ديـــوان المحاسبـــة
State Audit Bureau
State of Qatar • دولـــة قطـــر

مخاطر التشغيل الالكتروني للبيانات وكيفية اكتشاف وسائل الغش ومواطن الفساد

إعداد
عبدالرحمن طلال السليطي - مدقق مساعد

Public - عام

المحاور

- أولاً: تعريف ديوان المحاسبة وإدارة تكنولوجيا المعلومات
- ثانياً: تحديد أهم المخاطر التشغيل الالكتروني للبيانات
- ثالثاً: حالات عن مخاطر التشغيل الالكتروني
- رابعاً: طرق كشف الاحتيال في التشغيل الالكتروني وكيفية التحري منها
- خامساً: الخاتمة

Limited Access - وصول محدود

تاريخ الانشاء:

استناداً إلى القانون رقم (11) والمادة رقم (15) الصادر بتاريخ: 27/10/2016 بشأن ديوان المحاسبة، بدأ ديوان المحاسبة القطري التدقيق على تكنولوجيا المعلومات على الجهات الخاضعة للتدقيق.

نص القانون على أن يقوم الديوان في مجال الرقابة على تكنولوجيا المعلومات بتدقيق النظم والبرامج والتطبيقات الإلكترونية، والتحقق من كفاية وسلامة الضوابط الداخلية الخاصة بها والالتزام بتطبيقها، و تلبيتها لاحتياجات الجهة وانتظام سير أعمالها والمحافظة على حقوقها وممتلكاتها، ومن سرية البيانات وحمايتها، وذلك وفقاً للسياسات المعتمدة بشأنها، وقد انقسم التدقيق على تكنلوجيا المعلومات في ديوان المحاسبة الى فرعين وهما الرقابة على حوكمة تكنولوجيا المعلومات وعلى الرقابة على نظم المعلومات.

Public - عام

الرقابة على حوكمة تكنولوجيا المعلومات

- تقييم حوكمة وإدارة مخاطر تكنولوجيا المعلومات.
- مراجعة خطط استمرارية الأعمال.
- تدقيق مشروعات نظم المعلومات، وتقييم مدى توافقها مع احتياجات العمل بما ينسجم مع رؤية الجهة وأهدافها.
- تقييم كفاءة وفعالية الاستخدام للأصول المادية لتكنولوجيا المعلومات.

Public - عام

الرقابة على نظم المعلومات

- تدقيق نظم وبرامج وتطبيقات تكنولوجيا المعلومات.
- التحقق من كفاءة وفاعلية الضوابط الداخلية للنظم والبرامج والتطبيقات الإلكترونية.
- تدقيق ومراجعة أعمال تطوير النظم والبرامج والتطبيقات.
- تدقيق عمليات إدارة قواعد البيانات، وتقييم مخرجاتها وفقاً لمبادئ السرية والتكامل والتوافر.
- تقييم كفاءة وفعالية استخدام أصول النظم والبرامج والتطبيقات التي يتم حيازتها.

Public - عام

من أهم مخاطر التشغيل الإلكتروني للبيانات

- تقييم حوكمة وإدارة مخاطر تكنولوجيا المعلومات.
- مراجعة خطط استمرارية الأعمال.
- تدقيق مشروعات نظم المعلومات ، وتقييم مدى توافقها مع احتياجات العمل بما ينسجم مع رؤية الجهة وأهدافها.
- تقييم كفاءة وفعالية الاستخدام للأصول المادية لتكنولوجيا المعلومات.

Public - عام

حالات عن مخاطر التشغيل الالكتروني

- غياب مراقبة نظام التشغيل ERP للقيام ببعض التجاوزات المالية.

(Audit loges file)

- غياب اجراء حذف البيانات الحساسة من الأجهزة المستهلكة قبل التخلص منها.
- استغلال صلاحيات المستخدمين في نشر وتسريب المعلومات بوسائل التواصل الاجتماعي.

Public - عام

طرق كشف الاحتيال في التشغيل الالكتروني للبيانات

- تحليل البيانات.
- مراجعة المدخلات والمخرجات للبرامج.
- التحقق من السجلات الالكترونية.
- مراجعة دورية.
- مراجعة إجراءات العقود والمناقصات.
- تبادل المعرفة والمعلومة و الخبرات.

Public - عام

دور المراجع في معرفة مخاطر التشغيل الإلكتروني

- تقييم المخاطر.
- التأكد من فحص الأنظمة والبيانات.
- التدقيق والاختبار.
- التأكد من عملية المراقبة المستمرة و الامتثال.
- تقديم التوصية لوضع الضوابط الملائمة.

Public - عام

الخاتمة

- إبراز أهمية دور المراجعة المستمرة والمراقبة في إدارة مخاطر تكنولوجيا المعلومات.
- التركيز على مراجعة الأمن السيبراني ودقة البيانات المخزنة في الأنظمة المعلوماتية ضمن برامج التدقيق

Limited Access - وصول محدود

ديـــوان المحاسبـــة

State Audit Bureau

State of Qatar • دولـــة قطـــر

Public - عام

الديوان العام للمحاسبة
General Court of Audit

الإدارة العامة للرقابة على أداء تقنية المعلومات

قطاع الرقابة على الأداء

مكونات العرض

- نبذة عن الإدارة
- أعمال الإدارة
- أهداف التدقيق باستخدام أدوات تقنية المعلومات
- أمثلة عن حالات التدقيق في بيئة تقنية المعلومات

مدة العرض
(5) دقائق

عدد الشرائح
(7) شرائح

نبذة عن الإدارة

- أسست الإدارة في عام 1984م.
- تم ابتعاث (10) موظفين للولايات المتحدة لتلقي التدريب في مجال التدقيق في بيئة تقنية المعلومات.
- عام 1989م حصول الديوان العام للمحاسبة على جائزة بروغ كاندوتش العالمية خلال مؤتمر الإنكوساي في برلين لتبنيه تدقيق الحاسب الآلي.

اعمال الإدارة

- مراجعة الأنظمة والتطبيقات الآلية
- مراجعة أمن بيئة الحاسب الآلي
- مراجعة أداء شبكات الحاسب الآلي
- مساندة إدارات الديوان الأخرى
- مراجعة عقود الحاسب الآلي
- التدريب

أهداف التدقيق باستخدام أدوات تقنية المعلومات

- المحافظة على المال العام للدولة
- تحقيق اهداف التحول الرقمي في المملكة العربية السعودية
- التأكد من فاعلية وكفاءة الأنظمة وتحقيق أهدافها

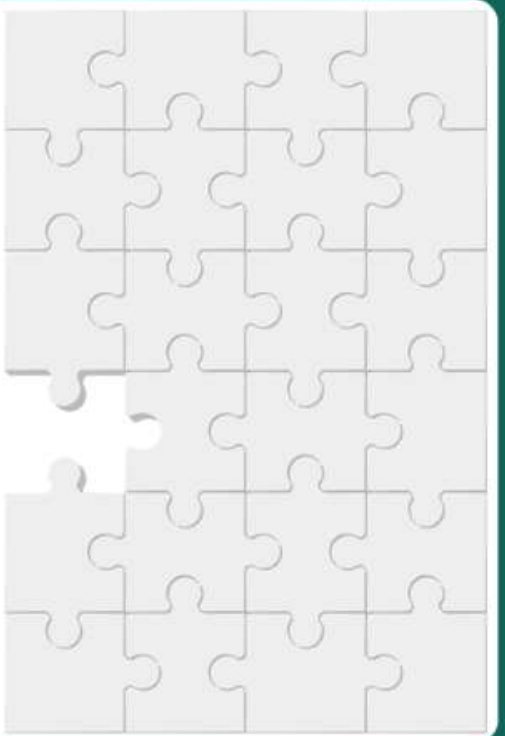
أمثلة عن حالات التدقيق في بيئة تقنية المعلومات

- من خلال تحليل بيانات الرواتب في أحد الجهات الحكومية باستخدام برنامج تحليل البيانات (IDEA) تكشف للديوان صرف مستحقات أكثر من موظف لحساب بنكي واحد.
- وجود صرف أكثر من مرتب لنفس الموظف على مدى سنتين.
- صرف أكثر من بدل لنفس الموظف
- صرف مستحقات انتداب خلال الاجازات
- صرف مرتبات بعد تاريخ الاستقالة
- وجود أكثر من مسمى لنفس البدل
- من خلال الفحص للتحقق من أعداد الرخص الموردة للجهة يتم مراجعة (Log file) لمقارنته بأعداد الموظفين المستفيدين فعليا من الرخص.

شكراً...

الديوان العام للمحاسبة
General Court of Audit

لنتكامل
Integratus



@SaudiGCA

رقابة تقنية المعلومات في جهاز الرقابة المالية والإدارية للدولة في سلطنة

الاطار القانوني لرقابة تقنية المعلومات

قانون جهاز الرقابة المالية والإدارية للدولة الصادر بالمرسوم السلطاني رقم 111/2011:

المادة (8) يهدف الجهاز الى بيان أوجه النقص أو القصور في الأنظمة المالية والإدارية المعمول بها واقتراح وسائل علاجها.

