingeben);

-als allgemeine Kontrollen eines Schuldenvertrages sind die „Datums"-Felder wesentlich. Sie sind besonders nützlich bei der Ratenkalkulierung, um Zahlungsverzögerungen zu vermeiden, Strafen zu verhängen, usw. Aus diesen Gründen muss die Applikation Grundregeln aufweisen, wie das „Datum" einzutragen ist.

-mit Ausnahme von simulierten Arbeitsvorgängen erlaubt es das Applikationssystem erlaubt keine Registrierung von Daten für ein zukünftiges Datum. Zum Beispiel: Auszahlung, Auszahlungsumkehr, Vertragsrücktritt und Vertragsadditiv.

Fehler bei der Dateneingabe

-Ein Prüfprotokoll ist ein für die Sicherheit wesentlicher chronologischer Bericht, eine Reihe von Berichten oder ein Ziel und eine Quelle von Berichten, die Beweismaterial für

eine Folge von Aktivitäten liefern, welche zu irgendeinem Zeitpunkt eine bestimmte Operation, ein Verfahren oder ein Ereignis beeinflusst haben. Protokolldateien sollen nur dem zuständigen Personal zur Verfügung stehen.

Das PDMIS kann folgende Funktionen enthalten:

-Die DMO soll die Verantwortung für in der Schwebe stehende Dateien festlegen;

-Programme zur Protokollierung von Fehlern, zur Berichterstattung von offenen Fehlern und zur Aufzeichnung von Fehlerkorrekturen sollen in die Applikation integriert sein;

-

-sobald die Applikation beim automatischen Herunterladen von Daten eine Lücke in den Datenserien entdeckt, wird ein automatisches E-Mail zum Follow-up an die zuständigen Benutzer geschickt; und

-die Applikation soll periodische Berichte von ungelösten Fehlern, priorisiert und datiert, an das zuständige Personal schicken.

Stützmechanismen bei der Dateneingabe

Diese Kontrollen stehen in Beziehung zu unterstützenden Maßnahmen der DMO, die den Benutzern helfen, Daten in die Computerapplikation einzugeben, die Applikationen neu zu starten und die Nutzeraktivitäten zu überwachen, um mögliche Abweichungen von den festgelegten Richtlinien zu vermeiden.

Diese Mechanismen sind oft in den allgemeinen Kontrollen enthalten.

3.3 VERARBEITUNGSKONTROLLE

Die Verarbeitungskontrolle gewährleistet die Genauigkeit, Vollständigkeit und Aktualität der Daten bei Stapel- oder Online-Verarbeitung. Diese Kontrollmechanismen gewährleisten, dass die Daten in der Applikation exakt verarbeitet werden und dass keine Daten bei der Verarbeitung hinzugefügt, verloren oder verändert werden. [5]

Vollständigkeit

Vollständigkeit kann bei der Stapelverarbeitung gewährleistet werden, indem man die Arbeitsvorgänge, die von einem System erhalten werden mit denen abgleicht, die von einem untergeordneten System geschickt werden.

Der Abgleich soll zwischen Applikationen gemacht werden, die gemeinsame Daten verwenden; hierbei soll ein Vergleichsbericht erstellt werden, der die Daten beider Applikationen enthält und eine Benutzergruppe über alle Unterschiede informiert.[6]

Der Summenabgleich soll einen Postenzähler und Gesamtsummen aller Mengenfelder für jeden Arbeitsvorgang enthalten sowie Querfußsummen für Detailfelder bis zu Gesamtfeldern.[7]

In Dateien ohne aussagekräftige Summen können Prüfsummen gemacht werden, die alle Zahlen in einer Spalte addieren, um zu bestätigen, dass die gleiche Summe im

[5] Information Technology Control and Audit – Zweite Ausgabe, Frederick Gallegos

[6] Information Technology Control and Audit – Zweite Ausgabe, Frederick Gallegos

[7] Information Technology Control and Audit – Zweite Ausgabe, Frederick Gallegos

nächsten Prozess verwendet wird. Zum Beispiel ist die Summe der Schuldenvereinbarungszahlen nicht aussagekräftig, doch kann sie verwendet werden, um zu bestätigen, dass alle richtigen Schuldenvereinbarungszahlen verarbeitet wurden.[8]

Das PDMIS kann folgende Funktionen enthalten:

-Wenn an der Schnittstelle mit anderen Systemen zwischen Applikationen ein Dateienverarbeitungsfehler auftritt, wird eine Fehlerdatei generiert, die in der Systemapplikation aufgezeichnet wird. Entwickeln Sie für technische Profile und Schulungen eine stärkere Interoperabilität;

-Für viele Aufgaben enthält die Applikation geplante Stapelverarbeitungsaufträge. Zum Beispiel Lagerbestandsaktualisierung, Finanzplanung, Indexe, zukünftige Zahlungen, u.s.w. Überprüfen Sie die die Ausgabe weicher Echtzeitsysteme mit Fokus auf batch-basierte Protokolle, wie auch die harte Echtzeitkapazitäten zur Messung der aktuellen Informationsverarbeitung;

-Wenn bei der Stapelverarbeitung ein Fehler auftritt, informiert die Applikation den Benutzer mittels einer Nachricht. Bestätigen Sie, dass die Konsolidierungsfähigkeiten innerhalb des Systems den Fehlerkorrekturvorschriften und Bildkontrollprozeduren entsprechen.

-Nach Abschluss der Operation zeigt die Applikation eine Erfolgsbestätigung der Verarbeitung und eine Zusammenfassung der eingegebenen Daten an.

-Nach Modifizierung von bereits eingegebenen Daten zeigt die Applikation, eine Erfolgsbestätigung der Modifizierung und eine Zusammenfassung der geänderten Daten an.

-Nach der Löschung von bereits eingegebenen Daten zeigt die Applikation eine Erfolgsbestätigung der Löschung und eine Zusammenfassung der gelöschten Daten an.

-Wenn die Datenlöschung die Integrität der Datenbank beeinflusst, erlaubt die Applikation die Löschung nicht und meldet, dass die Aufzeichnung nicht gelöscht werden kann. Beispielsweise können die Daten einer Kreditgeberbank können in der Kreditgebertabelle nicht gelöscht werden, wenn der Kreditgeber aktive Verträge in der Applikation hat; und

-Die Applikation prüft gelegentlich die Übereinstimmung von Daten des Front- und Back-Office. Sie verlangt z. B. vom Back-Office die Bestätigung von Eingangsdaten von Versteigerungen. Prüfen Sie Mitteilungen auf Wechselbeziehungen der Datenarchitektur von Komponenten und Systemen, um zu bestätigen, dass die Datenströme dem Interoperabilitätsdiagramm entsprechend verlaufen.

3.4. AUSGABEKONTROLLE

Die Ausgabekontrolle gewährleistet die Ausgabeintegrität und die richtige und pünktliche Verteilung der erzeugten Ausgabe.[9] Verarbeitungsschwächen können manchmal durch eine starke Ausgabekontrolle kompensiert werden. Eine ausreichend kontrollierte

[8] Information Technology Control and Audit – Zweite Ausgabe, Frederick Gallegos

[9] Information Technology Control Audit – Zweite Ausgabe, Frederick Gallegos

Applikation für Eingabe und Verarbeitung wird wahrscheinlich völlig unterminiert,[10] wenn die Ausgabe nicht kontrolliert wird.

Die Vollständigkeit und Integrität von Ausgabeberichten hängen davon ab, dass Möglichkeiten zur Abänderung der Ausgabe begrenzt und Vollständigkeitstests wie Seitenzahlen und Prüfsummen eingeführt werden.[11]

Ausgabedateien sollten geschützt werden, um das Risiko unerlaubter Modifizierungen zu reduzieren. Mögliche Beweggründe für die Änderung von Computerausgaben sind unter anderem die Verschleierung nicht autorisierter Verarbeitungsprozesse oder die Manipulation unerwünschter Finanzresultate.[12]

Die Ausgabe einer IT-Applikation kann die Eingabe für eine andere Applikation sein. Hierbei soll der Prüfer auf Kontrollen achten, die gewährleisten, dass die Ausgaben exakt von einer Verarbeitungsstufe zur nächsten transferiert werden.[13]

Im PDMIS kann auch eine Ausgabekontrolle programmiert werden, um kritische Information zu identifizieren, die vom Staatsschuldenmanagement vorranging behandelt werden muss. Zum Beispiel bei Verträgen, die im aktuellen Monat ablaufen, kann die Applikation täglich Warnmeldungen von Verträgen, deren Zahlungsfrist in den nächsten fünf Tagen abläuft, auf dem ersten Systembildschirm anzeigen.

Die Applikation kann auch gewissen Benutzerprofilen erlauben Berichte im Vorrangmodus zu verfassen; so kann die Applikation festlegen, welche Berichte prioritär behandelt werden müssen.

Das PDMIS kann folgende Funktionen enthalten:

-den automatischen Vergleich der Summe der Ursprungsdaten mit der Summe der verarbeiteten Daten;

-die Applikation soll Benutzer über den Status von Berichterstellungsanträgen informieren, zum Beispiel, „nicht begonnen", „im Gange" und „beendet"; und

-am Ende des Berichterstellungsprozesses benachrichtigt die Applikation den Benutzer, der den Antrag gestellt hat, dass die Aufgabe beendet ist.

3.3. PRÜFUNG DER APPLIKATIONSKONTROLLE

Sobald Kontrollmechanismen identifiziert worden sind, ist der nächste Prüfungsschritt die Bestätigung ihrer Wirksamkeit.

