ديوان المحاسبة الأردني

اللقاء العلمي "الطرق الحديثة للرقابة على الأنظمة المعلوماتية"

7-11 يوليو 2024

- دور تكنولوجيا المعلومات في عمل ديوان المحاسبة الأردني
- أهداف الرقابة على تكنولوجيا المعلومات
- التحديات والفرص
- التجربة الأردنية
- الملاحظات الشائعة
- الرؤية المستقبلية

ديوان المحاسبة الأردني

ديوان المحاسبة هو مؤسسة مستقلة و جهاز رقابي على إيرادات الدولة و نفقاتها، هدفه هو تعزيز النزاهة والمساءلة في إدارة الأموال العامة.

يُعنى الديوان بفحص وتقييم الحسابات المالية والإدارية لمختلف الجهات الحكومية، وتعتبر الرقابة على تكنولوجيا المعلومات أحد المحاور الرئيسية في عمله إضافة الى أنواع الرقابة المالية والالتزام والأداء.

دور تكنولوجيا المعلومات في عمل ديوان المحاسبة

تلعب تكنولوجيا المعلومات دورًا محوريًا في تعزيز دقة وكفاءة عمليات التدقيق واجراءات الرقابة بجميع أنواعها نظرا للتحول الرقمي و استخدام أنظمة المعلومات والخدمات الإلكترونية في أغلب أنشطة الجهات الخاضعة للرقابة .

يقوم ديوان المحاسبة الأردني باستخدام أدوات وبرمجيات متقدمة تمكن ديوان المحاسبة من:

- تحليل كميات كبيرة من البيانات بسرعة ودقة من خلال برامج
(CAATS: Teammate Analyses, IDEA)
- أتمتة اجراءات ومنهجيات الرقابة وحفظ المهام الرقابية وأوراق العمل .
- إعداد تقارير رقابية صحيحة وذات جودة عالية.
- تحسين الإجراءات والعمليات الرقمية في الجهات الخاضعة للرقابة من خلال التوصيات المستندة إلى البيانات .
- الاستعانة بتطبيقات الذكاء الاصطناعي في جميع مراحل التدقيق.

أهداف الرقابة على تكنولوجيا المعلومات في الجهات الخاضعة للرقابة

1. **تقييم وحدات الرقابة الداخلية: في الجهات الخاضعة للرقابة**
   - التأكد من أن نظم الرقابة الداخلية تعمل بفعالية وتحمي أصول المعلومات.
   - ضمان الامتثال للسياسات والإجراءات والمعايير القانونية والتنظيمية.

2. **تحديد وإدارة المخاطر التكنولوجية:**
   - التأكد من تقييم المخاطر المرتبطة بتكنولوجيا المعلومات وتحديد التدابير المناسبة للحد منها.
   - التأكد من تحديد الثغرات الأمنية ونقاط الضعف في الأنظمة.

3. **تحسين الكفاءة التشغيلية:**
   - تقييم أداء أنظمة المعلومات.
   - التأكد من أن نظم المعلومات تدعم تحقيق الأهداف التشغيلية للمنظمة بكفاءة وفعالية.
   - تحسين عمليات تكنولوجيا المعلومات وتقديم التوصيات اللازمة لتحسين الأداء.

4. **ضمان صحة وسلامة البيانات في أنظمة المعلومات:**
   - الـتأكد من فاعلية الضوابط العامة وضوابط التطبيقات.
   - التحقق من أن البيانات دقيقة، متكاملة، ومحفوظة بأمان.
   - مراجعة عمليات النسخ الاحتياطي واستعادة البيانات.

5. **الامتثال للمعايير والإجراءات:**
   - التأكد من التزام الجهات الخاضعة للرقابة بالمعايير الدولية والوطنية المتعلقة بتكنولوجيا المعلومات.
   - مراجعة الامتثال للسياسات الداخلية والخارجية.

التحديات والفرص

التحديات

- التغير السريع في تكنولوجيا المعلومات والتحول الرقمي و ظهور العديد من التقنيات الحديثة.
- الحاجة إلى تحديث مستمر في المهارات والأدوات لمواكبة التطورات التقنية.

الفرص

- تعزيز التعاون مع الجهات الدولية لتحسين أداء العمل الرقابي.
- استثمار أكبر في تكنولوجيا المعلومات لتعزيز كفاءة عمليات التدقيق.
- دعم وتشجيع موظفي الديوان في الحصول على شهادات مهنية دولية متخصصة في جميع أنواع الرقابة ومنها الرقابة على تكنولوجيا وأمن المعلومات.

تجربة ديوان المحاسبة الأردني في الرقابة على تكنولوجيا المعلومات

1. **تطوير البنية الأساسية للرقابة تكنولوجيا المعلومات.**

مشاريع توأمة مع أجهزة الرقابة الأوروبية (جهاز الرقابة الاسباني ، جهاز الرقابة البولندي).