المادة (10) : للجهاز في سبيل ممارسة اختصاصاته ربط الأنظمة الإلكترونية المعمول بها في الجهات الخاضعة لرقابته بالجهاز.

الأدلة المعتمدة لتنفيذ مهام رقابة تقنية المعلومات:

1- دليل الرقابة على تقنية المعلومات الصادر من جهاز الرقابة المالية والإدارية للدولة بسلطنة عمان ،

2- دليل تدقيق تكنلوجيا المعلومات لأجهزة الرقابة العليا – مجموعة عمل الانتوساي لتدقيق تكنلوجيا المعلومات

قسم الاسناد الرقابي

قسم تابع لدائرة تقنية المعلومات بالجهاز تم استحداثه مؤخرا.

تقديم الدعم والاسناد لأعضاء فرق الفحص بمهام الرقابة على تكنلوجيا المعلومات من خلال توفير الأعضاء الرقابيين بتخصصات مرتبطة بتكنلوجيا المعلومات (التحول الرقمي ، الشبكات ، النظم والتطبيقات ، البرمجة)

الأنظمة الالكترونية التي يعتمد عليها العضو الرقابي

- أنظمة الكترونية لتحليل البيانات ACL
- نظام العمل الرقابي (AMS)
- ربط الكتروني Oman Sai Mate

مهام رقابة منفذة في مجال تقنية المعلومات

السنة	عددها
2019	2
2021	1
2023	2

- كما يتم فحص أنظمة تقنيات المعلومات في مهام المطابقة والالتزام ورقابة الأداء والرقابة الادارية

مواضيع الفحص

الضوابط العامة لتقنية المعلومات	ضوابط التطبيقات
حوكمة تكنلوجيا المعلومات	إجراءات التوثيق وحفظ مستندات النظام
ضوابط التطوير والاقتناء	فحص واختبار النظام
ضوابط الاستعانة بمصادر خارجية	ضوابط فصل المسؤوليات والواجبات
ضوابط إدارة استمرارية الاعمال	ضوابط المدخلات
ضوابط امن التشغيل	ضوابط العمليات
ضوابط الوصول الى المعلومات وإدارة أسماء المستخدمين وكلمات المرور	ضوابط المخرجات
ضوابط الرقابة على الانظمة	

امثلة من ملاحظات مبلغة من مهام الرقابة على تقنية المعلومات

- لم يتم إعداد وإعتماد سياسة عامة لأمن المعلومات بالوزارة بالرغم من أهميتها وأثرها البالغ في حماية الموارد المعلوماتية للوزارة من المخاطر.
- لم يتم اعداد واعتماد دليل مدير النظام (Admin User Manual) و دليل المستخدم (User Manual)
- عدم وجود سجلات بيانات الدخول (Logs Files) وسجلات التتبع (Audit Trail) في نظام وقواعد بيانات الأنظمة بالوزارة لتسجيل العمليات وحفظ السجلات وتسجيل التغييرات على كافة الأنظمة وقواعد البيانات
- لم يتم توقيع موظفي الوزارة وفني الشركة (غير عماني) المنفذة لخدمات التقنية بالوزارة (طرف ثالث) على اتفاقية عدم الإفصاح والتي تشمل على بنود الخصوصية بما يضمن التزامهم بقوانين واجراءات الوزارة.
- لم يتم اعداد سياسة وخطة لاستمرارية خدمات تقنية المعلومات الضرورية للاستجابة للحالات غير الاعتيادية أو الطارئة لاستمرار خدمات تقنية المعلومات فضلاً عن عدم اعداد سياسة لاستعادة الأوضاع من الكوارث والخاصة بإسترداد البنية التحتية لتقنية المعلومات (مثل: أنظمة التشغيل والتطبيقات ، أجهزة التخزين ، نظام ادارة قواعد البيانات ، وغيرها) واختبارها بعد وقوع الكارثة.

امثلة من ملاحظات مبلغة من مهام الرقابة على تقنية المعلومات

- منح بعض الموظفين عدة صلاحيات تتعلق بعمل أكثر من دور وظيفي والذي يشير الى عدم وجود فصل في المسؤوليات عند منح تلك الصلاحيات.
- منح صلاحيات لبعض الموظفين لأعمال غير مرتبطة بالدوائر التي يعملون بها
- عدم الغاء/تعطيل صلاحيات الموظفين المستقيلين

احكام صادرة لجرائم إساءة استخدام تقنية المعلومات

أقدم أحد موظفي دائرة الشؤون الإدارية بإحدى الوزارات على شبهة إساءة استعمال الوظيفة والتزوير الإلكتروني من خلال قيامه باعتماد عدد من العقود الوهمية إلكترونيا وإدخال كشوفات الحضور الشهري لعدد من العقود الخاصة بالعاملين بالأجر اليومي بخلاف الواقع ترتب عليه صرف مبالغ دون وجه حق. بهدف الحصول على منفعة له ولغيره

ادانة المتهم عن جنابة الاختلاس للمال العام بالتزوير و عن جناية التزوير المعلوماتي و عن جنحة إساءة استعمال الوظيفة العامة والإخلال بواجباتها الوظيفية وإدانته و عن جنحة استغلال المنصب ومعاقبته بالسجن والغرامة والعزل من الوظيفة ومن تولي الوظائف العامة ،

احكام صادرة لجرائم إساءة استخدام تقنية المعلومات

أقدم أحد موظفي إحدى البلديات على شبهة جريمة الرشوة وشبهة جريمة غسل أموال غير معروفة المصدر ، وشبهة استخدام وسائل تقنية المعلومات لارتكاب جريمة التزوير المعلوماتي في النظام الإلكتروني للبلدية من خلال تجاوز شرط التفتيش الفني والصحي الميداني اللازم للحصول على الموافقة

إدانة المتهم الأول بالعقوبة الأشد عن جناية غسل الأموال وبمعاقبته عنها بالسجن والغرامة وعزل المتهم عن وظيفته وحرمانه من تولي الوظائف العامة بصورة مطلقة. وإدانة المتهم الثاني بالعقوبة الأشد عن جناية الرشوة ومعاقبته بالسجن وبالغرامة

شكرا لكم

مخاطر التّشغيل الالكتروني للبيانات وكيفية اكتشاف وسائل الغش ومواطن الفساد

تجربة محكمة المحاسبات بتونس

تاريخ العرض: 25 أكتوبر 2023

مكوّنات العرض

1. مقدّمة عامّة
2. التّشغيل الالكتروني : المزايا والمخاطر
3. مراحل الرقابة على أنظمة المعلومات
4. تقديم الحالة العمليّة
5. أبرز الملاحظات
6. توصيات محكمة المحاسبات

مقدّمة عامّة

أهمية تكنولوجيا المعلومات

الأداة الضّروريّة لإصلاح وتحديث القطاع العامّ بهدف إرساء إدارة أكثر نجاعة وأكثر قربا من مختلف المتعاملين معها وتوفير خدمات ذات قيمة مضافة.

توجهات الدولة التونسية

الاستراتيجية الوطنية لتطوير الإدارة الالكترونية بهدف تحديث أساليب العمل الإداري والرفع من أداء المؤسسات الاقتصادية وإحداث الفارق في حياة المواطن من خلال تقديم خدمات أكثر نجاعة وفاعلية.

الإطار القانوني والمرجعي

- القانون عدد 5 لسنة 2004 المؤرخ في 03 فيفري 2004 والمتعلق بالسلامة المعلوماتية
- القانون الأساسي عدد 63 المؤرّخ في 27 جويلية 2004 والمتعلّق بحماية المعطيات الشّخصيّة ونصوصه التّرتيبيّة
- منشور عدد 24 لسنة 2020 مؤرخ في 5 نوفمبر 2020 حول تدعيم إجراءات السلامة المعلوماتية بالهياكل العمومية.

- منشور الوزير الأول عدد 10 المؤرّخ في 20 ماي 2011 حول نظم المعلومات والاتصال.
- منشور الوزير الأول عدد 19 المؤرخ في 11 افريل 2007 حول تدعيم إجراءات السلامة الم

التّشغيل الالكتروني

المزايا

- الترفيع في كفاءة العمل والإنتاجية
- سهولة الوصول إلى البيانات والمعلومات وتقاسمها

المخاطر المحتملة ونقاط الضّعف

- فقدان أو التلاعب بالمعطيات وتزويرها نتيجة أعطال أو سرقات
- المسّ من أمن المعطيات ومن خصوصيّتها
- الغشّ والفساد بهدف تحقيق مكاسب غير قانونيّة

أمثلة من المهمات الرقابية

الصندوق الوطني للتأمين على المرض	الصّندوق الوطني للضمان الاجتماعي	الصّندوق الوطني للتقاعد والحيطة الاجتماعية
• سنة الإنجاز 2015 • الفترة الرّقابيّة 2009-2014	• سنة الإنجاز 2016 • الفترة الرّقابيّة 2010-2015	• سنة الإنجاز 2018 • الفترة الرّقابيّة 2012-2017

مراحل الرقابة على أنظمة المعلومات في القطاع الصحي

المرحلة 1:

التعرف على نظام المعلومات وتحديد نطاق مهمة الرقابة

المرحلة 2:

مراجعة محيط الرقابة المعلوماتية وإجراءاته

المرحلة 3:

اختبارات الرقابة على مستوى التطبيقات المعلوماتية

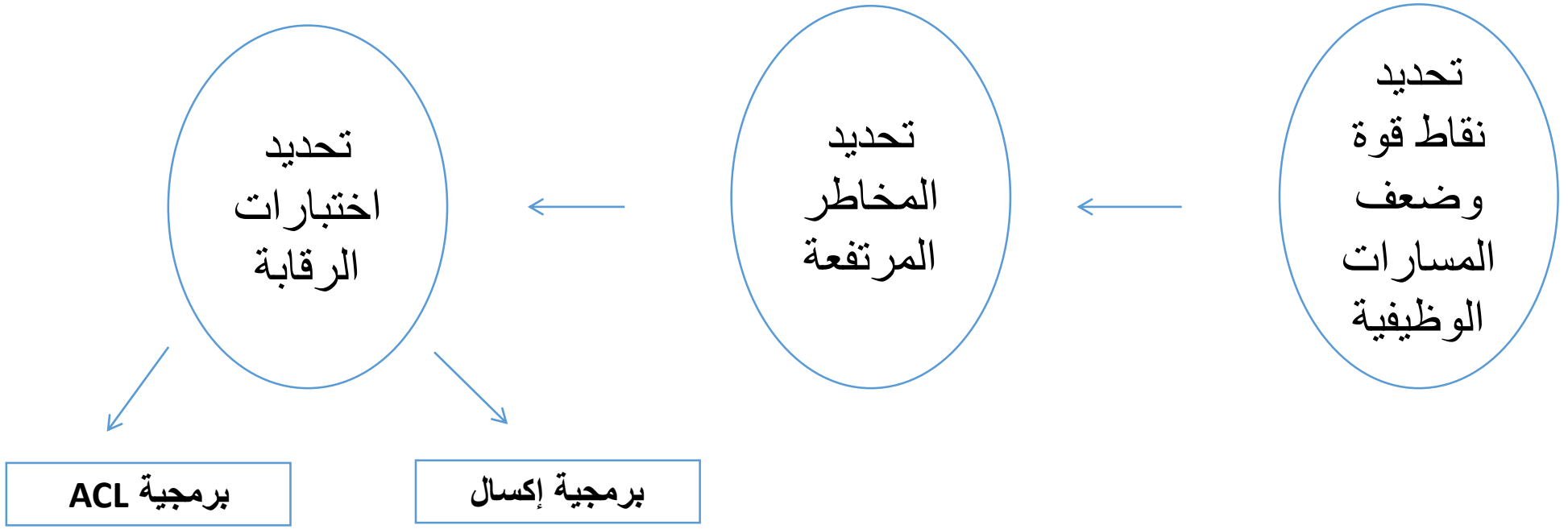
التعرف على نظام المعلومات وتحديد نطاق مهمة الرقابة

- التعرف على محيط نظام المعلومات
- التعرف على التطبيقات الجوهرية وتطبيقات المساندة والبنية التحتية المرافقة
- التعرف على مسارات المعلومة (ترابط أو اندماج التطبيقات□ مرجعيات قواعد البيانات...)
- تحديد إجراءات الرقابة الآلية وقائمات الرقابة المستخرجة آليا من التطبيقات المعلوماتية

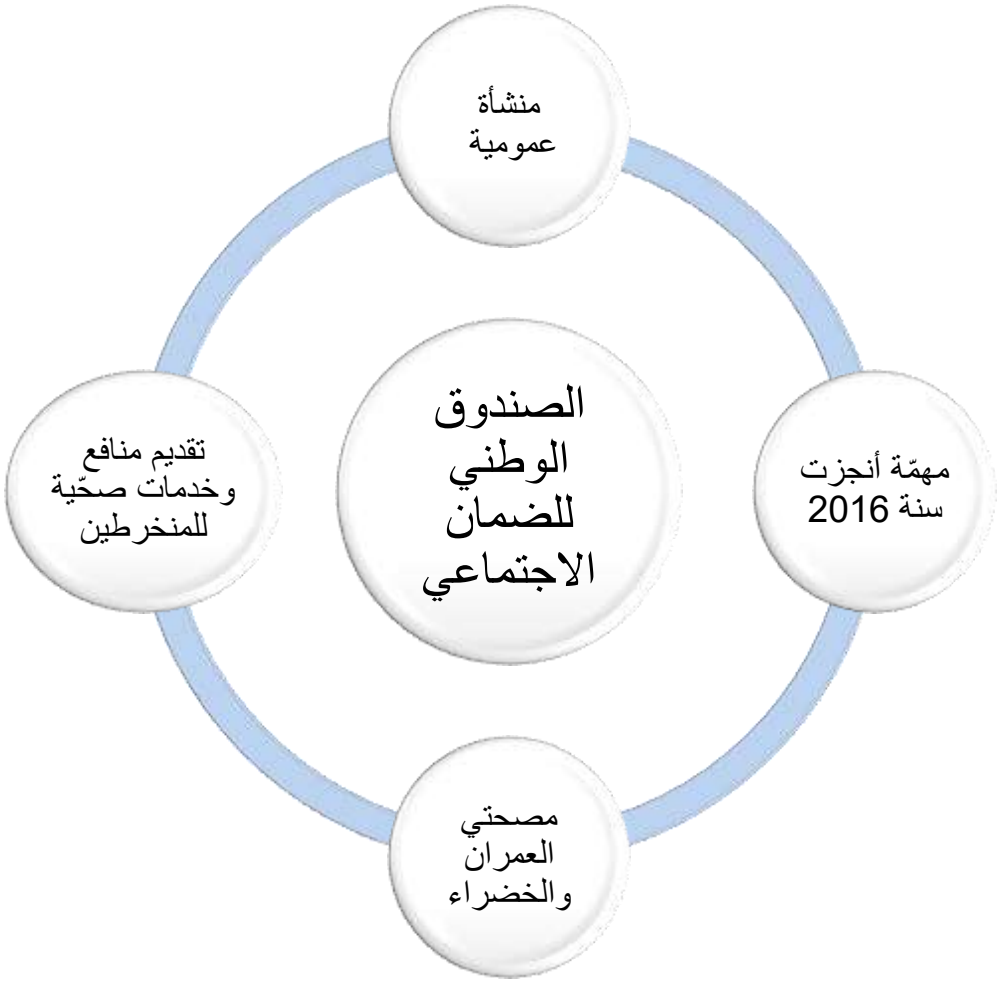
مراجعة محيط الرقابة المعلوماتية وإجراءاته

- التعرف على تنظيم الهيكل الإداري المكلف بالإشراف على نظام المعلومات ("إدارة الإعلامية"/ "إدارة نظم المعلومات"...) وآليات ومسارات الإشراف المتوفرة لديه
- النفاذ إلى التطبيقات والبرمجيات المعلوماتية
- التصرف في عمليات التحيين وإدراج التعديلات على التطبيقات والبرمجيات المعلوماتية
- التصرف في عمليات الاقتناء أو تطوير تطبيقات جديدة
- مخطط استعادة النشاط في حالة الكوارث أو الأزمات (plan de reprise de l'activité).

اختبارات الرقابة على مستوى التطبيقات المعلوماتية



الحالة العملية: الصندوق الوطني للضّمان الاجتماعي



التأكد من مدى أداء دور المصحتين بالجودة والكفاءة والفعالية اللازمة من حيث التصرف الإداري والمالي، اسداء الخدمات الصحية والتصرف في الأدوية

أبرز الملاحظات

- ✓أدّى عدم ارتباط التطبيقات المركزيّة للصندوق بتطبيقتي المحاسبة والتصرف في الأعوان على مستوى المصحّتين إلى تضارب في الوضعية الإدارية لبعض الأعوان (اختلاف مستوى السلّم والصّنف الإداري ...) تسبّب في وجود مستحقات غير مسدّدة لبعضهم وخاصّة المرتبطة بمنح الإحالة على التقاعد.
- ✓أدّى عدم ارتباط تطبيقتي المكتب المركزي للتّسجيل والمواعيد وال المصحّتين إلى انتفاع مرضى بالأدوية دون تسجيل.

أبرز الملاحظات

- مقاربة بيانات المنتفعين بخدمات طبية بمصحتي العمران والخضراء أسفرت عن وجود 23078 منتفعا مسجلا بمصحّة الخضراء برقم انخراط غير موجود بسجلاّت الصندوق الوطني للضمان الاجتماعي صرفت لفائدتهم أدوية بقيمة 8,246 م.د.