[10] IT-Prüfungsrichtlinien, ASOSAI

[11] Informationstechnologieprüfung – Richtlinien (IT-Prüfung Monografie Serie # 1) – Office of the Comptroller und Auditor General, Indien

[12] Informationstechnologieprüfung – Richtlinien (IT-Prüfung Monografie Serie # 1) – Office of the Comptroller und Auditor General, Indien

[13] Informationstechnologieprüfung – Richtlinien (IT-Prüfung Monografie Serie # 1) – Office of the Comptroller und Auditor General, Indien

Das kann durch Folgendes erreicht werden:

-Eingabe einer Reihe von Testdaten die bekannte Resultate ergeben, wenn die Applikation richtig funktioniert;

-Entwicklung unabhängiger Programme, um die Applikationslogik nachzuahmen.

-Auswertung der Ergebnisse der Applikation.

Die oben angegebenen Verfahren prüfen die Integrität eines in das PDMIS eingebauten Programmes und nicht die Datenintegrität.

Wenn die Applikation über ein Testumfeld verfügt, kann dieses verwendet werden, um die Kontrollmechanismen zu überprüfen, doch nur dann, wenn das Testumfeld eine bestätigte Kopie des Produktionsumfeldes ist.

Um Kalkulationsregeln zu testen, wie die, die sich auf die Aktualisierung von Lagerbeständen oder von Schuldendiensten beziehen, muss der Prüfer möglicherweise Computergestützte Prüfungstechniken (CAAT) verwenden, die viele Instrumente und Techniken enthalten, wie allgemeine Prüfungssoftware, Anwendungssoftware, Testdaten, die Rückverfolgung und Abbildung der Applikationssoftware und Applikationen für Prüfungsspezialisten. Sie können Instrumente zur Analyse der Kalkulationstabellenlogik auf Genauigkeit enthalten. Instrumente können auch zur Analyse von Datenbankapplikationen oder zur Erstellung eines logischen Flussdiagramms verwendet werden. Allgemeine Prüfungssoftware kann verwendet werden, um Daten zu analysieren, die von den meisten Applikationen produziert werden.

Der Prüfer sollte abwägen, ob die Verwendung von CAAT notwendig ist. Diese Prüfungstechniken sollten je nach Komplexität der Staatsschuldenapplikation verwendet werden.

Dieses Dokument enthält eine vorgeschlagene Testmatrize (Anhang III), die vom Prüfungsteam als Referenz zur Revision der Applikationskontrollen verwendet werden kann. Diese Matrize identifiziert einige Anforderungen und Funktionalitäten, die das Staatsschuldensystem zur Verfügung stellen sollte, Anfragen, die es ermöglichen sollte, sowie die minimalen Anforderungen an die Kapazitäten solcher Systeme.

Da die Verschuldung jedes Landes unterschiedliche Zusammensetzungen und Merkmale aufweist, verfügen sicherlich auch die Schuldenmanagementsysteme über verschiedene Eigenschaften. Deshalb ist das Prüfungsteam verantwortlich dafür, jene Punkte zu identifizieren, falls notwendig anzupassen und zu verwenden, die für die Prüfung der Schuldensysteme ihrer Länder anwendbar sind.

3.6. BERICHTERSTATTUNG ÜBER DIE PRÜFUNGSERGEBNISSE

Die Berichterstattung des Informationssystems des Staatsschuldenmanagement muss der *Deklaration von Lima über die Leitlinien der Finanzkontrolle* und muss, falls angebracht, den Anforderungen der *ISSAI 5440 – Leitfaden zur Durchführung von Prüfungen der Staatsverschuldung – Vertiefte Prüfungen bei Finanzkontrollen, 2.6 Berichterstattung über die Prüfungsergebnisse* entsprechen.

Wie bereits erwähnt, ist diese Revision eine Wirtschaftlichkeitsprüfung. Deshalb ist es wichtig, dass der Bericht den Berichterstattungsnormen von Wirtschaftlichkeitsprüfungen entspricht, die in *ISSAI 3000 - Grundsätze für die Durchführung von Wirtschaftlichkeitsprüfungen* (Teil 5) und *ISSAI 300 – Allgemeine Grundsätze der Wirtschaftlichkeitsprüfung (Seite 19)* angegeben werden.

Anhang I: Planungstabelle

Erforderliche Information, Dokumente und Berichte
- Bestandsaufnahme der von der DMO verwendeten Informationssysteme und diesbezügliche Systemdokumentation; - Bestandsaufnahme der von der DMO verwendeten Rechner- und Netzwerkbetriebssysteme ; - Aktualisierte Darstellung der Prozessströme der DMO; - Vorherige Prüfungsberichte über die DMO; - Vorherige Prüfungsberichte, bezogen auf IT-Schuldensysteme; - Gesetze und Vorschriften bezogen auf den DMO-Rahmen und deren Verwaltung von Staatsschulden; - Eine Liste der DMO-Manager und des IT-Managements, des Managements für Geschäftskontinuität, des Personalmanagements, des Risikomanagements, der internen Rechnungsprüfung und anderer Konzepte, sowie deren Rollen, Adressen, E-Mail-Adressen und Telefonnummern; - Dokumente, die die Funktionalität der DMO und/oder ihrer Systeme als schriftliche Leitfäden zu Richtlinien und Verfahren der DMO oder des Finanzministeriums demonstrieren: • Personalmanagement • Informationssicherheit • Management von Veränderungen • Physischer Zugang • Anforderungen an das IT-Umfeld/den Standort • Logischer Zugriff • Geschäftskontinuitätsplanung (BCP) • Katastrophensanierungsplan (DRP) • Backup-Plan • Service von dritter Seite (IT-Service) • Berichte vorheriger Risikobewertungen • Aktuelle Zusammenfassung von Sicherheitsbewertungen • Aktuelle Sicherheitsentscheidungen und empfohlene Maßnahmen • Status der empfohlenen Maßnahmen • Genehmigung der Geschäftsleitung zur Systembereitstellung - Berichte, die von Instanzen außer Haus verbreitet werden und deren Aufgabe die Systeminstandhaltung ist; - Andere Dokumente zusammenhängend mit der Staatsschuldenmanagementbehörde und/oder ihrer Systemen (Folien, Texte, Ziele und jährliche Schuldenmanagementberichte); - Anzahl der DMO Angestellten, die das System verwenden und ihr Zugriffsprofil;

- Anzahl der IT-Angestellten und Stellenbeschreibung (Rollendefinition) der DMO und des IT-Personals;
- Liste der Angestellten, die Zugang zum Serverraum haben;
- Beschreibung des Zugriffsprofil auf das PDMIS;
- Formelle Angaben der Form und Periodizität mit der das Betriebssystem, die Firewall und Antivirus-Programme aktualisiert werden;
- Die Rolle physischer Hindernisse und automatischer Instrumente, die verwendet werden, um unerlaubten Zugang zum Großrechner, zu Arbeitsplätzen, Servern und anderen DMO-Einrichtungen zu verhindern;
- Die Lage jeden Raumes innerhalb und außerhalb der DMO;
- Eine Mengenliste von: Personal, Arbeitsplätzen, Servern;
- Höhe der Budgetzuweisung in den letzten 5 Jahren;
- Liste früherer Weiterbildungen zur Verwendung des PDMIS (DMO-Personal) und zur Aktualisierung der IT (IT-Personal);
- Erklärte Regeln, Praktiken und bauliche Beschreibungen, um Schäden durch Stromschwankungen, Feuer, Staub, Wasser, Lebensmittel. extreme Temperaturen oder Feuchtigkeit und statische Elektrizität vorzubeugen.
- Funktionsbeschreibung einer unterbrechungsfreien Stromversorgung (falls vorhanden);
- Zwischenfallsprotokoll von PDMIS-Fehlern oder Einschulungen auf Wunsch der DMO.
- Protokoll von Sicherheitszwischenfällen;
- Liste der Änderungen des PDMIS-Programmes in den letzten 12 Monaten;
- Protokolle und Berichte früherer BCP- und DRP-Tests und tatsächlicher Ereignisse;
- Applikations- und Nutzerdokumentation;
- Nutzungsbegriffe jeder Applikationen;
- Handbuch über die Verfahren zur Behandlung von Prozessfehlern;
- Datenproben, um Operationen zu wiederholen und so die Applikationskontrollen und Berechnungen zu testen.

Verfahren

- Studium der Systemdokumentation (Handbücher und Nutzungsbedingungen) zur Kenntnis der wesentlichen Schuldenprozesse, die vom Informationssystem umgesetzt werden. Ist die vorliegende Dokumentation von DMO Verfahren unzureichend, sollte das Prüfungsteam sie untersuchen und aufzeichnen;

- Bestätigung des Bestehens von rechtlichen Regeln für Gebrauch, Instandhaltung und geschäftliche Verwaltung des Staatsschuldeninformationssystems;
- Ermittlung von Befunden in vorherigen Prüfungen, die sich auf Schwachstellen des operativen Staatsschuldenflusses und/oder Staatsschuldenmanagementsysteme beziehen;
- Identifizierung der wesentlichen allgemeinen Kontrollen mithilfe der Systemdokumentation;
- Identifizierung der wesentlichen Applikationskontrollen mithilfe der Systemdokumentation: Dateneingabekontrolle, Verarbeitungskontrolle und Ausgabekontrolle;
- Durchführung einer Risikobewertung in Bezug auf die wichtigsten allgemeinen und Applikationskontrollen, um festzustellen, welchen Risiken diese Systeme ausgesetzt sind und wie stark sie das Staatsschuldenmanagement beeinflussen;
- Feststellen, welche Systeme sich auf kritische Funktionen und Daten auswirken, wie Dateneingabe, Verarbeitung und Ausgabe, Kreditgeberliste, Staatsschuldenberechnung, Berichterstattung und Entscheidungsfindung;
- Identifizierung der internen Kontrollen, die eingesetzt wurden, um festgestellte Risiken zu reduzieren;
- Einstufung von Systemen und Verfahren nach Risikobewertung und Festlegung des Prüfungsumfanges;
- Ressourceneinschätzung und Zeitplan;
- Vereinbarung von Interviews mit dem Leiter der IT-Einheit, mit Managern und Technikern, deren Aufgabe und Verantwortung es ist, das System zu entwickeln und Instand zu halten und zu steuern;
- Entwicklung der Matrize zur Prüfung allgemeiner und Applikationskontrollen und Bestimmung der notwendigen Test. (Siehe Matrizen-Vorschlag im Anhang III).