مذكرات تفاهم مع أجهزة رقابية عربية.

تكوين فرق متخصصة في الرقابة على تكنولوجيا المعلومات (تدقيق شمولي ومتكامل ، تدقيق مستقل).

اعتماد معايير الانتوساي والاطارات والمعايير الدولية كمرجعية في تنفيذ مهام التدقيق.

2. **استخدام البرمجيات والأدوات المتقدمة.**

اعتماد برامج تحليل البيانات للكشف عن الأخطاء والتلاعب.

استخدام أنظمة إدارة التدقيق لتتبع وتوثيق العمليات.

3. **التدريب وبناء القدرات.**

تنظيم دورات تدريبية متخصصة لموظفي الديوان لتعزيز مهاراتهم في الرقابة على تكنولوجيا المعلومات(COBIT2019,CISA,ISO27001,ISO22301).

التعاون مع منظمات دولية ومحلية لتبادل الخبرات والمعرفة.

4. **القيام بعدة مهام ناجحة ومتخصصة في الرقابة على تكنولوجيا المعلومات في العديد من المؤسسات الحكومية والجهات الخاضعة للرقابة.**

العمل مع الوزارات والدوائر الحكومية لتحسين نظم تكنولوجيا المعلومات والخدمات الإلكترونية .

تقديم توصيات لتحسين الأمن السيبراني وحماية البيانات والضوابط العامة و ضوابط التطبيقات.

5. **نتائج ملموسة**

اكتشاف الثغرات والمخاطر في النظم المالية والإدارية وأمن المعلومات وتقديم توصيات فعّالة أدت إلى تحسين الإجراءات والحد من الفساد المالي والإداري في نظم المعلومات.

اكتشاف العديد من المخالفات و الملاحظات و نقاط الضعف التي تحتاج الى إجراءات تصحيحية.

إعداد تقارير رقابية متخصصة و ذات نفع للجهات الخاضعة للرقابة أدت الى تحقيق وفر مالي.

الملاحظات الأكثر شيوعا للرقابة على تكنولوجيا المعلومات في الجهات الخاضعة للرقابة

- غياب دور التدقيق الداخلي في تقييم التزام تطبيق سياسة أمن المعلومات الوطنية وضوابط التطبيقات والضوابط العامة لتكنولوجيا المعلومات ومراجعة صلاحيات مستخدمي الأنظمة والشبكات بصورة دورية.
- غياب فصل المهام على مستوى دورة تطوير الأنظمة المحوسبة وإدارة التغييرات (مثال: مدير قاعدة البيانات والمبرمج والفاحص ومطبق التغيير على بيئة العمل الفعلي).
- ضعف ضوابط الوصول المنطقي وإدارة صلاحيات مستخدمي الأنظمة النهائيين وغياب فصل المهام والرقابة المزدوجة على مستوى إجراءات الأنظمة العاملة ، ووجود تضارب في الصلاحيات في الأنظمة العاملة (مثال: موظفي الموارد البشرية والمحاسبة).
- غياب (أو عدم توثيق ومراجعة) السياسات والإجراءات والخطط الخاصة بإدارة مخاطر تكنولوجيا المعلومات وإدارة التغييرات واستمرارية العمل والتعافي من الكوارث.
- عدم وجود فصل بين بيئة اختبار وتطوير الأنظمة (Development &Testing)وبيئة العمل الفعلي (Production).
- ضعف ضوابط إدارة سجلات تتبع حركات مديري قواعد البيانات (DBA)ومستخدمي الأنظمة المميزين (administrators)ومستخدمي الأنظمة النهائيين (end users).
- ضعف ضوابط الإدخال والمعالجة والإخراج وضوابط سلامة قواعد البيانات لبعض الأنظمة المحوسبة.
- غياب وعي واختصاص أمن المعلومات في بعض المؤسسات الحكومية.
- عدم وجود خطة للتدريب وتحليل الاحتياجات التدريبية لتكنولوجيا المعلومات.
- عدم تأهيل كوادر بشرية بديلة للأدوار الرئيسية والحساسة في دوائر تكنولوجيا المعلومات.
- ضعف إدارة الحوادث والمشاكل الفنية وعدم وجود تطبيقات مختصة (مثال: .(Helpdesk
- ضعف الضوابط البيئية والمادية في بعض المؤسسات الحكومية

الرؤية المستقبلية لمجال الرقابة على تكنولوجيا المعلومات في ديوان المحاسبة الأردني:

تسعى الإدارة العليا في ديوان المحاسبة الأردني الى:

- تأسيس دائرة الرقابة على تكنولوجيا المعلومات بشكل مستقل.
- تعزيز بيئة العمل الرقابي لتوفير نظام رقابة قوي وفعال يضمن حماية الأصول الرقمية وتحقيق الامتثال في المعايير والسياسات الداخلية والخارجية في الجهات الخاضعة للرقابة.
- تقديم تقارير دقيقة وموثوقة تساعد في تحسين أداء الأنظمة التكنولوجية وتعزيز الثقة بين مختلف الأطراف ذات العلاقة.
- تطوير مهارات الفريق باستمرار واعتماد أحدث التقنيات لضمان تقديم خدمات تدقيق عالية الجودة تسهم في تحقيق الأهداف الاستراتيجية لديوان المحاسبة الأردني و ترفع من أدائه.