- مكّنت أعمال المقاربة بين السجلاّت الإعلاميّة المستقاة لدى الصّندوق الوطني للتأمين على المرض مع سجّل صيدليّة مصحّة العمران من الوقوف على 2055 رقم انخراط تمّ بواسطتها صرف أدوية خصوصيّة بمبلغ تجاوز 17,739 م.د خلال الفترة 2010-2015 والحال أنّه لم تصدر للمرضى حاملي أرقام الإنخراط المذكورة أي قرارات تكفّل خلال كامل تلك الفترة

أبرز الملاحظات

- ✓أفضى التدقيق في عينة من نتائج التحاليل البيولوجية إلى استعمال نفس الملفّ الطبي لأكثر من مريض وهو ما تمّ التفطّن إليه من خلال عدم التطابق بين هويّة المريض حسب الملفّ والاسم المدرج بالمطلب أو من خلال التضارب الوارد في نتائج التحاليل وصل في إحدى الحالات حدّ التضارب في فصيلة دم المريض.
- ✓صرف كميات كبيرة من الأدوية (مخدّرة وأخرى تستعمل لعلاج أمراض مزمنة) تتجاوز المقادير القصوى لفائدة مريض دون وجه حقّ وصلت حدّ صرف 34 وصفة في سنة واحدة في ظلّ غياب فحوصات من قبل الأطباء الذين تمّ استعمال رموزهم

أبرز الملاحظات

- ✓مقاربة البيانات الالكترونية للمضمونين الاجتماعيين المنتفعين بخدمات طبية بمصحّة العمران ببنك المعطيات المتوفّر بالصندوق الوطني للضمان الاجتماعي أسفرت عن حالات إسداء خدمات باستخدام أرقام انخراط منتفعين متوفين في تاريخ إسداء الخدمات منذ أكثر من 3 سنوات وحالات يعود فيها تاريخ الوفاة إلى ما يزيد عن 20 سنة مقارنة بتاريخ إسداء الخدمة الطبيّة.

- ✓بلغ عدد المضمونين الاجتماعيين المتوفين في تاريخ إسناد الخدمة الطبية ما عدده 218 مضمونا اجتماعيا بمصحة العمران انتفعوا بما عدده 2223 عيادة طبية و 1348 عملا طبيا تكميليا بكلفة قدرها 17,622 أ.د و 313 فحصا بالأشعّة بكلفة قدرها 8,496 أ.د وصرفت

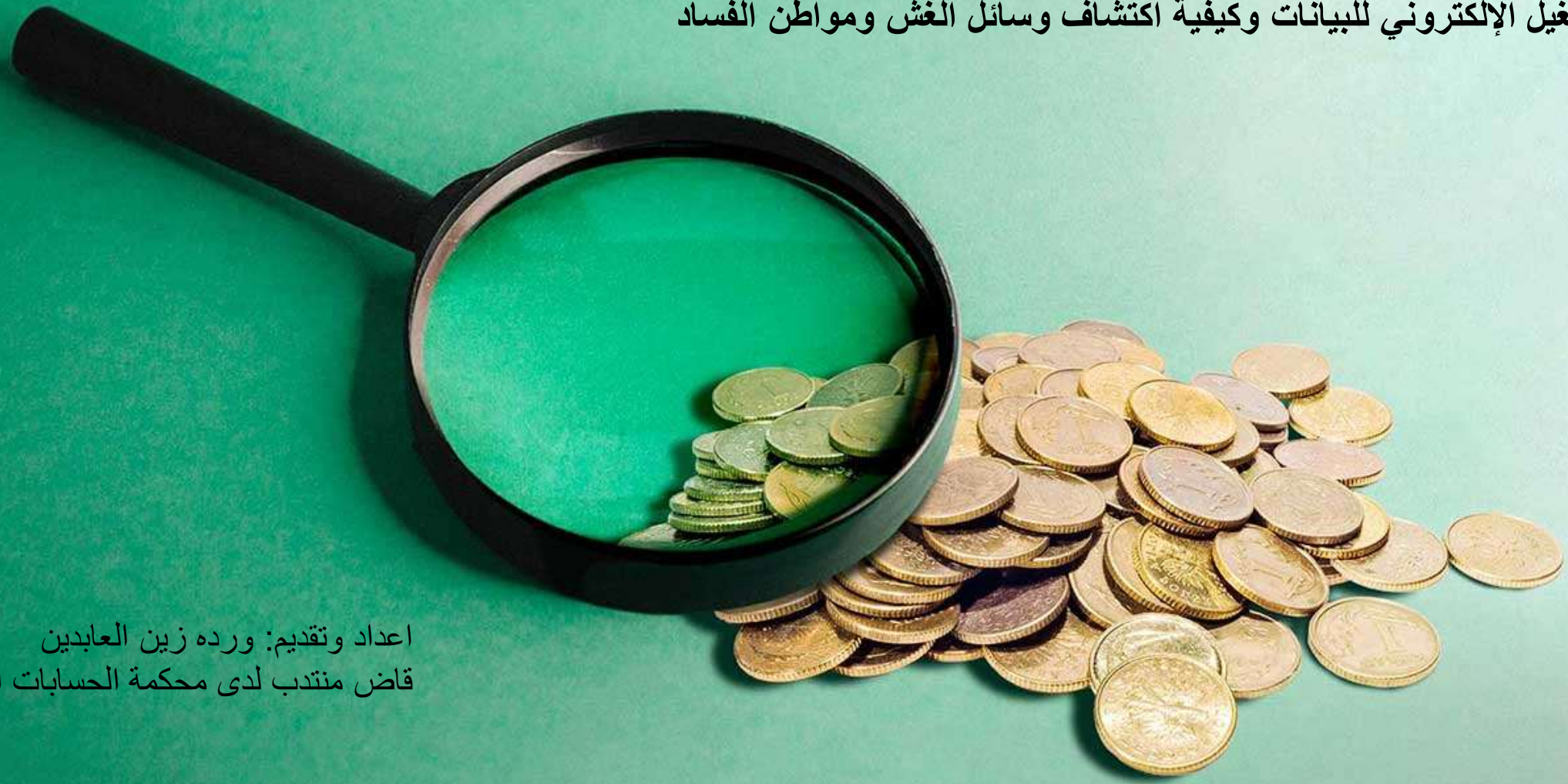
المقترحات والتوصيات

- ✓وجوب احترام التّراتيب الجاري بها العمل وإرساء نظام رقابة داخليّة ناجع واستحثاث تركيز نظام معلومات طبي مندمج بما في ذلك الملفّ الطّبي الموحّد الجامع لكلّ المعطيات المتّصلة بالمريض بما يضمن حسن حوكمة الخدمات الصحّيّة بالمصحّتين؛
- ✓تلافي نقائص النّظام المعلوماتي وتركيز آليات متابعة ومراقبة بين الصّندوق ومصحّتيه بما يساعد على ترشيد التّصرّف فيها وتجنّب إحداث الاخلالات درء للتّجاوزات؛

شكرا على حسن المتابعة

التجربة الموريتانية

مخاطر التشغيل الإلكتروني للبيانات وكيفية اكتشاف وسائل الغش ومواطن الفساد



اعداد وتقديم: ورده زين العابدين
قاض منتدب لدى محكمة الحسابات الموريتانية

01 نبذة عن محكمة الحسابات الموريتانية

02 الإطار القانوني والتشريعي للرقمنة والتحول الرقمي

03 الحالة

04 الخلاصة

محكمة الحسابات الموريتانية

1968

يعود إنشاء رقابة الدولة في موريتانيا إلي سنة 1968.
ذلك أن القانون رقم 68-66 الذي أنشأ هذه الوظيفة يعاقب الاختلاسات و غيرها من طرق الاستيلاء غير الشرعي على المال العام من طرف وكلاء الدولة أثناء ممارساتهم لوظائفهم.

1972

ثم جاء القانون الجنائي سنة 1972 لتمكين مراقب الدولة من القيام بمهام اقتصادية.
في سنة 1972 كانت تتشكل هيكلة الرقابة من 3 مراقبي دولة إلى جانب سكرتاريا.
ثم تم إنشاء وزارة الوظيفة العمومية و الرقابة سنة 1978.

1979

و في سنة 1979 أنشئت الرقابة العامة للدولة تحت السلطة المباشرة للوزير الأول، رئيس الحكومة. حيث كانت الرقابة تدار من قبل مراقب دولة يتمتع برتبة وزير يحضر اجتماعات مجلس الوزراء. يساعده مراقبوا دولة و يحدد مرسوم التنظيم الإداري للرقابة العامة للدولة. حيث تتكون هذه الرقابة من مراقبين اثنين يتبعان لرئيس الدولة و اثنين آخرين للوزير الأول.

1987

ثم أعيد نظام الرقابة العامة للدولة في سنة 1987 عن طريق إنشاء الوزارة المكلفة بالرقابة العامة للدولة و كانت الرقابة المقام بها ذات طبيعة إدارية و لا تشكل رقابة تسيير حقيقية حيث و لم يكن هناك برنامج للرقابة. ذلك أن هذه الأخيرة تتم بطلب من السلطة التنفيذية.

1991
1993

و قد حلت محكمة الحسابات محل الرقابة العامة للدولة بموجب دستور 20 يوليو 1991 في مادته 68. و قد صدر القانون رقم 19-93 المتعلق بصلاحيات و اختصاصات محكمة الحسابات بوصفها الهيئة العليا للرقابة المالية، في 26 من يناير1993.