ORKB soll folgende Fragen beantworten

- Was sind die Informationssysteme zur Verwaltung von Staatsschulden und welche Rolle spielt jedes System?
- Wurde das PDMIS ausschließlich von der DMO entwickelt oder wurde es von Dritten erworben? Ist in letzterem Fall eine Anpassung gemacht worden, um spezifischen Notwendigkeiten der DMO nachzukommen?
- Wer soll zu allgemeinen IT-Kontrollen in der DMO befragt werden?
- Wer soll zu Applikationskontrollen des PDMIS befragt werden?
- Wer sind die Hauptbenutzer des PDMIS?
- Was stark ist das PDMIS bereits ausgereift?
- Was sind die wichtigsten allgemeinen und die Applikationskontrollen der PDMIS?

- Können interne Kontrollen die Informationssystemrisiken reduzieren, die das Staatsschuldenmanagement beeinträchtigen können?

- Was sind die höchsten Risiken in Bezug auf Dateneingabekontrolle, Verarbeitungskontrolle und Ausgabekontrolle des PDMIS?

- Welche Tests zu allgemeinen und Applikationskontrollen sollen gemacht werden?

Anhang II: Testmatrize für allgemeine Kontrollen

PRÜFUNG DER ALLGEMEINEN KONTROLLEN		
Ziel allgemeiner Kontrollen ist es Daten zu sichern, Applikationsprogramme zu schützen und bei unerwarteten Unterbrechungen kontinuierliche Rechneroperationen zu gewährleisten.		
ANFORDERUNG/ FUNKTIONALITÄT	**ALLGEMEINE KONTROLLEN**	**VORSCHLÄGE FÜR PRÜFUNGSVERFAHREN**
Allgemeine Angelegenheiten	Die Aktionen des IT Sektors müssen dem Auftrag der DMO entsprechen. Im Hinblick auf die Ziele der DMO soll die Leistung des PDMIS überwacht werden. Ein interne Revision der DMO/PDMIS-Operationen soll regelmäßig durchgeführt werden.	Überprüfung von Stichproben von Managemententscheidungen oder Memoranden, die sich auf IT-Maßnahmen beziehen, um zu gewährleisten, dass sie klar, gut begründet und entsprechend der Aufgabe der DMO abgefasst sind. Evaluierung der Leistung des PDMIS im Vergleich zu den erwarteten Indikatoren und Sicherstellen, dass die Geschäftsleitung diese Maßnahmen zur Kenntnis nimmt. Auswertung früherer interne Prüfungsberichte allgemeiner IT-Kontrollen, um schwerwiegende Mängel zu identifizieren. Bewertung der relativen Anzahl und Leistungsfähigkeit von IT-Arbeitsplätzen und von anderen IT-Geräten sowie Personal, um zu gewährleisten, dass das Personal entsprechend qualifiziert ist. Bewertung der relativen Anzahl von Budgetzuweisungen im Vergleich zu vorherigen Perioden und den IT-Sektoren anderer Regierungsbehörden.

Organisations-kontrollen	Die Verwaltung des DMO oder Finanzministeriums soll ein gutes, allgemeines IT-Umfeld entwickeln und aufrechterhalten. Das DMO- und das IT-Personal sollen regelmäßige und angemessene Schulungen, insbesondere zur Verbesserung des Sicherheitsbewusstseins erhalten. Ein Trainingsprogramm soll vorhanden sein. Es sollen schriftliche Regeln und Standardverfahren existieren bzgl.: • Informationssicherheit • Personal • IT-Leistungen von Dritten • Verwaltung von Änderungen • Physischer und logischer Zugang • Planung von äftskontinuität und Katastrophensanierung Regeln und Standardverfahren sollen regelmäßig aktualisiert werden. Die Geschäftspolitik soll von der DMO-Geschäftsleitung hinreichend verbreitet werden. Die DMO-Angestellten sollen die Geschäftsregeln kennen. Alle Tätigkeiten des Schuldenmanagements soll in einer Verfahrensdokumentation aufgezeichnet werden. Die Organisation soll eine angemessene Aufgabentrennung umsetzen, die gewährleistet, dass die Benutzer nur über die Befugnisse verfügen, den sie zur Ausübung ihrer Arbeit brauchen.	Befragung der DMO-Geschäftsleitung in Bezug auf ihr Interesse an IT, um so zu bewerten, ob sie bestrebt ist ein gutes, allgemeines IT-Umfeld zu entwickeln und aufrechtzuhalten. Überprüfung von Belegen, um festzustellen, ob Ausbildungen gemacht wurden. Befragung der DMO- Benutzer und des IT- Personals zu interviewen bzgl.: • der Häufigkeit von Schulungen • der Notwendigkeit von Kenntnissen/ Schulungen • der Kenntnis der Geschäftspolitik . Auswertung, ob die schriftlichen Regeln und Standardverfahren in Bezug auf IT-Dienste angemessen sind. Beobachtung, ob das DMO - Personal in Übereinstimmung mit den Standardverfahren arbeitet (im Handbuch festgelegt).
Physische Kontrollen	Der physische Zugang zum Großrechner und zu den Servern	Bestätigung des Vorhandenseins und der Wirksamkeit physischer

	soll gut geschützt sein. (Tür, Schloss, etc.) Videoüberwachung soll verwendet werden. Die Fenster des Raumes, in dem sich der Grossrechner und die Server befinden, sollten gegen erzwungenen Zugang geschützt werden. Nur autorisiertes Personal soll Zugang zum Serverraum haben.	Hindernisse, die den unerlaubten Zugang zum Großrechner, den Servern und Arbeitsplätzen der DMO blockieren. Kontrolle, ob die Verwaltungsmaßnahmen, wie formell festgelegt, zur Vorbeugung von unerlaubtem Zugang zu und Störung von IT-Diensten zufriedenstellend funktionieren. Beobachtung der Funktionsweise von elektronischen Hilfsmitteln wie elektronischen Türschlössern, elektronischen Key-Lock-Systemen, Kameras und anderer Mittel zur Begrenzung des physischen Zugangs zu Servern und anderen kritischen Infrastrukturen, um jede mögliche Schwachstelle automatischer Kontrollen zu identifizieren. Überprüfung der gemeinsamen Verwendung von Passwörtern bei Key-Lock-Systemen.
Logische Kontrollen	Wenn IT-Dienste in Bezug auf Staatsschulden außer Haus vergeben werden, soll der Vertrag angemessene Kontrollmaßnahmen festlegen, die gewährleisten, dass Dritte keinen Zugriff auf Geschäftsgeheimnisse, wichtige Daten und Strategien für Staatsschulden haben. Kein ehemaliger Angestellter, Außenstehender oder „virtueller" Benutzer soll ein aktives Zugangsprofil aufweisen. Die Zugangsrechte sollen regelmäßig überprüft werden. Die aktualisierte Antivirus-Software, Firewall, Intrusion- und	Überprüfung, ob die Zugangsprofile der Angestellten ihren Funktionen entsprechen. Feststellen, ob ein ehemaliger Angestellter oder jemand, der nicht bei der DMO angestellt ist, ein aktives Zugangsprofil hat. Kontrolle, ob Firewalls, aktualisierte Antivirus-sowie Intrusion- und Malware-Detection-Programme vorhanden sind. Überprüfung, ob das Betriebssystem am Arbeitsplatz und auf dem (den)

	Malware-Detection-Programme soll funktionstüchtig sein. Am Arbeitsplatz und dem (den) Server(n) soll eine systematische Aktualisierung des OS umgesetzt werden. Die Organisation soll ihre Maßnahmen zur Autorisierung, zum Widerruf oder zur Modifizierung von Zugangskontrollen bei veränderten Bedingungen (Neueinstellungen, Entlassungen, Funktionswechsel usw.) definieren. Die Organisation soll ihre Politiken und Richtlinien bzgl. Sicherheitspassworte und andere Sicherheitskontrollen (Schlüsselkarten etc.) allen Benutzern des Schuldenmanagementsystems mitteilen.	Server(n) systematisch aktualisiert wird. Kontrolle, ob die Passwortpolitik richtig umgesetzt wird. Prüfung, ob die Verfahren definiert sind und dokumentiert werden.
Umfeldkontrollen	Im gesamten Serverraum sollen Rohre (Wasser, Heizungssystem, Elektrizität etc.) verwendet werden. Wasser, Hitze und Feuchtigkeitsdetektoren sollten verwendet werden. Im Serverraum soll ein System zum Schutz vor Überschwemmungen verwendet werden. Rauch/Feuerdetektionssysteme sollten verwendet werden. Der Raum soll einen doppelten Boden haben oder die Geräte sollten auf einem Gestell 15-20 cm über dem Boden installiert sein. Die Arbeit des Großrechners und der Server soll mit einer unterbrechungsfreien	Der Datenbank-Serverraum sollte aufgesucht werden, um seine Umfeldbedingungen zu inspizieren und zu bewerten; ebenso die anderen DMO Räume. Die Existenz und wirksame Instandhaltung der Geräte zur Prävention von Feuer, Überschwemmungen und Feuchtigkeit sollten geprüft werden. Die Existenz und wirksame Funktion einer alternativen Stromversorgung zur Vermeidung von Unterbrechungen des IT-Service sollen bestätigt werden.