ديوان المحاسبة
AUDIT BUREAU

شكراً

المجلس الأعلى للحسابات بالمملكة المغربية

تجربة المجلس في الرقابة على الأنظمة المعلوماتية

2024

الدكتور محمد عساوي
قاضي مستشار مشرف
رئيس فرع

السيد جواد البيش
رئيس قسم
مديرية الأنظمة المعلوماتية

البرنامج

1. تقديم المجلس الأعلى للحسابات بالمملكة المغربية
2. تدقيق تكنولوجيا المعلومات في المجلس الأعلى للحسابات بالمملكة المغربية
3. أهداف ونطاق تدقيق تكنولوجيا المعلومات بالمجلس الأعلى للحسابات
4. منهجية تدقيق تكنولوجيا المعلومات المعتمدة في المجلس الأعلى للحسابات
5. حالة عملية بالمجلس الجهوي للحسابات بجهة الرباط سلا القنيطرة
6. خلاصة

1. تقديم المجلس الأعلى للحسابات بالمملكة المغربية

- المجلس الأعلى للحسابات مؤسسة دستورية تضطلع بدور المساهمة الفعالة في عقلنة تدبير الأموال العامة وتمارس كليا وظيفتها كمؤسسة عليا للرقابة مستقلة بذات الوقت عن السلطة التشريعية والسلطة التنفيذية

- بناء على الباب العاشر من الدستور المغربي، يتولى المجلس الأعلى للحسابات ممارسة الرقابة العليا على تنفيذ القوانين المالية و يبذل مساعدته للبرلمان و الحكومة في الميادين التي تدخل في نطاق اختصاصاته بمقتضى القانون، و يرفع إلى جلالة الملك نصره الله بيانات جميع الأعمال التي يقوم بها في إطار تقريره السنوي

- أهم الرقابات الممارسة من قبل المحاكم المالية تهم الرقابة القضائية على مدى قانونية العمليات المالية و مدى مطابقتها للنصوص (البت في الحسابات، التسيير بحكم الواقع و التأديب المتعلق بالميزانية و الشؤون المالية)، و مراقبة التسيير المركزة على تقييم نتائج أداء الوحدات المراقبة من حيث الفعالية و الاقتصاد و الكفاءة

2.تدقيق تكنولوجيا المعلومات في المجلس الأعلى للحسابات بالمملكة المغربية

تبني التكنولوجيات الحديثة في عملية التدقيق

لقد أدرك المجلس الأعلى للحاسبات الأهمية الاستراتيجية لعمليات تدقيق تكنولوجيا المعلومات في ضمان نزاهة وكفاءة المؤسسات والأجهزة الخاضعة.

الخبرة المتخصصة

تتوفر المؤسسة على فريق متخصص في تدقيق تكنولوجيا المعلومات من ذوي المهارات اللازمة للتعامل مع مختلف البيئات الرقمية المعقدة.

التحسين المستمر

تتطور وظيفة تدقيق تكنولوجيا المعلومات في المجلس الأعلى للحاسبات باستمرار لمعالجة المخاطر الناشئة والاستفادة من التطورات التكنولوجية الجديدة.

3.أهداف ونطاق تدقيق تكنولوجيا المعلومات

1 ضمان موثوقية النظام المعلوماتي	2 تعزيز الكفاءة التشغيلية	3 تقوية الحوكمة الرقمية
تقييم فعالية ضوابط تكنولوجيا المعلومات والتدابير الأمنية لحماية البيانات والبنية التحتية.	استغلال فرص تحسين العمليات التي تدعم تكنولوجيا المعلومات وتحقيق الاقتصاد في تكاليف القطاع العام المغربي.	تقييم مدى توافق استراتيجيات تكنولوجيا المعلومات مع أهداف الأجهزة المعنية في توافق مع مبادرات التحول الرقمي الوطنية.

4.منهجية تدقيق تكنولوجيا المعلومات المعتمدة في المجلس الأعلى للحسابات

الاسكتشاف

الفهم الشامل لبيئة تكنولوجيا المعلومات، بما في ذلك الأنظمة والعمليات وضوابط التحكم.

اختبار التدقيق

تصميم وتنفيذ إجراءات التدقيق للتحقق من فعالية ضوابط وعمليات تكنولوجيا المعلومات.