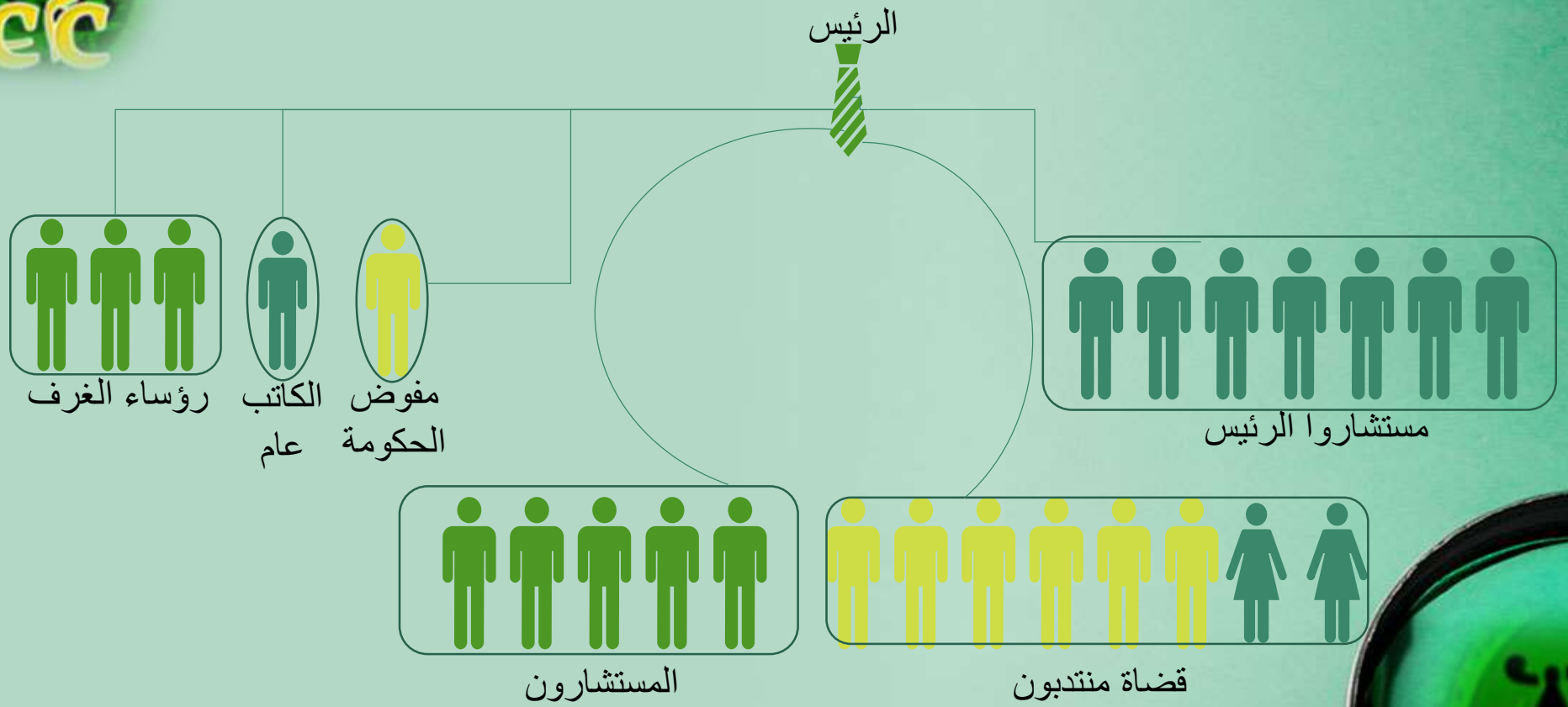
تساهم محكمة الحسابات بعملها الدائم والمنظم في مجال التدقيق والتقييم والإعلام والمشورة في تحقيق الأهداف المبينة أدناه

تستهدف الرقابة المسندة إلى محكمة الحسابات كشف أي انحراف أو خرق أو مخالفة للقواعد القانونية وتلك المتعلقة بالتسيير بحيث يمكن في كل حالة القيام بالتصحيحات الضرورية أو مساءلة الأشخاص المعنيين أو الحصول على التعويض أو اتخاذ تدابير من شأنها تفادي وقوع مثل هذه التصرفات أو جعل ارتكابها أكثر صعوبة في المستقبل.

تمارس هذه الرقابة بصورة لاحقة على الوثائق وفي عين المكان، بصفة شاملة أو عن طريق العينات على شكل قضائي أو إداري.

تبدي محكمة الحسابات رأيا استشاريا بناء على طلب الحكومة، حول النصوص المتعلقة بالتنظيم ورقابة الأموال العمومية.

الهيكل التنظيمي



الإطار القانوني والتشريعي

01 القوانين

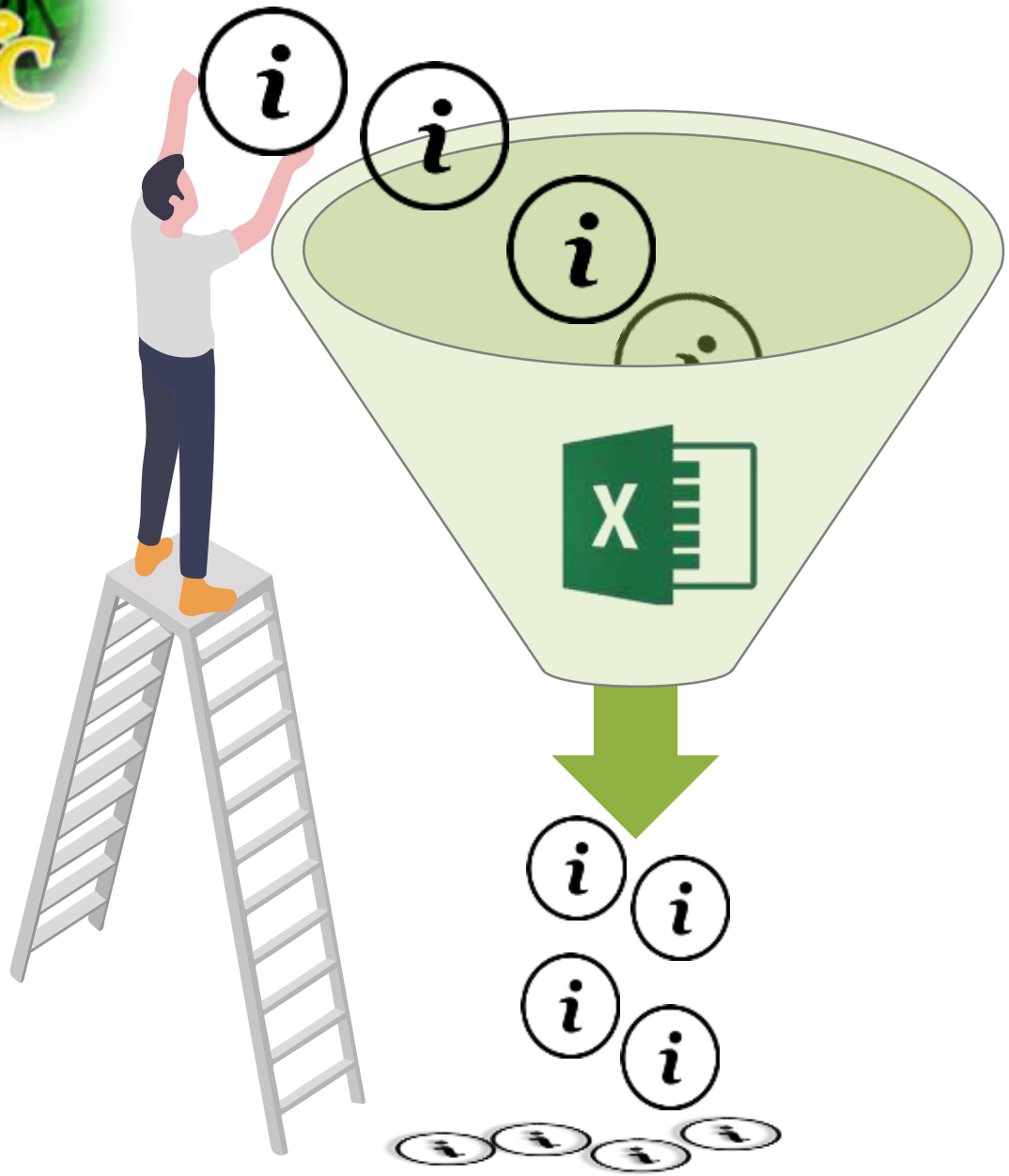
- القانون المتعلق بالجريمة السبرانية رقم 2016-007
- القانون التوجيهي لمجتمع المعلومات رقم 2016-006
- قانون رقم 2013-025 المتعلق بالاتصالات الالكترونية
- القانون 2016- 014 المتعلق بمكافحة الجرائم المرتبطة بالفساد

02 المراسيم

- مرسوم يتعلق بحفظ البيانات الإلكترونية والفرز تطبيقا لبعض أحكام القانون رقم 2018-022 المتعلق بالمعاملات الإلكترونية
- مرسوم يتعلق بالتبادلات الإلكترونية بين المستخدمين والسلطات الإدارية وفيما بين السلطات الإدارية
- مرسوم يتعلق بتشكيلة وتنظيم وسير عمل سلطة حماية البيانات ذات الطابع الشخصي

رواتب الموظفين العموميين

قبل سنة 2011



كان يتم تسجيل بيانات الموظفين العموميين على لوائح EXCEL و من ثم إدخالها في برنامج آخر لمعالجة الرواتب و الأجور.