	Stromversorgung (USV) gewährleistet werden.	
Kontrollen zur Programmänderung	Die IT-Verwaltung soll ein Prüfungsprotokoll zu Operationsproblemen, Zwischenfällen und Fehlern führen. Das Protokoll soll den Zwischenfall von seinen Ursachen bis zur Lösung des Problems analysieren. Im Help-desk sollen keine wichtigen, ungelösten Anforderungen von PDMIS Schulungen vorliegen. Bei kritischen Zwischenfällen soll eine Problemeskalation und ein der Dringlichkeit des Zwischenfalles angemessener Reaktionsgrad vorgesehen sein. Bei Sicherheitszwischenfällen soll ein Bericht verfasst und den DMO-Managern übergeben werden. Frühere Änderungen sollen nach Standardverfahren umgesetzt werden. Wenn ein ungewöhnliches Schuldenmanagementsystem verwendet wird, soll die Organisation ihre Änderungskontrollverfahren dokumentieren und beschreiben, wer autorisiert Änderungen am System vorzunehmen. Die Organisation soll alle Schuldenänderungen im System verfolgen und überwachen (Prüfprotokoll).	Die zur Lösung von Anforderungen der DMO benötigte Zeit bzgl. Instruktionen und Fehler der PDMIS sollte bewertet werden. Häufigere PDMIS-Fehler und deren wahrscheinliche Ursachen sollten identifiziert werden. Frühere Änderungen sollten mit Standardverfahren verglichen werden.
BCP und DRP	Von der DMO etablierte BCP und DRP sollten existieren. Das für operationelle Kontinuität verantwortliche Personal soll seine Rolle kennen und sich	Die Konsistenz und Vollständigkeit von BCP und DPR sollte geprüft werden, ebenso, ob sie aktuell sind. Berichte früherer BCP, DRP Tests und Tests des

	seiner Verantwortung bewusst sein. Schwachstellen bei früheren BCP- und DRP-Tests oder bei Ernstfällen sowie die Maßnahmen der DMO zu ihrer Beseitigung sollen aufgezeichnet werden. Die Darlehensdokumente sollen sicher und geschützt vor Diebstahl, Feuer, Überschwemmungen oder anderen Zwischenfällen, die sie beschädigen oder zerstören können, aufbewahrt werden.	Datensicherungsplanes sollten bewertet werden Es sollte geprüft werden, ob der BCP und DRP ordnungsgemäß an alle Personalmitglieder verteilt worden sind. Es sollte festgestellt werden, ob die Datensicherung außer Haus in gutem Zustand ist und bei Systemversagen zur Reaktivierung verwendet werden kann.

Anhang III: Testmatrize für Applikationskontrollen

DOKUMENTATIONSNORMEN		
Ziel ordentlicher Dokumentationsnormen ist zu gewährleisten, dass die Kontrollen kontinuierlich funktionieren und Fehlerrisiken vermieden werden.		
VORAUSSETZUNG / FUNKTIONALITÄT	**APPLIKATIONSKONTROLLE**	**VORSCHLÄGE FÜR TESTVERFAHREN**
Dokumentations-kontrollen	Die Applikationskontrolldokumentation soll umfassend sein (mit allen Funktionalitäten und den damit verbundenen Funktionen).	Prüfung der Dokumentation
	Die Dokumentation soll aktualisiert werden, um Applikationsänderungen zu reflektieren.	Prüfung der Dokumentation
	Die in der Dokumentation enthaltenen Applikationskontrollen sollen wirksam implementiert und durchgeführt werden.	Eine Stichprobe der in den Dokumentationskontrollen festgelegten Applikationskontrollen ziehen und prüfen, ob sie der Dokumentation folgend wirksam implementiert werden und durchgeführt werden.
Dokumentations-datensicherung	Eine Sicherungskopie der Dokumentationsdaten soll aufbewahrt werden	Prüfung der Sicherungskopie der Dokumentationsdaten.
EINGABEKONTROLLE		
Ziel der Eingabekontrolle ist es, die Autorisierung, Genauigkeit, Vollständigkeit und Aktualität der in die Applikation eingegebenen Daten zu gewährleisten.		
VORAUSSETZUNG / FUNKTIONALITÄT	**APPLIKATIONSKONTROLLE**	**VORSCHLÄGE FÜR TESTVERFAHREN**
Felder mit Pflichteingabe	Die Applikation erteilt keine Operationsbestätigung, wenn eines der Pflichteingabefelder nicht ausgefüllt ist.	Beim Versuch, die Operation zu bestätigen, ohne die notwendigen Daten einzugeben, wird festgestellt, dass die Transaktion nicht stattgefunden hat. Dieser Test soll bei folgenden Verfahren angewendet werden:

		Vertragsregistrierung, Vertragsaktivierung, Wertpapierausstellungs-register etc.
Richtige und ordnungsgemäße Dateneingabe	Die Applikation erlaubt keine Eingabe von falschen oder unsachgemäßen Daten.	Das Datenformat in der Datenbank prüfen. Spezifikationen zur Eingabeblockierung prüfen und einige in der Applikation testen. Beim Versuch, falsche oder unsachgemäße Daten einzugeben, feststellen, ob es zu Blockierung und Fehlerbenachrichtigung kommt. Dieser Test soll bei folgenden Prozessen angewendet werden: Vertragsregistrierung, Vertragsaktivierung, Wertpapierausstellungs-register, Aktualisierung von Indexen, Wertpapiereinlösung etc.
	Die Applikation erlaubt keine Datenverdoppelung.	Beim Versuch, einen Vertrag oder ein Wertpapier mit einem schon existierenden Namen zu registrieren, feststellen, ob es zu einer Blockierungs- und Verdoppelungsmeldung kommt.
	Zur Berechnung von Vertragszinsen sollen keine überlappenden oder ungedeckten Perioden bezüglich Zinsanwendbarkeit vorhanden sein.	In der Datenbasis prüfen, ob überlappende oder ungedeckte Zinsperioden vorliegen.
	Im Falle eines Schenkungsvertrages soll die Applikation die Eingabe der Auszahlung erlauben, da es hierbei keine Amortisation und keine Zinsen gibt.	Beim Versuch, die Auszahlung eines Schenkungsvertrages einzugeben, feststellen, ob die Applikation keine Amortisations- und Zinsoperationen verlangt.

	Wenn der Benutzer Verträge sucht, um eine Auszahlung aufzuzeichnen, soll die Applikation auf dem Auszahlungseingabebildschirm nur „aktive" Verträge in „Auszahlungsphase" oder „Auszahlungs- und Amortisierungsphase" zeigen.	Beim Versuch, eine Auszahlung einzugeben, sollte die von der Applikation gezeigte Vertragsphase überprüft werden.
	Bei variablem Zinssatzregime soll die Applikation die Indexbeigabe verlangen.	Bei Auswahl des variablen Zinssatzregimes sollte geprüft werden, ob die Applikation eine Indexbeigabe verlangt.
	Die Applikation soll die Eingabe von Dezimalzahlen für ausgegebene Wertpapiere verweigern.	Beim Versuch, Dezimalzahlen für ausgegebene Wertpapiere einzugeben, sollte geprüft werden ob es zu einer Blockierung kommt.
	Die Applikation soll die Erstellung eines Wertpapieres vor seiner Emission erlauben.	Die Erstellung eines Wertpapieres ohne.Durchführung der Emission sollte simuliert werden.
Informations-vollständigkeit	Alle relevanten Schuldeninformationen soll in die Applikation eingegeben werden.	Es sollte geprüft werden, ob alle wesentlichen Schuldendaten wie Kreditgeschäfte, Garantien, Anleihen, Zinsen, Wechselkurs etc. in die Applikation eingegeben wurden.
Datums-kompatibilität	Das Initialdatum zur Berechnung der Bindungsrate muss vor dem Projektabschlussdatum liegen.	Beim Versuch ein Initialdatum zur Berechnung der Bindungsrate einzugeben, das nach dem Projektabschlussdatum liegt, soll festgestellt werden, ob es zu einer Blockierung und Fehlermeldung kommt.

	Das Wirksamkeitsdatum muss vor dem Projektabschlussdatum liegen	Beim Versuch ein nach dem Projektabschlussdatum eintretendes Wirksamkeitsdatum einzugeben soll festgestellt werden, ob es zu einer Blockierung und Fehlermeldung kommt.
	Das Wirksamkeitsdatum muss vor dem Auszahlungsfristdatum liegen.	Beim Versuch, ein nach der der Auszahlungsfrist liegendes Wirksamkeitsdatum einzugeben, soll festgestellt werden, ob es zu einer Blockierung und Fehlermeldung kommt.
	Das Datum der Auszahlungsfrist muss vor dem des Projektabschlusses liegen.	Beim Versuch, für die Auszahlungsfrist ein Datum nach dem des Projektabschlusses einzugeben, soll festgestellt werden, ob es zu einer Blockierung und Fehlermeldung kommt.
	Um den Fälligkeitsbericht zu erhalten, muss das Enddatum der Wertpapierfälligkeit nach dem Initialdatum eintreten.	Beim Versuch, ein Initialdatum einzugeben, das nach dem Enddatum der Wertpapierfälligkeit liegt, soll festgestellt werden, ob es zu einer Fehlermeldung kommt.
	Die Applikation verweigert ein in der Zukunft liegenden Operationsdatum.	Beim Versuch, Operationen mit einem zukünftigen Datum zu machen, soll festgestellt werden, ob es zu einer Blockierung und Fehlermeldung kommt.