تقييم المخاطر

تحديد المخاطر المتعلقة بتكنولوجيا المعلومات وترتيب أولوياتها بناءً على تأثيرها المحتمل واحتمالية حدوثها.

5.حالة عملية: برنامج التدبير التجاري لشركة مفوض إليها تدبير قطاع الماء والكهرباء والتطهير السائل على مستوى جهة الرباط سلا القنيطرة

إبرام عقد التدبير المفوض بين 13 جماعة تابعة لجهة الرباط سلا القنيطرة وشركة ريضال لتدبير مرافق توزيع الكهرباء والماء الصالح للشرب والتطهير السائل دخل حيز التنفيذ ابتداء من فاتح يناير 1999.

Communes	Service délégué		
	Electricité	Eau	Assainissement
Rabat	●	●	●
Salé	●	●	●
Sidi bouknadel	●	●	●
Shoul	●		
Témara	●	●	●
Harhoura	●	●	●
Skhirat	●	●	●
Sidi yahya Zaers	●		
Ain attig	●	●	●
Sabbah	●	●	●
Mers el kheir	●	●	●
Bouznika	●		
Cherrat	●		

حالة عملية: برنامج التدبير التجاري لشركة مفوض إليها تدبير قطاع الماء والكهرباء والتطهير السائل على مستوى جهة الرباط سلا القنيطرة

شركة ريضال شركة مساهمة برأسمال يقدر ب 400 مليون درهم منها نسبة 99% لفائدة Veolia service Environnement

الهدف من مراقبة التسيير:

تقييم التدبير المحاسباتي والمالي للشركة المفوض إليها .

حالة عملية: خريطة المخاطر ومحاور المهمة الرقابية

استنادًا إلى خريطة المخاطر التي وضعها فريق المراقبة، يمثل التدبير المحاسبي لفواتير الاستهلاك والنفقات المسترجعة مخاطر كبيرة للتدبير المفوض مع عواقب على كل من:

- أهمية وموثوقية المعلومات المحاسبية والمالية وأثرها على نتائج السنوات المالية وإدارة السيولة النقدية وحساب فروق الاستثمار ومراجعة الأسعار
- المواطن من خلال فوترة هوامش ربحية إضافية غير تعاقدية لأشغال واستهلاك الكهرباء والماء الصالح للشرب والتطهير السائل
- تحقيق مؤشرات الأداء المنصوص عليها في العقد (نسب الربط، المردودية، جودة الخدمات، الخ)

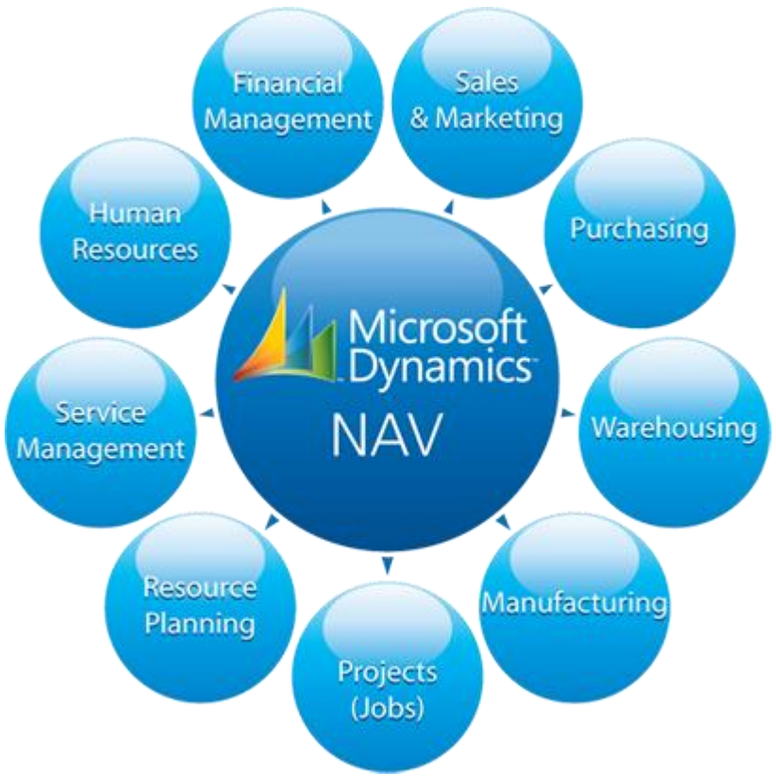
شملت هذه المهمة الرقابية ثلاث محاور :