الخروقات

مما أدى الى ظهور حالات رواتب مزدوجة أي المعرف المالي الواحد يتم تقييده لأكثر من راتب ولدى اكثر من جهة احيانا.

في سنة 2011

تم اطلاق نظام الرشاد لتسيير جميع النفقات العمومية وخصص الجزء الأول من الميزانية لرواتب الموظفين العموميين.

تم ربط المعرف المالي بالرقم الوطني.

الرقم الوطني	الاسم	المعرف المالي	الراتب
XXX XXX	احمد	0000001A	XXX
YYY YYY	محمد	0000002B	XX
ZZZ ZZZ	محمود	0000003C	X

الحالة

في اطار مهمة تفتيش لوزارة تم طلب لوائح موظفي أحد المشاريع التابعة للوزارة و تبين أنه يتم صرف رواتبهم من خلال الجزء الأول من الميزانية كموظفين عموميين، علما بأنه يوجد من ضمنهم مقدمي خدمات بعقود مؤقتة، وبعد التحريات توصلت البعثة الى أنه تم انشاء معرفين ماليين لإثنين منهم بأرقام بعيدة جدا من التسلسل الطبيعي للمعرفات المالية النظامية. تم رفع الملاحظة لإدارة التنسيق ونظم المعلوماتية في الإدارة العامة للميزانية و بالتعاون مع المحكمة تم تحديد المسؤول عن هذه العملية وتشديد القيود على الوصول الى النظام.

الخلاصة

أظهرت تجربتنا في المحكمة أن إدارة مخاطر البيانات الإلكترونية، واكتشاف الاحتيال، ومنع الفساد تتطلب مزيجًا من المهارات التقنية، والأدوات المتقدمة، والتعاون الوثيق مع جهات حكومية أخرى، باستخدام أساليب تدقيق ملائمة لكل حالة.

شكرا لحسن استماعكم

الجهاز المركزي للرقابة والمحاسبة -
الجمهورية اليمنية

تقييم إجراءات تنفيذ الأعمال عبر أنظمة المعلومات

دراسة حالة تم تطبيقها في عملية مراجعة للهيئة العامة للتوفير البريدي –

حسابات التوفير البريدي-

مراجع نظم معلومات/ فيصل الربيعي

قبل الزيارة الميدانية

1. ما **الضرورات الملحة** لتنفيذ عملية المراجعة ؟
   - **بلاغات عن قضايا فساد مالي وإداري**
   - **تقييم روتيني لأداء الجهة في تشغيل البيانات الإلكترونية**
2. ماهي التوقعات حول **نوع البيانات** التي يتوجب على الفريق جمعها ؟
3. ماهي التوقعات حول **تعاون الجهة** في توفير البيانات ؟

قبل الزيارة الميدانية

خلفية عن خدمة التوفير البريدي

1 قانون رقم (64) لسنة1991م بشأن البريد والتوفير البريدي

يهدف صندوق التوفير البريدي إلى تقديم خدمات مالية مصرفية لتشجيع صغار المدخرين على ادخار أموالهم وتجميع المدخرات لتوظيفها واستثمارها بأفضل الطرق مما يسهم في تدعيم بنيان الاقتصاد الوطني، مع ضمان توفير الفائدة للمدخرين، كما يهدف صندوق التوفير البريدي إلى تنمية الوعي الادخاري لدى المواطنين

2 تقارير سابقة عن مراجعة خدمة التوفير البريدي

يقدم صندوق التوفير البريدي خدماته من خلال نظام معلومات يعمل عبر شبكة معلومات منتشرة في 360 مكتب بريدي.

تقييم مستوى الكفاءة والفاعلية في إدارة البيانات المالية لحسابات التوفير

تقييم أداء النظام وأمنه.

1 فهم مبدئي للنظام

- تاريخية : مراحل البناء والتطوير – أساليب وأدوات التطبيق والتنفيذ، المطورون، الاختبار، نقاط الفشل والمعالجات والتوثيق المصاحب لها.
- نظام التشغيل، قاعدة البيانات
- وظائف (عمليات) النظام: الرئيسية والأساسية والعلاقات بينها.
- مخطط جداول البيانات والبيانات الترابطية بينها.
- تأثيرات تنفيذ كل وظيفة على البيانات.
- العناصر الرقابية على البيانات .
- عمليات التقييم للنظام .

نقاش مع مدير النظم (مسؤول النظام)

الزيارة الميدانية

فهم بيئة عمل نظام معلومات التوفير البريدي

2 إدارة نظم المعلومات

- المهام والواجبات المتعلقة بإدارة النظم.
- الهيكل التنظيمي للإدارة.
- الخبرة، الكفاءة للفريق .
- المسؤوليات

الزيارة الميدانية

تقييم الرقابة الداخلية على البيانات وموارد تكنولوجيا المعلومات

1. تحديد الضوابط العامة
   - سياسات
   - إجراءات
   - قواعد
2. تحديد تعقيدات أنظمة المعلومات
   - المخططات الوظيفية Functional Charts
   - الهيكل التنظيمي للهيئة
   - الدليل الفني لقاعدة البيانات (جداول البيانات الرئيسية)
   - مخطط وظائف النظام والأنظمة ذات العلاقة
3. توثيق الملاحظات
   - دراسة النتائج
   - تحديد المخاطر
   - وضع خطة الفحص الجوهري

الضوابط العامة في بيئة تكنولوجيا المعلومات

3 فحص جوهري

2 تقييم اولي

1 قبل النزول الميداني

مخرجات

مخرجات الضوابط العامة
السرية التكامل الوفرة

معالجة

اجراءات وقواعد التشغيل الالكتروني للبيانات

رقابة الامتثال	رقابة الوصول للبيانات والملفات	ضمان الاستعادة واستمرارية العمل	إدارة التغيير	التوثيق

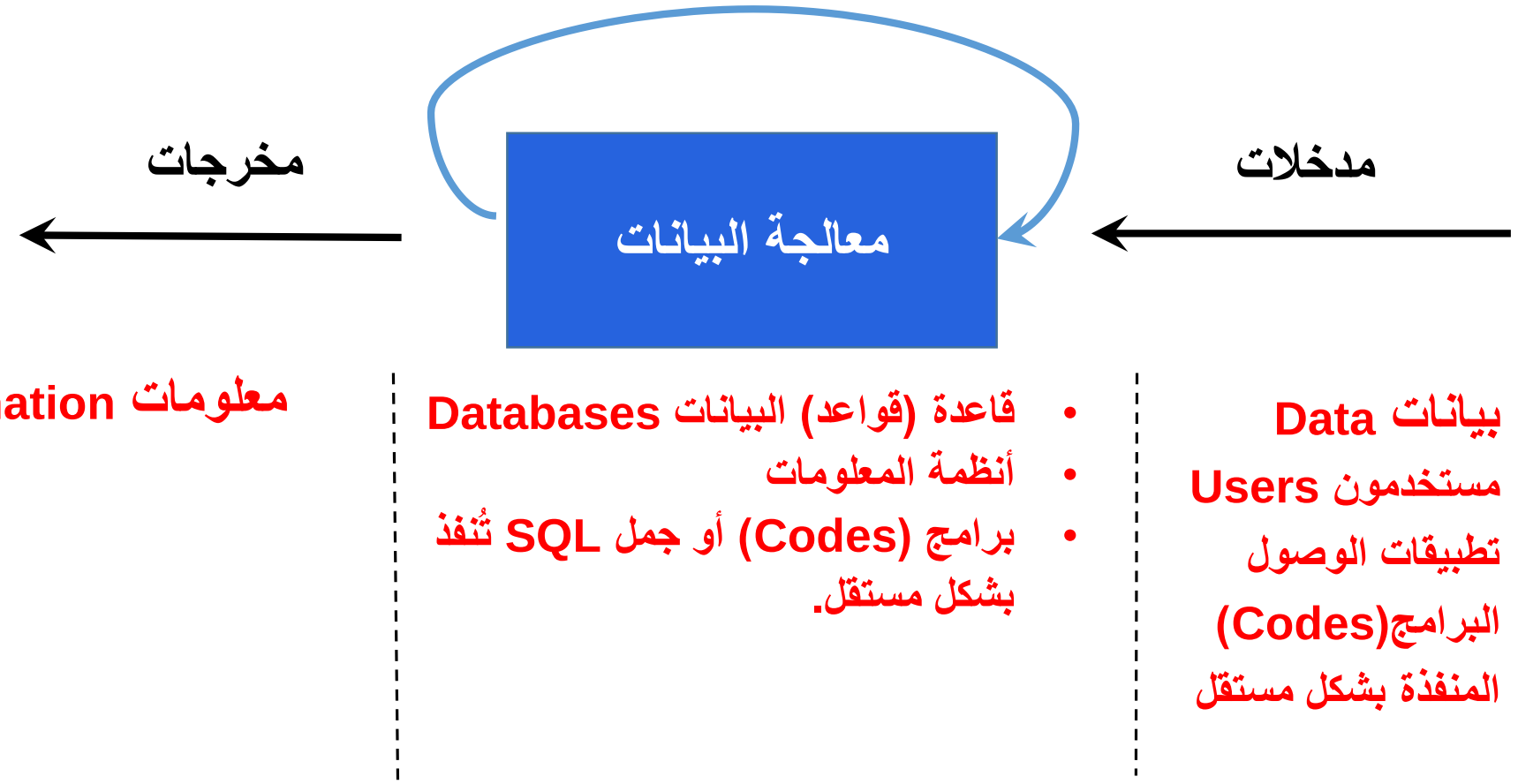
مدخلات

قانون إنشاء الخدمة – الهيكل التنظيمي – استراتيجية نظم المعلومات – اللائحة التنظيمية – تحديد موارد تكنولوجيا المعلومات (المادية ، البيانات)
لها مرجع قانوني ، تتعلق ببيانات نطاق المراجعة ، تتعلق بالرقابة التنظيمية وأمن البيانات

تفاصيل

* مدخلات، معالجة، مخرجات : تشير هنا الى المصادر التي يستند عليها في وضع الضوابط العامة ونتائج العمل بها .