		Dieser Versuch sollte bei folgenden Verfahren angewendet werden: Vertragsregistrierung, Vertragsaktivierung, Wertpapieremissionsregister Indexaktualisierung, Wertpapiereinlösung, Zahlungsaufzeichnung , Vertragsadditive etc.
	Das Wertpapieremissionsdatum muss vor dem seiner Fälligkeit liegen.	Beim Versuch, ein nach dem Fälligkeitsdatum liegendes Ausstellungsdatum einzugeben, soll festgestellt werden, ob es zu einer Blockierung und Fehlermeldung kommt.
	Bei Registrierung einer Amortisationszahlung und in Fällen, wo die eingegebene Summe oder das Datum nicht mit denen der Applikation übereinstimmen, soll die Applikation dem Benutzer die Sachlage melden bevor die Operationsbestätigung abgeschlossen werden kann.	Kontrolle, ob die Applikation bei Registrierung einer Zahlung mit anderem Datum oder einer anderen Summe als der, die in die Applikation eingegeben wurde, eine Meldung anzeigt.
	Wenn das Liquidierungsdatum nicht mit dem Fälligkeitsdatum übereinstimmt, soll die Applikation verlangen, Felder zur „Begründung" oder „Kreditgeberbestätigung" auszufüllen.	Eingabe verschiedener Daten für Wertpapierfälligkeit und Liquidierung ein und Feststellung, ob die Applikation eine Berechtigung oder Bestätigung verlangt.
	Geplante Auszahlungen können keine überlappenden Zeitperioden aufweisen. Das Initialdatum der zweiten Auszahlung kann, zum Beispiel, nicht vor dem Enddatum der ersten Auszahlung liegen.	Beim Versuch, das Datum der zweiten Auszahlung vor dem Datum der ersten einzugeben, feststellen, ob es zu einer

		Blockierung und Fehlermeldung kommt.
Sicherheit von Dateneingabe und Operationen	Die Applikation soll nicht autorisierten Personen den Zugang zum Dateneingang und zu Operationen verweigern.	Prüfung der Existenz von Merkmalen und Bedingungen eines bestimmten Profils. Beim Versuch, ohne das erforderliche Profil Daten einzugeben und Operationen zu machen, feststellen, ob es zu einer Blockierung kommt. Dieser Test soll bei folgenden Verfahren angewendet werden: Vertragsregistrierung, Vertragsaktivierung, Wertpapieremissionsregister, Indexänderungen, Wertpapiereinlösung, Zahlungsaufzeichnung etc.
	Bei manueller Dateneintragung soll die Applikation das Zugangsprotokoll aufzeichnen.	Prüfung, ob beschränkte Zugangsprotokolle existieren und ob diese von unbefugten Individuen gesehen oder modifiziert werden können.
	Die Applikation soll nicht gestatten, dass ein Wert in einem aktiven Vertrag verändert wird.	Beim Versuch, einen Wert eines aktiven Vertrages zu verändern ist, feststellen, ob dies blockiert wird.
	Die Applikation soll die Veränderung und Löschung von Daten in „annullierten" oder „abgeschlossenen" Verträgen verhindern.	Beim Versuch, einige Daten eines „annullierten" oder „abgeschlossenen" Mustervertrages zu verändern und zu löschen, soll festgestellt werden, ob das PDMIS derartige Versuche blockiert.
	Die Applikation darf einen aktiven Vertrag nicht ausschließen, es sei	Beim Versuch, einen aktiven Vertrag zu

	denn er ist in der Verhandlungsphase oder ist inaktiv.	löschen, prüfen, ob dies blockiert wird.
	Die Applikation soll keinen unsachgemäßen Ausschluß eines ausgegebenen Wertpapieres erlauben, es sei denn das Wertpapier hat keine Operationsverbindung.	Beim Versuch, ein ausgegebenes Wertpapier mit einer Operationsverbindung zu löschen, prüfen, ob dies blockiert wird.
	Für kritische Operationen braucht die Applikation eine zweifache Autorisierung.	Feststellen, ob kritische Operationen für ihre Beendigung zwei Autorisationen brauchen. Dieser Test soll bei folgenden Verfahren angewendet werden: Vertragsaktivierung, Wertpapieremission Amortisierungszahlung, Wertpapiereinlösung, Vertragswertänderung, Couponbezahlung, Zahlungsumkehr; Zinssatzänderung etc.
	Die Applikation sollte die Eingabe von Daten nur von bekannten Quellen erlauben. Das eingegebene Darlehen soll dem Abkommen und den akzeptierten Normen entsprechen.	Prüfungs, dass wesentliche Daten zweimal eingegeben werden und dass bei Datenunterschieden eine Fehlermeldung ausgegeben wird.
	Die Applikation sollte es erlauben, den Vertragswert zu reduzieren, es sei denn er ist größer als der Wert des „auszuzahlenden Restbetrags".	Beim Versuch, den Vertragswert über den auszuzahlenden Wert hinaus zu reduzieren, feststellen, ob es zu einer Blockierung und Fehlermeldung kommt.
	Die Applikation soll alle Transaktionen nur einmal aufzeichnen.	Machen Sie zwei identische Transaktionen (z.B. eine Amortisierungszahlung). Prüfen Sie, ob eine Blockierung entsteht und ob die Transaktionen in der Datenbank nur

		einmal oder doppelt registriert wurden.
	Bei Registrierung einer Zahlung soll die Applikation, wenn die Erlaubnis des Benutzers widerrufen wurde, nur über den Widerruf berichten wenn der Benutzer das Kommando „Eingabe" aktiviert; so wird es ermöglicht, sowohl den erfolglosen Versuch als auch die Daten, die der Benutzer eingeben wollte, zu protokollieren.	Beim Versuch, eine Zahlung mit widerrufener Erlaubnis zu registrieren, die Blockierung und Protokolle prüfen.
	Bei automatischem Dateientransfer zwischen Applikationen muss das PDMIS die Originaldaten, die es von anderen Applikationen erhalten hat, für einen vom DMO festgelegten Zeitraum aufbewahren.	Überprüfung der gespeicherten und von anderen Applikationen übernommenen Daten, um zu gewährleisten, dass sie verschlüsselt oder vor Schaden, Verlust oder Verstößen geschützt sind.
	Die Applikation soll keine Zinssatzänderung bei einer Rate erlauben, die schon bezahlt wurde. Jede Änderung eines Zinssatzes benötigt eine zweite Genehmigung, um umgesetzt werden zu können.	Beim Versuch einer Zinssatzänderung bei einer schon bezahlten Rate überprüfen der Blockierung. Prüfung, ob die Applikation eine zweite Genehmigung braucht, um einen Zinssatz zu ändern.
Kompatibilität zwischen Werten	Der Tranchenwert muss geringer sein als der Vertragswert.	Beim Versuch eine Tranche einzugeben, die höher ist als der Vertragswert, prüfen der Existenz einer Blockierung und Fehlermeldung.
	Der Einlösungswert muss geringer sein als der des ausgegebenen Wertpapiers	Beim Versuch, eine Wertpapiereinlösung zu machen, die höher ist als die des ausgegebenen Wertpapieres, feststellen, ob es zu einer Blockierung und Fehlermeldung kommt.

	Vor der Verarbeitung zeigt die Applikation eine Warnung von Unter- oder Überbezahlung an.	Simulation einer Unter- oder Überbezahlung und Feststellung, ob eine Fehlermeldung erscheint.
Quelldokumente	Um die Authentizität der Dateneingabe zu garantieren, soll die Eingabequelldokumente nachverfolgt werden können.	Auswahl einiger Dateneingaben und Prüfung, ob sie ein entsprechendes Quelldokument haben (z.B. Darlehensvertrag, E-Mail, elektronische Information etc.)
VERARBEITUNGSKONTROLLE		
Ziel der Prozeskontrolle ist, zu gewährleisten, dass die Daten von der Applikation exakt verarbeitet werden und, dass im Prozess keine Daten hinzugefügt, verloren oder modifiziert werden.		
VORAUSSETZUNG / FUNKTIONALITÄT	**APPLIKATIONSKONTROLLE**	**VORSCHLÄGE FÜR TESTVERFAHREN**
Korrekte Statusanzeige	Nach einer vollständigen Auszahlung soll die Applikation die Vertragsstatusanzeige ändern.	Simulieren Sie einen Auszahlungsabschluss und stellen Sie fest, ob der Vertragsstatus von „in Auszahlung" auf „vollständig ausgezahlt" wechselt.
	Die Applikation soll die Statusangabe von Wertpapieren ändern sobald deren Emission bestätigt wurde.	Simulieren Sie eine Ausgabebestätigung von Wertpapieren und stellen Sie fest, ob der Wertpapierstatus von „nicht aktiv" auf „aktiv" wechselt.
	Nach vollständiger Zahlung soll die Applikation die Statusangabe des Vertrages oder Wertpapieres ändern.	Simulieren Sie die letzte Zahlung und stellen Sie fest, ob sich der Vertrags- oder Wertpapierstatus ändert.
	Die Applikation muss mindestens folgende Phasen vorhersehen: • in Auszahlung: in dieser Phase werden Auszahlungen erstellt.	Erstellen Sie einen Vertrag, versuchen Sie in jeder Phase eine Auszahlung zu machen und stellen Sie fest, ob es