1. **التدبير المحاسبي والمالي**
2. **النفقات المسترجعة**
3. **التدبير التجاري**

حالة عملية: البيئة المعلوماتية للشركة المفوض إليها

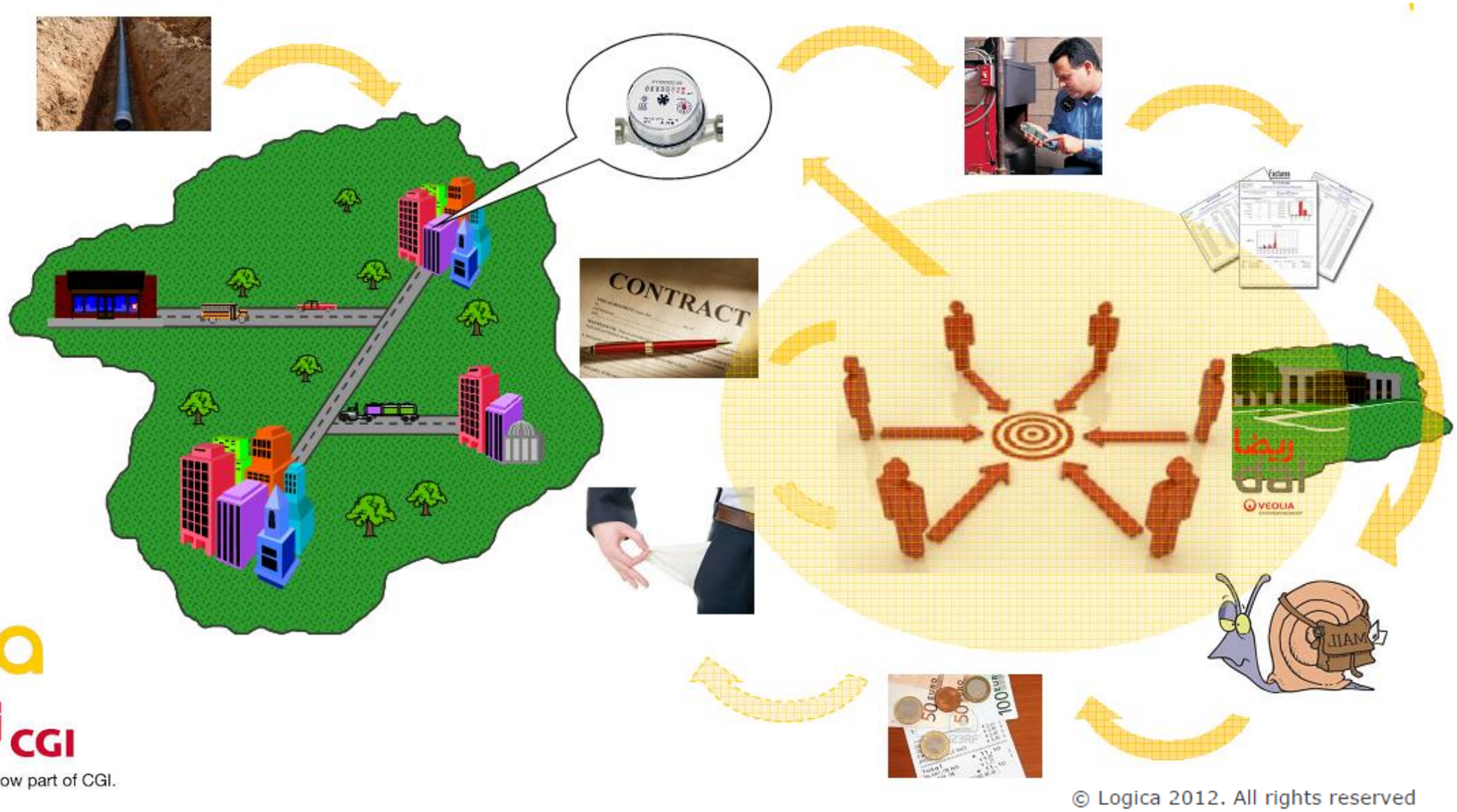
بيئة الرقابة وتكنولوجيا المعلومات تتضمن تطبيقين معلوماتيين وظيفيين Progiciel:

- نظام معلوماتي للتدبير التجاري حول تطبيق ELAG لشركة Logica
- نظام معلوماتي مندمج للتدبير المحاسبي حول تطبيق Microsoft NAVISION/Dynamics NAV