تعقيدات أنظمة المعلومات



تفاصيل

تعقيدات أنظمة المعلومات

البيانات المطلوبة

مدخلات ← معالجة البيانات ← مخرجات

1. قائمة بالمدخلات الرئيسية.
2. قائمة بالوظائف الرئيسية (أنواع العمليات)
3. قائمة بمجموعات المدخلات، بحسب كل وظيفة.
4. مصادر البيانات ووسائل وأدوات إدخالها وحفظها في قاعدة البيانات .

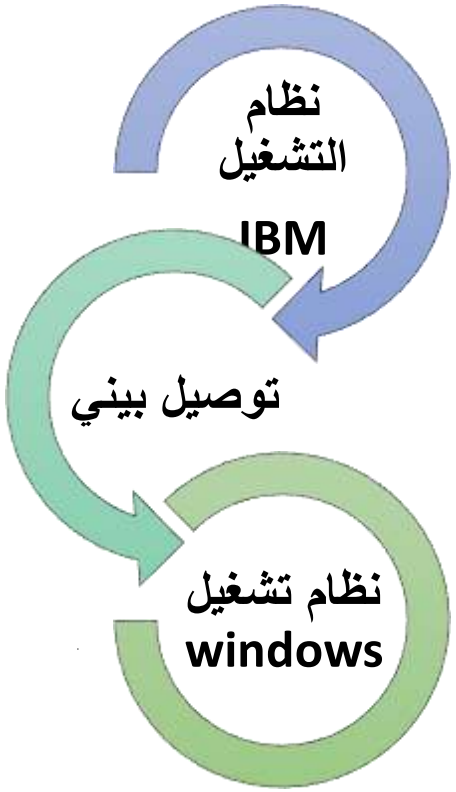
1. قائمة بأنظمة المعلومات
2. برامج (Codes)أو جمل SQL تُنفذ بشكل مستقل.
3. الوظائف الرئيسية وجداول البيانات الأساسية المتعلقة بها.

معلومات Information

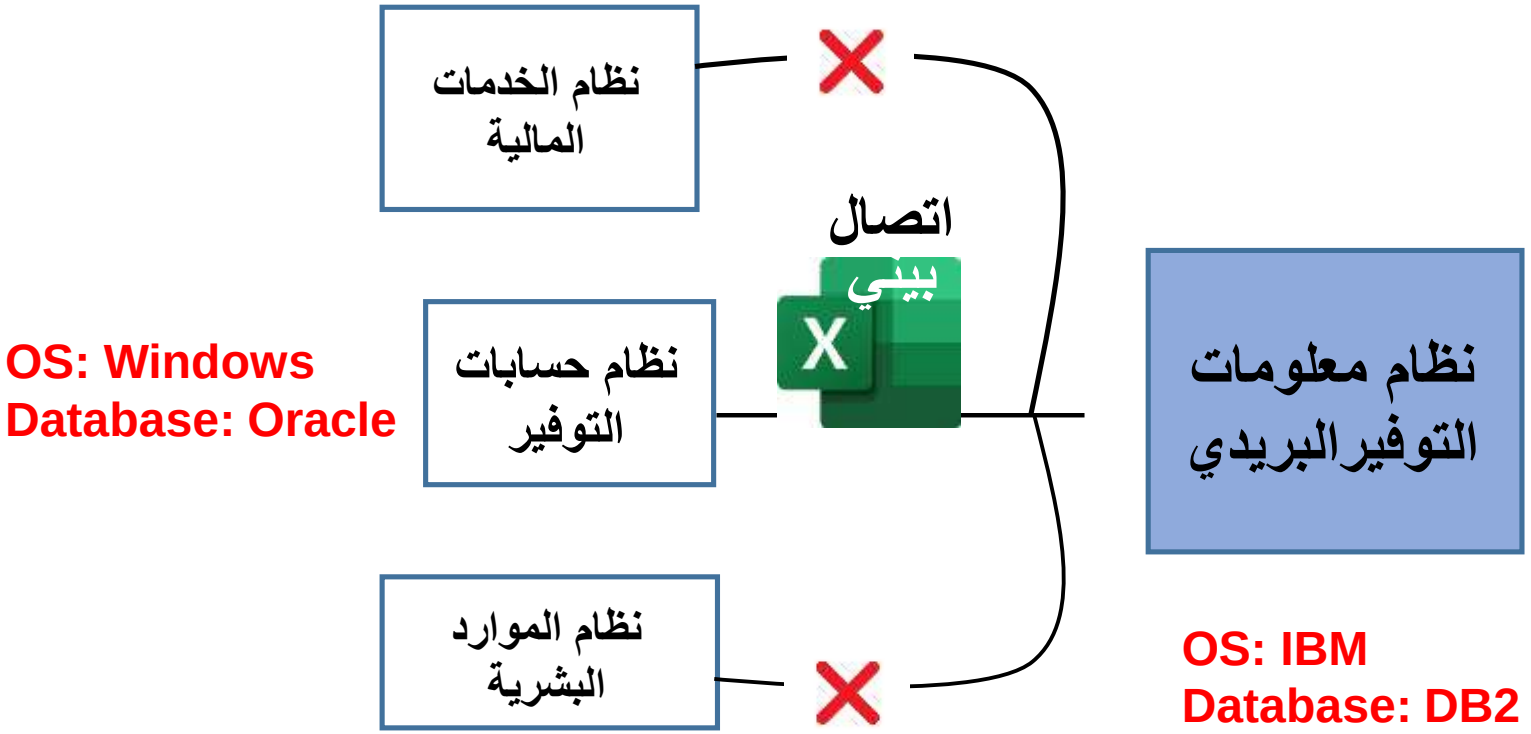
1. قائمة بالمخرجات
2. تحديد الوظائف
3. تحديد المخرجات لكل وظيفة

تفاصيل

تعقيدات أنظمة المعلومات



التوصيل البيني



1. تحديد نظام التشغيل وقاعدة البيانات لكل نظام
2. تحديد طريقة الاتصال البيني مع نظام التوفير

تفاصيل

الزيارة الميدانية

التوثيق

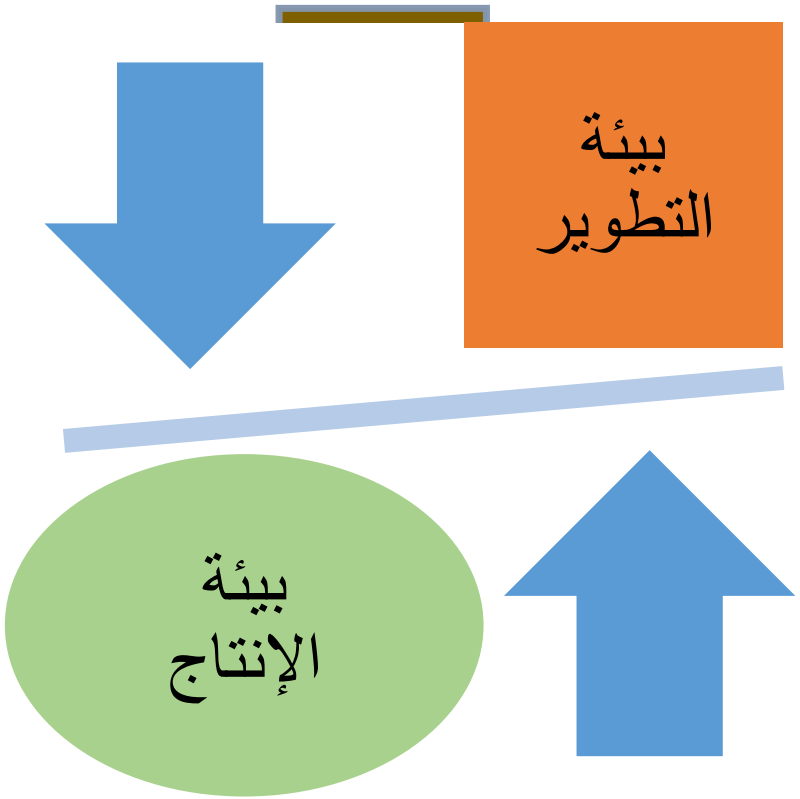
توثيق ملاحظات التقييم الأولي لمخاطر التشغيل الالكتروني للبيانات

دراسة النتائج وتحديد المخاطر

تداخل مهام متعارضة

الوظيفة	المهام المتعارضة
مدير النظم	لديه كافة امتيازات الوصول إلى البيانات
مسؤول عن تطوير الأنظمة	لديه كافة صلاحيات النشر لتحديثات النظام في بيئة الانتاج

فصل المهام المتعارضة



إجراءات ومحاور الفحص الجوهري

5
- عمليات التحديث على:
- كود النظام
- معادلة احتساب الفائدة
- أذون الوصول
- الضوابط الرقابية.