	• vollständig ausgezahlt: in dieser Phase sind Auszahlungen nicht erlaubt. • abgeschlossen: in dieser Phase erhalten Auszahlungen keine finanziellen Operationen und Datenveränderungen sind nicht erlaubt	zu einer Blockierung und Fehlermeldung kommt.
	Die Applikation soll Regeln enthalten, um den Vertragsstatus (aktiv, nicht aktiv) mit den Phasen (in Auszahlung, vollständig ausgezahlt, in Amortisierung, in Amortisierung und Auszahlung, abgeschlossen) in Einklang zu bringen, um widersprüchliche Information zu vermeiden. Ein „nicht aktiver" Vertrag kann, zum Beispiel, nicht „in Auszahlung" oder „in Amortisierung" sein.	Simulieren Sie Änderungen des Vertragsstatus und der Vertragsphasen und stellen Sie fest, ob sie kompatibel sind.
	Die Applikation muss ein Programm zur Aktualisierung der Phasen des Vertrages enthalten. Bei einer Auszahlungsbilanz von null muss sich die Phase von „in Auszahlung" auf „vollständig ausgezahlt" ändern.	Simulieren Sie die notwendigen Bedingungen zur Vertragsphasenänderung und stellen Sie fest, ob dies geschieht.
Richtige Berechnung	Die Applikation soll korrekte Berechnungen machen.	Prüfen Sie die Berechnungen und Neuberechnungen. Dieser Test sollte auf folgende Informationen angewendet werden: Schuldenstand (von Vertrag und Wertpapieren) Fälligkeitsdatum, Amortisierungsplan, (mit Daten und Werten) Wert von Vermittlerkomissionen, Wertpapierzahlungsfluss, Wertpapiereinlösung etc.
	Nach Änderung der eingegebenen Daten soll die Applikation die	Ändern Sie die Eingabe und überprüfen Sie die

	Berechnung durchführen und die Daten aktualisieren.	Aktualisierung und die Ergebnisse. Zum Beispiel: • simulieren Sie eine Zahlung und stellen Sie fest, ob die ausstehende Bilanz und der Abschreibungsfluss aktualisiert wurden. • Ändern Sie einige Indexe und stellen Sie fest, ob der Schuldenstandwert aktualisiert wurde.
	Die Programmierung der Applikation soll mindestens folgende Ratenberechnungsmethoden enthalten: gleichmäßige Verteilung, einfache Zinsen, Rate, Preisanwendung, kontinuierliche Abschreibungsanwendung, Pool-Einheit Währungskorb (IBRD) und UAC Währungskorb (IDB).	Prüfen Sie die Methoden des Systems zur Ratenberechnung. Die Richtigkeit dieser Methoden kann an Beispielsdaten überprüft werden.
	Sobald das Feld „vertraglich vereinbarter Wert" geändert wird muss die Applikation automatisch das Feld „vertraglich vereinbarte auszuzahlende Bilanz" neuberechnen.	Ändern Sie den vertraglich vereinbarten Wert und stellen Sie fest, ob die vertraglich vereinbarte auszuzahlende Bilanz richtig aktualisiert worden ist.
	Die Daten der Raten sollen von der Applikation automatisch und nach folgenden möglichen Methoden erstellt werden: • Initialdatum und festgelegte Ratenanzahl. • Initialdatum, Enddatum und absteigende Ratenanzahl. • Initialdatum, Enddatum und festgelegte Ratenanzahl. • Initialdatum und Periodenanzahl	Tragen sie die von jeder möglichen Methode geforderten Daten ein und prüfen Sie, ob die Daten der Raten korrekt sind.

	• Perioden	
	Wenn das Datum für eine Rate auf einen Feiertag fällt, muss die Applikation zwei Optionen anbieten: die Rate auf den folgenden oder den vorhergehenden Arbeitstag verschieben,	Konfigurieren Sie die Rate auf einen Feiertag und stellen Sie fest, ob die Applikation es ermöglicht, das Datum auf den folgenden oder den vorhergehenden Arbeitstag zu verschieben.
	Das System soll automatisch den nominalen Wertpapierwert aktualisieren sobald die jeweilige Indexierung geändert wird.	Ändern Sie die Indexierung eines Wertpapieres und prüfen Sie, ob der entsprechende Nominalwert aktualisiert wird.
	Bei einer Zahlung, die niedriger ist als der von der Applikation berechnete Wert, erscheint im Moment des Zahlungseinganges eine Meldung. Diese Meldung soll bis zur Fälligkeit der nächsten Rate wiederholt werden.	Simulieren Sie eine Zahlung, die niedriger ist als der von der Applikation berechnete Wert, und stellen Sie fest, ob eine Meldung erscheint und ob sie bis zur Fälligkeit der nächsten Rate wiederholt wird.
	Das System soll Wertpapiere mit simulierten Emissionsdaten in der Datenbank voneinander unterscheiden.	Prüfen Sie in der Datenbank ob die simulierten Wertpapiere differenziert werden und, dass diese nicht zur Berechnung des Schuldenstands und seiner Fälligkeit herangezogen werden.
	Wenn der Benutzer ein Wertpapier löscht, soll die Applikation die entsprechenden Werte in der Datenbank löschen.	Löschen Sie ein Wertpapier und stellen Sie fest, ob sein Wert in der Datenbank gelöscht wird.
	"Annullierte" Wertpapiere sollen zur Berechnung von Wertpapierschulden (z.B. IRR, Fälligkeit) nicht in Betracht gezogen werden. Die entsprechenden Werte sollten in der Datenbank permanent gelöscht werden.	Ändern Sie den Status eines Wertpapiers in „annulliert" und stellen Sie fest, dass sein Wert nicht zur Berechnung von Schuldenstand,

		Fälligkeit usw. herangezogen wird.
	Die Applikation soll Raten mit überfälligen Zahlungen unterschiedlich behandeln.	Prüfen Sie, ob die Applikation alle Gebühren auf überfällige Raten richtig berechnet.
Richtige Prozessfehlerkontrolle	Tage- oder wochenalte Prozessfehler sollen behoben werden.	Prüfen Sie, ob ein Kriterium existiert, das sich auf die Anzahl der Tage bezieht, die benötigt werden, um einen Systemfehler zu beheben. Prüfen Sie, ob Fehlermeldungen vorliegen und diskutieren Sie mit dem System-/Schuldenmanager die zur Behebung der angezeigten Fehler erforderlichen Maßnahmen.
	Beim Auftreten eines Prozessfehlers soll die Applikation die Datenverarbeitung stornieren und in der Datenbank Datum, Uhrzeit und technische Gründe des Problems speichern.	Simulieren Sie einen Prozessfehler und stellen Sie fest, ob die Applikation das vorgefallene Problem in der Datenbank speichert.
Richtige Berichterstattung	Die Applikation soll gewährleisten, dass Schuldenmanager den Cash-Flow (bzgl. von Anleihen in ausländischer und nationaler Währung, Hedging und Handel, Garantien und Kreditweitergabe) aller Transaktionen ordnungsgemäß aufzeichnen können	Machen Sie eine Transaktion und stellen Sie fest, ob der diesbezügliche Bericht richtig und ordnungsgemäß ist.
	Die Applikation soll die während der Vertragsgültigkeit umgesetzte Transaktionsgeschichte speichern und muss die Daten des Kreditgebers, des vertraglich vereinbarten Wertes, des Projektabschlusstages sowie der Datengrenzen der Auszahlungsfelder enthalten.	Prüfen Sie einige Verträge, um festzustellen, ob sie deren Transaktionsgeschichte mit allen notwendigen Einzelheiten ihrer Lebensdauer enthalten.

	Die Applikation soll für jedes Schuldeninstrument ein Protokoll führen.	Prüfen Sie, ob die historischen Transaktionen eines Wertpapieres oder Vertrages ihren Schuldenprotokollen entsprechen.
Korrekte Aufgabenplanung	Die Applikation soll einen automatischen Start für vom DMO geplante Aufgaben aufweisen, um Indexierungen, Schuldenstand etc. zu aktualisieren.	Prüfen Sie, ob ein automatischer Start vorhanden ist und, ob er richtig funktioniert.
	Falls ein Wertpapiertyp vorliegt, dessen Amortisierung in der gleichen Frequenz wie die der Zinsen programmiert ist (z.B. Preis), soll das System gewährleisten, dass Zinsen und Amortisierung den gleichen Zahlungsplan verwenden.	Stellen Sie ein Wertpapier aus, dessen Amortisierung und Zinsen die gleiche Frequenz haben und prüfen Sie, ob sie den gleichen Zahlungsplan aufweisen.
Prüfprotokoll	Ein PDMIS Prüfprotokoll soll erhalten werden, um zu gewährleisten, dass der Schuldenvertrag oder das Wertpapier von seiner Unterzeichnung oder Emission bis zur Rückzahlung verfolgt werden kann.	Stellen Sie fest, ob für Stichproben von Verträgen und Wertpapieren ein Prüfprotokoll von deren Registrierung bis zur Rückzahlung existiert.
AUSGABEKONTROLLE		
Ziel der Ausgabekontrolle ist die Gewährleistung der Ausgabeintegrität und die korrekte und rechtzeitige Verteilung der produzierten Ausgabe.		
VORAUSSETZUNG / FUNKTIONALITÄT	**APPLIKATIONSKONTROLLE**	**VORSCHLÄGE FÜR TESTVERFAHREN**
Kontrolle des Informationsnutzers	Die Applikation soll über ein Bericht-Protokoll verfügen, das den Namen des Benutzers, der den Bericht angefordert hat, speichert, wie auch das Datum und die Uhrzeit der Anforderung.	Fordern Sie Berichte an und stellen Sie fest, ob die Applikation diesbezügliche Daten speichert.
	Die Applikation soll eine besondere Genehmigung brauchen, um spezielle Berichte zu laden (besonders bzgl. vertraulicher Informationen).	Versuchen Sie einige vorgegebene Berichte zu erzeugen.