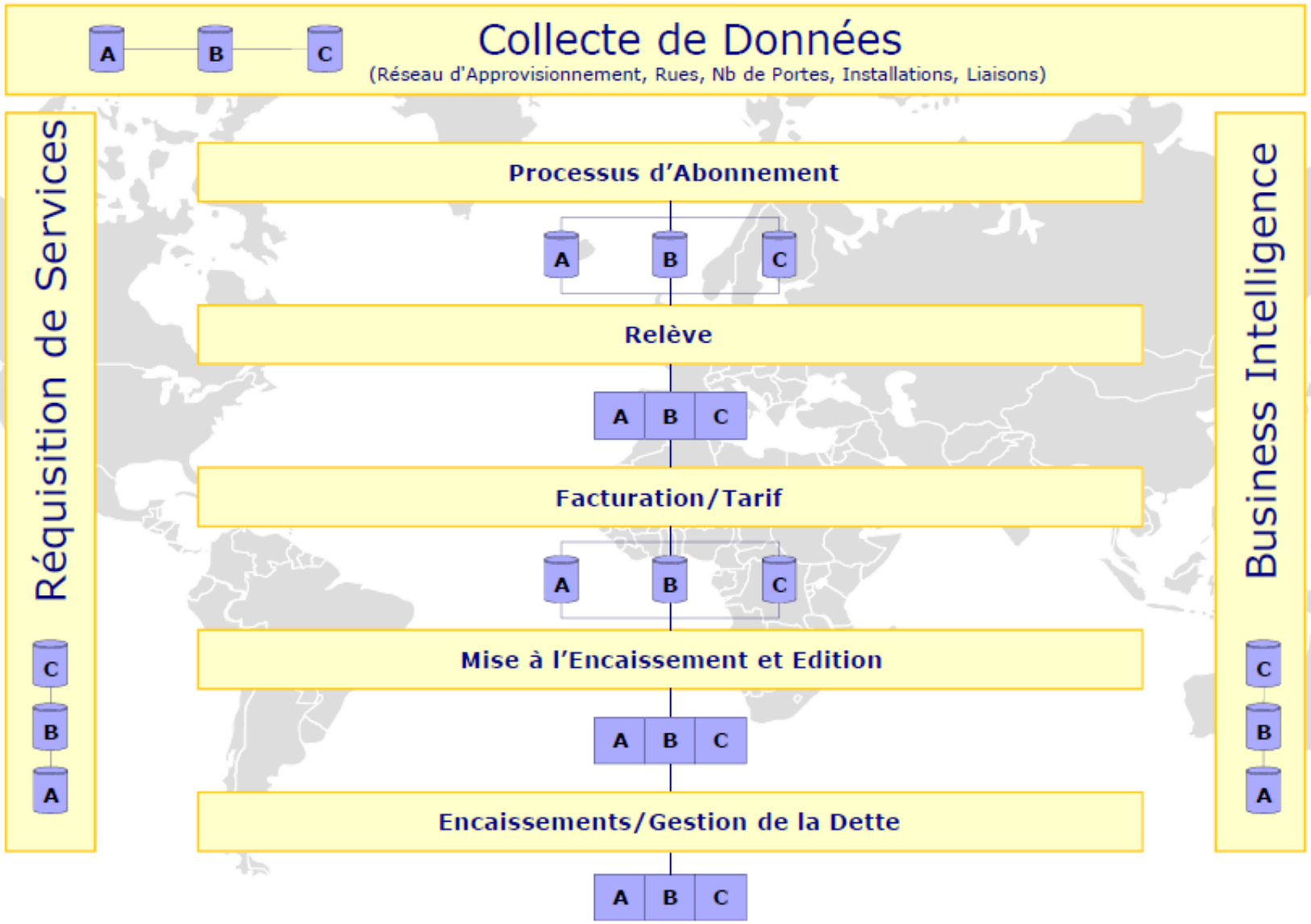
حالة عملية: برنامج التدبير التجاري وسلسلة العمليات الوظيفية لتطبيق ELAG