(مثل اغلاق سجل رقابي لمسائل تتعلق بالمساحة التخزينية)

4
- الشمولية
- الاكتمال
- الوصول للملفات

3
- القيود في الواجهات وقاعدة البيانات بهدف إدخال بيانات صحيحة ومتسقة

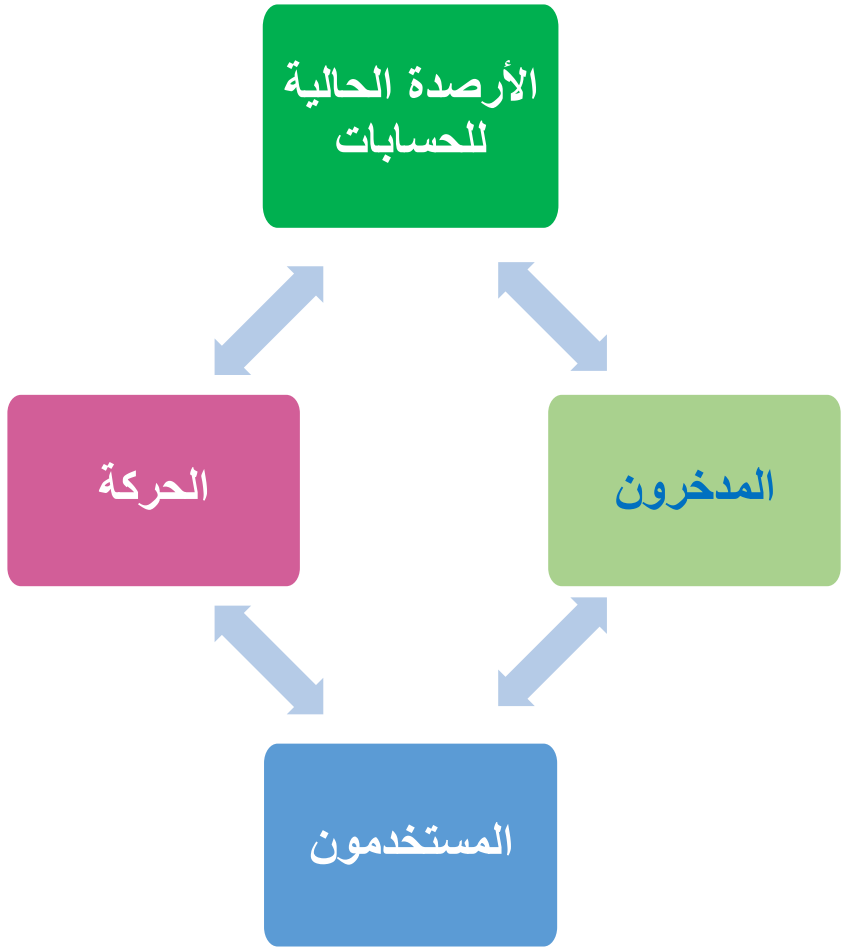
2
- التفويض
- المصادقة
- الوصول للبيانات

1
- البيانات الرئيسية للمدخرين
- حركة الايداعات والمسحوبات
- ارصدة الحسابات
- البيانات الرئيسية للمستخدمين
- الوصول الى البيانات

إجراءات الفحص الجوهري المخططة

تكامل البيانات (النزاهة)

الكيانات الرئيسية لبيانات التوفير البريدي



الاستعلامات SQL جدول بيانات الحركة

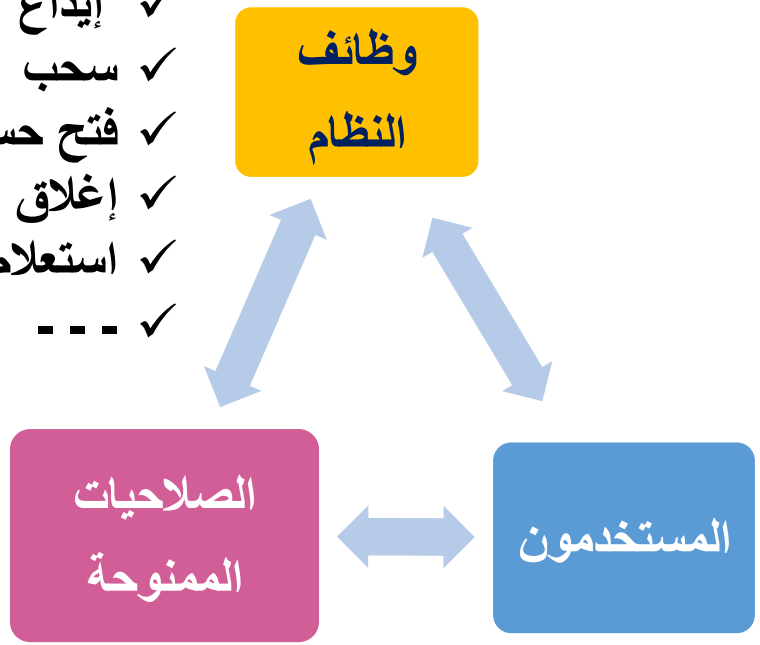
تكامل مع	بيانات جدول الحركة
جدول الحركة	• هل تسلسل ارقام المعاملات لكل حساب سليمة (*لا يوجد فيها فجوات ومتسلسل بحسب تاريخ العملية*).
جدول الارصدة	• هل كل حساب في جدول الحركة يقابله حساب بنفس الرقم في جدول الأرصدة ؟ • هل رصيد حساب يتطابق من حركة الحساب خلال السنة؟
جدول المستخدمون	هل تم تسجيل اسم المستخدم مدخل البيانات ضمن بيانات القيد ؟ هل يوجد اسم المستخدم ضمن بيانات جدول المستخدمين ؟

إجراءات الفحص الجوهري المخططة

تكامل البيانات

بيانات الوصول

الضرورة تتطلب أن يكون أحد أعضاء الفريق متخصص في نظم معلومات

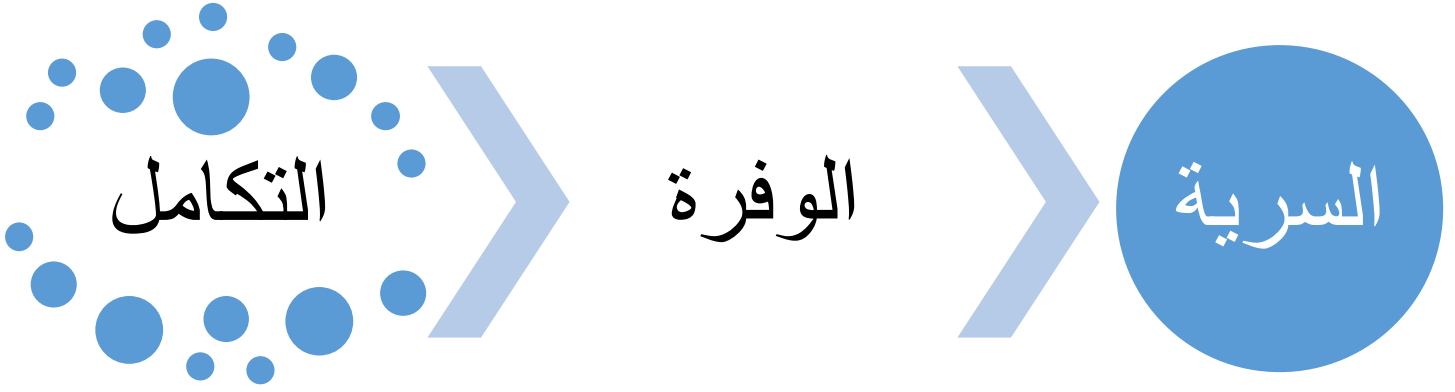


- ✓ إيداع
- ✓ سحب
- ✓ فتح حساب
- ✓ إغلاق
- ✓ استعلام عن رصيد
- ✓ - - -

- ✓ قراءة
- ✓ تحرير
- ✓ تحديث
- ✓ قراءة وتحرير
- ✓ الكل

الأدوات مثل الأذونات وعناصر التحكم الأخرى في وصول المستخدم إلى الملفات أو الى البيانات ، وإدارة هوية المستخدم بشكل جيد جميعها تساعد على ضمان تكامل البيانات.

تأمين الوصول إلى البيانات



الأهداف الرئيسية لأمن المعلومات

- فحص مستوى التعقيد الأدنى المقبول في كلمة المرور
- إظهار اسم المستخدم في الواجهات المفتوحة .
- معلومات المستخدمين المحفوظة في قاعدة البيانات مستوفية.