Rechtzeitige und verlässliche Berichterstattung	Die Applikation soll vorgegebene Berichte erzeugen (Anleihe, Darlehen und Tranchenklassifizierung, z.B. Fälligkeit, Status, Finanzquellen, Finanztyp, Typ von Kreditinstrumenten Bedingungen, unbezahlte Rechnungen etc.)	Versuchen Sie diese Berichte zu erzeugen.
	Die Applikation soll ordentliche Berichte produzieren, die die Vollständigkeit und Integrität der Information gewährleisten.	Prüfen Sie, ob die Berichte den Nutzungsbedingungen entsprechen. Prüfen Sie, ob die Berichte Seitenzahlen und Prüfsummen aufweisen. Dieser Test soll bei folgenden Berichten angewendet werden: Fälligkeitsbericht (für Vertrags- und Wertpapierschulden), Bericht über ausstehende Restbeträge, Empfangsbericht , etc.
	Die Applikation soll globale (alle Wertpapierschulden) und spezifische Berichterstattung erlauben, wie: • Nach Wertpapierstatus (ausgegeben, annulliert, eingelöst etc.) • Für Ereignisse in einem gewissen Zeitraum (Ausgaben Erlösungen etc.) • Für kurz- und langfristiges Aktienkapital • Nach Portfolioposition • Nach Wertpapiertyp • Nach Fälligkeitsintervall, etc.	Versuchen Sie globale und spezifische Berichte mit folgenden Kriterien zu erstellen: • Nach Wertpapierstatus (ausgegeben, annulliert, eingelöst etc.) • Für Ereignisse in einem gewissen Zeitraum (Ausgaben Erlösungen etc.) • Für kurz und langfristiges Aktienkapital • Nach Portfolioposition • Nach Wertpapiertyp • Nach Fälligkeitsintervall, etc.

	Die Berichte müssen vollständige und richtige Information präsentieren.	Berichte erstellen und die Berechnungen wiederholen Dieser Test soll bei folgenden Berichten angewendet werden: Fälligkeitsbericht (für Vertragsschulden und Wertpapierschulden), Bericht über ausstehende Restbeträge, Empfangsbericht etc .
	Die Berichte sollen genau dieselbe Information präsentieren wie die Applikation.	Vergleichen Sie die Berichte auf Übereinstimmung mit der auf den Applikationsbildschirmen präsentierten Information. Dieser Test soll bei folgenden Berichten angewendet werden: Fälligkeitsbericht (für Vertragsschulden und Wertpapierschulden), Bericht über ausstehende Restbeträge, Empfangsbericht etc.
	Die im Fälligkeitsbericht, dem Bericht über ausstehende Restbeträge und dem Kapitalbestandsbericht präsentierten Werte müssen zusammenpassen.	Vergleichen Sie die Berichte auf ihre Übereinstimmung.
	Das System soll fähig sein, Berichte von Gesamtschulden auf individueller und aggregierter Basis zu erstellen, und zwar mit einer Schuldendienstprognose von existierenden und zukünftigen Anleihen und Wertpapieren.	Versuchen Sie derartige Berichte zu erstellen. Prüfen Sie, ob die Berichte existierende und erwartete Schuldenoperationen umfassen.

	Die Applikation soll automatisch tägliche Finanzprogrammberichte aller „aktiven" Verträge erstellen. Auch soll sie die manuelle Berichterstattung für spezifische Verträge erlauben.	Prüfen Sie die Existenz automatischer Berichte über alle aktiven Verträge und versuchen Sie manuelle Berichte für spezifische Verträge zu erstellen.
Exakte Datenübertragung	Die Datenübertragung zwischen Applikationen und/oder Verarbeitungsstufen soll exakt und komplett sein.	Simulieren Sie eine Datenübertragung zwischen Applikationen und überprüfen Sie die Genauigkeit und Vollständigkeit der Daten.
Nützliche Ausgabemeldungen	Beim Zugriff der Applikation sollte sie eine Meldung mit folgender Information anzeigen: • Verträge die in den nächsten fünf Tagen fällig werden • • Verträge mit überfälliger Ratenzahlung • Verträge mit teilweise bezahlten Raten • Verträge mit überfälligen Auszahlungsdaten. • Bei Verträgen mit einer Auszahlungsfrist von 5 Tagen soll die Applikation täglich eine Meldung schicken bis die Zahlung gemacht ist oder der zu zahlende Wert annulliert oder die Frist verändert worden ist.	Greifen Sie auf die Applikation zu und prüfen Sie, ob sie all diese Meldungen anzeigt.
	Die Applikation soll über den Berechnungszustand Auskunft geben, entweder als „laufende" oder „beendete" Berechnung.	Fordern Sie eine Berechnung an und prüfen Sie, ob die Applikation über den Operationszustand Auskunft gibt.
	Nach Abschluss eines Berichtes soll die Applikation melden, dass die Berichterstattung beendet wurde oder den gewünschten Bericht anzeigen.	Fordern Sie einen Bericht an und prüfen Sie, ob die Applikation anzeigt, dass die Operation abgeschlossen ist oder

		der gewünschte Bericht gezeigt wird.
	Die Applikation soll über den Erstellungsstatus des Berichtes Auskunft geben, und zwar mit „in Bearbeitung” oder „abgeschlossen”.	Erstellen Sie einen Bericht und prüfen Sie, ob die Applikation über den Operationsstatus Auskunft gibt.
	Wenn es zu irgendeiner Änderung des Zinssatzes, kommt muss die Applikation eine Warnung anzeigen.	Ändern sie den Zinssatz und stellen Sie fest, ob eine Warnung erscheint.
	Vor Umsetzung des Ausschlusses oder der Einlösung eines Wertpapieres soll die Applikation auf einem Bildschirm das zu annullierende oder einzulösende Wertpapier zur Bestätigung durch den Benutzer anzeigen..	Versuchen Sie, ein Wertpapier einzulösen oder zu annullieren, und prüfen Sie, ob die Applikation dies meldet und eine Bestätigung verlangt.

Abbildung 1: Staatsschuldenprüfung der ORKB: Der Fall Brasilien

Prüfung des Integrierten Schuldensystems (SID) der Bundesregierung von Brasilien durch den Brasilianischen Rechnungshof im Jahr 2014.

Da das Integrierte Schuldensystem auf interne Wertpapierschulden geprüft wird, hat das Prüfungsteam beschlossen, sich nur auf die Prüfungsverfahren zu konzentrieren, die sich mit dem Management von Auslandsschulden (in Form von Wertpapieren und Verträgen) befassen. Die Prüfungsbemerkungen und Ergebnisse waren wie folgt:

IT Systemstrategie & allgemeines Management;

In seinem Verfahrenshandbuch wird das SID, sobald es völlig abgeschlossen ist, folgende Funktionen beinhalten:

a) ein breites Berechnungsspektrum, wie aktualisierten Nennwert, Stückpreis, Bestand (von Vertrags- und Wertpapierschulden), finanzielle Vertragsplanung, Preisinformation, Anleihepreis und Verfallsdatum;

b) eine Anzahl von Untersuchungen und Berichten von Datenregistrierungen und Rechnungsergebnissen.

c) finanzielle Operationen wie Emission von Anleihen, Vertragsrückzahlungen, Vertragsablösung und Transferenz, unter anderen:

d) ein völlig benutztes Informationsregister der verschiedenen Geschäftsmodule.

Was Systemstrategie und allgemeines Management angeht waren die wesentlichen Bemerkungen und Prüfungsergebnisse:

- Es gibt kein Trainingsprogramm für die am häufigsten verwendeten Staatschuldenmanagementsysteme, Seorfi und SID;
- Es gibt keine erwarteten Daten zur völligen Implementierung des SID, einschließlich interner Wertpapierschulden;
- Einige wichtige Operationen wie Vertragsaktivierung, Rückzahlungen, Reverse- Rückzahlungen, Zinssatzänderungen oder Vertragswertänderungen werden nur von einer Person umgesetzt. Das System sieht keine Bewilligung oder Doppelkonferenz vor. Die Verfahrenssicherheit beruht nur auf der Eignung des Profil, was ein Problem mit der Aufgabentrennung darstellt.