التدبير التجاري والتطبيق الوظيفي ELAG لشركة Logica



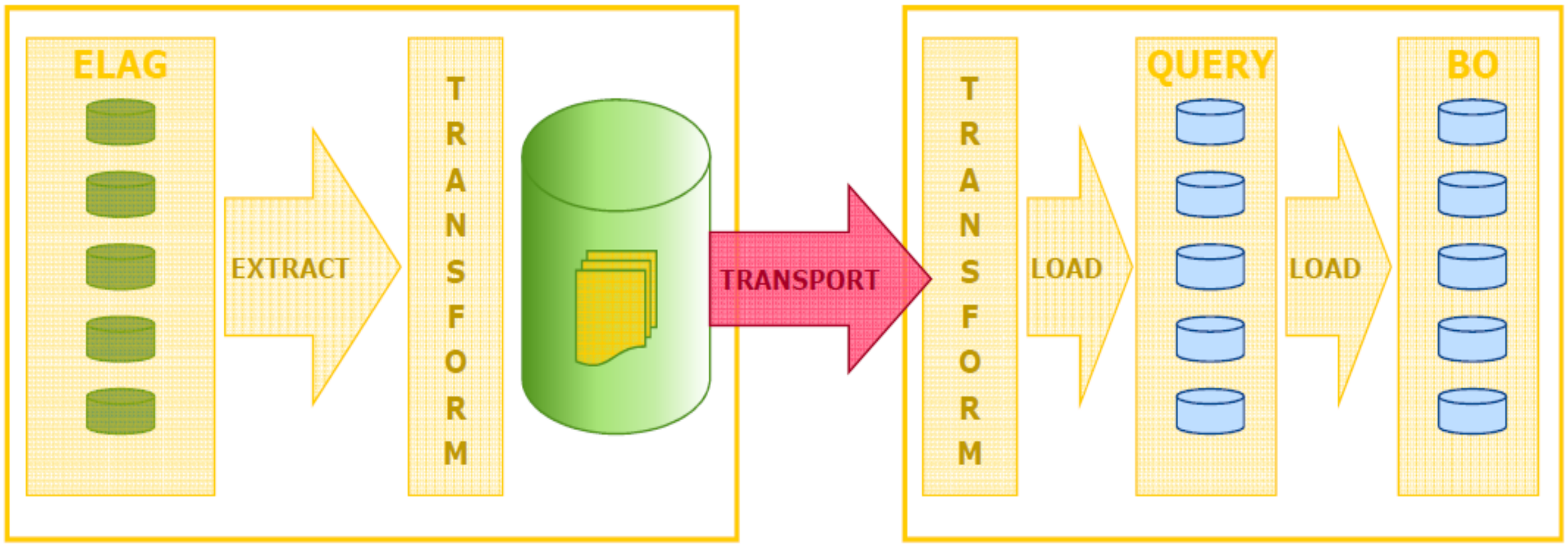
Logica is now part of CGI.

حالة عملية: برنامج التدبير التجاري وسلسلة العمليات الوظيفية لتطبيق ELAG



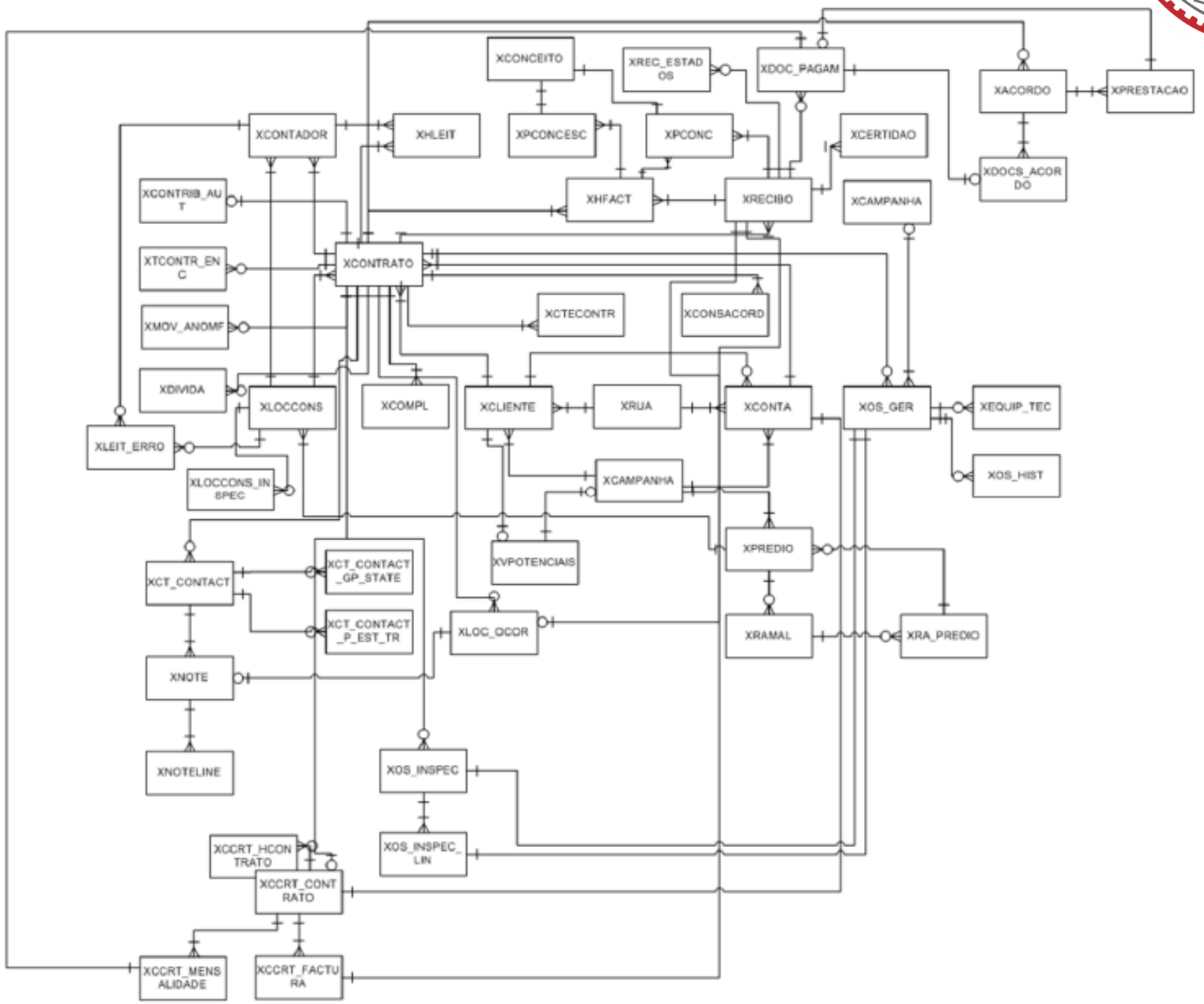
Logica is now part of CGI.