  Ein weiteres Problem mit der Aufgabentrennung ist der Personalmangel zur Entwicklung des SID. Das DMO Personal arbeitet gegenwärtig neben seinen üblichen Funktionen daran.
- Die Bewertung der Verwundbarkeit und operationellen Risiken in Verbindung mit IT-Prozessen ist fertig, doch die Studie zur Reduzierung dieser Risiken ist noch nicht gemacht worden.
- **Sicherheit & Umfeldkontrollen;**

Bezüglich Sicherheit und Umweltkontrollen waren die wesentlichen Beobachtungen und Ergebnisse wie folgt:

- Die DMO hat keinen Manager für Informationssicherheit und Kommunikation ernannt und das Informationssicherheitskomitee, dessen Aufgabe es ist den IS Manager zu ernennen, hat noch nicht effektiv zu arbeiten begonnen.
- Kein Plan für Geschäftskontinuität (BCP) ist formell erstellt worden und die Arbeitsprozesse des Staatsschuldenmanagements werden revidiert, um den BCP auszuarbeiten.
- Die Analysen des Prüfungsteams haben die Existenz von drei aktiven generischen Nutzern ermittelt, was die guten IT-Praktiken verletzt, vor allem den Artikel 11.2.1 der ISO / IEC 27002: 2005, der die Verwendung einer persönlichen Benutzeridentifizierung empfiehlt, um die Verantwortlichkeit jeder Person, die das System benutzt, zu gewährleisten;
- Obwohl die Zugangsdefinition zum SID nur mit einem digitalen A3 Zertifikat gemacht werden soll und die Zugangsmöglichkeit mit nationaler Identifikationsnummer und Passwort eine Ausnahme darstellt, gibt die Analyse der SID-Datenbankbenutzer an, dass keine Beendigungsfrist dieses Ausnahmeverfahrens existiert.
- Die Analyse der SID Datenbank bzgl. Benutzer gibt Fehler des Revisionsprozesses des Benutzerzugangs an;
- Das Prüfungsteam hat auch Fehler in der täglichen automatischen Instandhaltungsroutine der SID Nutzerdatenbank festgestellt;
- Das SID zeichnet für die meisten seiner Transaktionen kein Prüfprotokoll auf; daraus ergibt sich, dass die DMO keine periodische Revision von vom System erstellten Prüfprotokollen macht und ebenso wenig die im SID umgesetzten Transaktionen überwacht.
- Das SID ist nicht fähig routinemäßig Systemprotokolle umzusetzen, zu speichern und zu analysieren.
- Das Prüfungsteam bemerkte, dass zu den von der DMO am meisten verwendeten Systemen, Seorfi und SID, keine Testpläne und Testergebnisse vorliegen.
- Das Prüfungsteam hat keine Bestätigung der tatsächlichen Schaffung eines Teams zur Bearbeitung von Vorfällen in Computernetzwerken erhalten, welches dafür verantwortlich ist, Mitteilungen zu Zwischenfällen in Computernetzwerken entgegenzunehmen, zu prüfen und darauf zu antworten.
- Das Prüfungsteam bemerkte das Fehlen eines IT-Servicekontinuitätsplans, d.h. des formellen Dokuments, welches die Kontinuitätsinitiativen aller IT-Dienste, die bei der Agentur oder Einheit umgesetzt werden, zentral beschreibt.

Operationskontrollen & Dokumentation;

Bezüglich Operationskontrollen und Dokumentation waren die wesentlichen Beobachtungen und Prüfungsergebnisse wie folgt:

- Die Schnittstelle ist nicht sehr nutzerfreundlich, weshalb Nutzer des SID im Vorhinein bereits über viele Systemkenntnisse verfügen müssen;
- Es gibt keine SID-Benutzerhandbuch;

- Die Verarbeitungsgeschwindigkeit der Berechnungen ist niedrig. Dies verhindert die gleichzeitige Erstellung von Berechnungen und Berichten. Da es viele gleichzeitige Systembenutzer gibt, kann das die Leistungsfähigkeit des Systems beeinträchtigen. Das Prüfungsteam schlug der DMO vor, Verbesserungen in Betracht zu ziehen, um die Verarbeitungskapazität des Systems zu erhöhen.

Applikationskontrollen

Nach Durchführung der Eingabe-, Verarbeitungs- und Ausgabekontrolltests des SID zu Auslandsstaatschulden durch das Prüfungsteam waren die Prüfungsergebnisse und Beobachtungen wie folgt:

- Viele Fehlermeldungen sind unklar und manchmal für den Benutzer nicht sichtbar;
- Mittels Eingabe von Applikationskontrolltests fand das Prüfungsteam mehrere Fehlermeldungen, die den Grund des Fehlers nicht erklären;
- Bei der Verarbeitung von Applikationskontrolltests von Vertragsschulden im Ausland fand man unterschiedliche Werte im Cash-Flow-Finanzbericht bezogen auf eine Umkehrung, die bei Ausgabe dieses spezifischen Berichtes nicht in Betracht gezogen wurde;
- Im Rahmen der Applikationskontrolltests der Ausgabe erstellt die Applikation bei fehlerhafter Dateneingabe nicht alle Vertragsschuldenberichte wie erwartet, und die Applikation teilt dem Benutzer diesen Fehler nicht mit;
- Durch Ausgabeskontrolltests der Applikation wurden Fehler in Vertragsschuldenberichten identifiziert, die auf die Verwendung veralteter Inhaltsverzeichnisse des Systems zurückzuführen waren;
- Einige Vertragsschuldenberichte wurden unvollständig ausgegeben.

Empfehlungen

Auf Grund der berichteten Prüfungsergebnisse und Beobachtungen empfahl das Prüfungsteam dem National Treasure Secretariat in 90 (neunzig) Tagen einen Aktionsplan auszuarbeiten, der einen Zeitplan zur Implementierung folgender Schritte enthält:

- Ein Datum zur vollständigen Implementierung des SID einschließlich interner Wertpapierschulden festzulegen;
- Den Manager für Informations- und Kommunikationssicherheit und das Informationssicherheitskomitee zu ernennen;
- Den Plan für Geschäftskontinuität zu formalisieren;
- Den Plan für IT-Servicekontinuität zu formalisieren;
- Ein Team zur Bearbeitung von Vorfällen in Computernetzwerken einzusetzen;
- Die Auswertung und Reduzierung operationeller IT-Risiken umzusetzen;
- Die tägliche automatische Routineinstandhaltung der SID-Benutzerdatenbank zu überprüfen.
- Den SID-Bewertungsprozess des Benutzerzugangs zu überprüfen;

- Den SID-Prozess für Zugangsgewährung für generische Benutzer zu überprüfen;
- Periodische Revisionsverfahren von vom SID erstellten Prüfprotokollen zu etablieren;
- Applikationsprotokollberichte des SID zur Verfügung stellen;
- Fehlermeldungen des SID zu prüfen;
- Eine SID Benutzerhandbuch zu entwickeln;
- Die Berichterstattungsroutine des SID zu überprüfen.

Bild 2: Staatsschuldenprüfung der ORKB: Der Fall Moldawien

Applikationskontrollprüfung des Rechnungshofes der Republik von Moldawien

Die DMFAS-Applikation verfügt über genügend interne Kontrollen die automatisch prüfen, ob der Dateneingang richtig erfolgte; zur Bestätigung gibt es einige bedenkliche Aspekte, eliminiert werden müssen: Benutzer haben die Möglichkeit, Daten in das Klassifizierungssystem und in andere Systemtabellen einzugeben, was die Genauigkeit und Integrität von Daten durch Verdoppelung oder Löschung von Registern beeinträchtigen kann.

Empfehlung Nr. 15: Überprüfung der Möglichkeit, die Rechte von Benutzern zur Eingabe, Änderung oder Löschung von Daten im DMFAS Datenbankklassifikator einzuschränken oder derartige Operationen zu identifizieren, um Datenverdoppelung oder fehlerhafte Eingaben zu vermeiden.

Neben den Standardberichten, die Teil der DMFAS-Applikation sind, wurde eine große Anzahl von Berichten allgemeiner Natur, mit den meisten notwendigen Aspekten, in „Excel" entwickelt. Nicht alle Arten von Berichten werden systematisch verwendet. Die meisten angeforderten Berichte werden in „Excel" produziert. Dennoch werden gewisse Berichte manuell und mit Daten aus anderen Berichten erstellt. Besorgniserregend ist die Modalität Daten in „Excel"-Berichten zu erneuern. Die Erstellung von Berichten ist eine sehr komplizierte Angelegenheit, die drastisch vom menschlichen Faktor beeinträchtigt werden kann. Zusätzlich können erstellte Berichte unerlaubt modifiziert werden, und diese Fehler können in anderen wichtigen Kurzberichten auftreten, die höchste Sicherheitsstufe haben sollten und das Hauptresultat der Public Debt General Division darstellen.

Es ergibt sich, dass kleinere Mängel die Verlässlichkeit und Genauigkeit von Daten wichtiger Berichte der Public Debt General Division beträchtlich beeinträchtigen können.

Empfehlung Nr. 16: Erwägung der Möglichkeit, den Änderungsprozess von zu erstellenden Berichten zu optimieren oder zu automatisieren. Identifizierung einer Möglichkeit, die automatisch einen Kurzbericht unter Ausschluss des menschlichen Faktors erzeugt. Die mögliche Migration zur Version 6.0 kann als Gelegenheit angesehen werden.

BIBLIOGRAFIE

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

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

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

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

International Organization of Supreme Audit Institution. ISSAI 5440 – Guidance for Conducting a Public Debt Audit – The Use of Substantive Tests in Financial Audits. November 2007.

International Organization of Supreme Audit Institution. ISSAI 3000 – Standards and guidelines for performance auditing based on INTOSAI's Auditing Standards and practical experience. . July 2004.

International Organization of Supreme Audit Institution. ISSAI 5310 – Information System Security Review Methodology. October 1995

INTOSAI Development Initiative. WGTI – IDI Handbook on IT Audit for Supreme Audit Institutions. February 2014.

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

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

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