حالة عملية: برنامج التدبير التجاري ELAG تنظيم المهام التشغيلية واتخاذ القرار



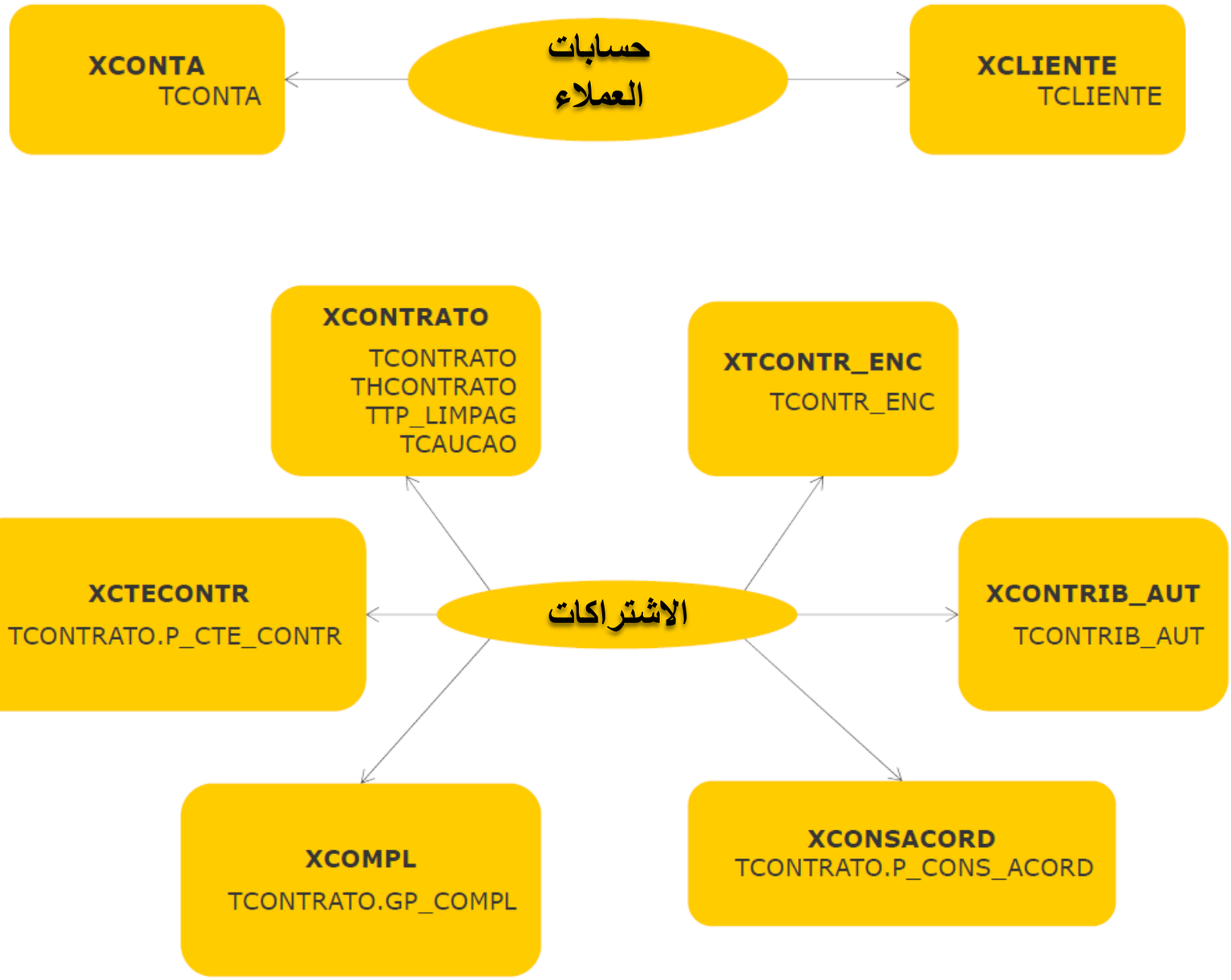
Logica is now part of CGI.

حالة عملية: نموذج بيانات اتخاذ القرار (decision-making data model)



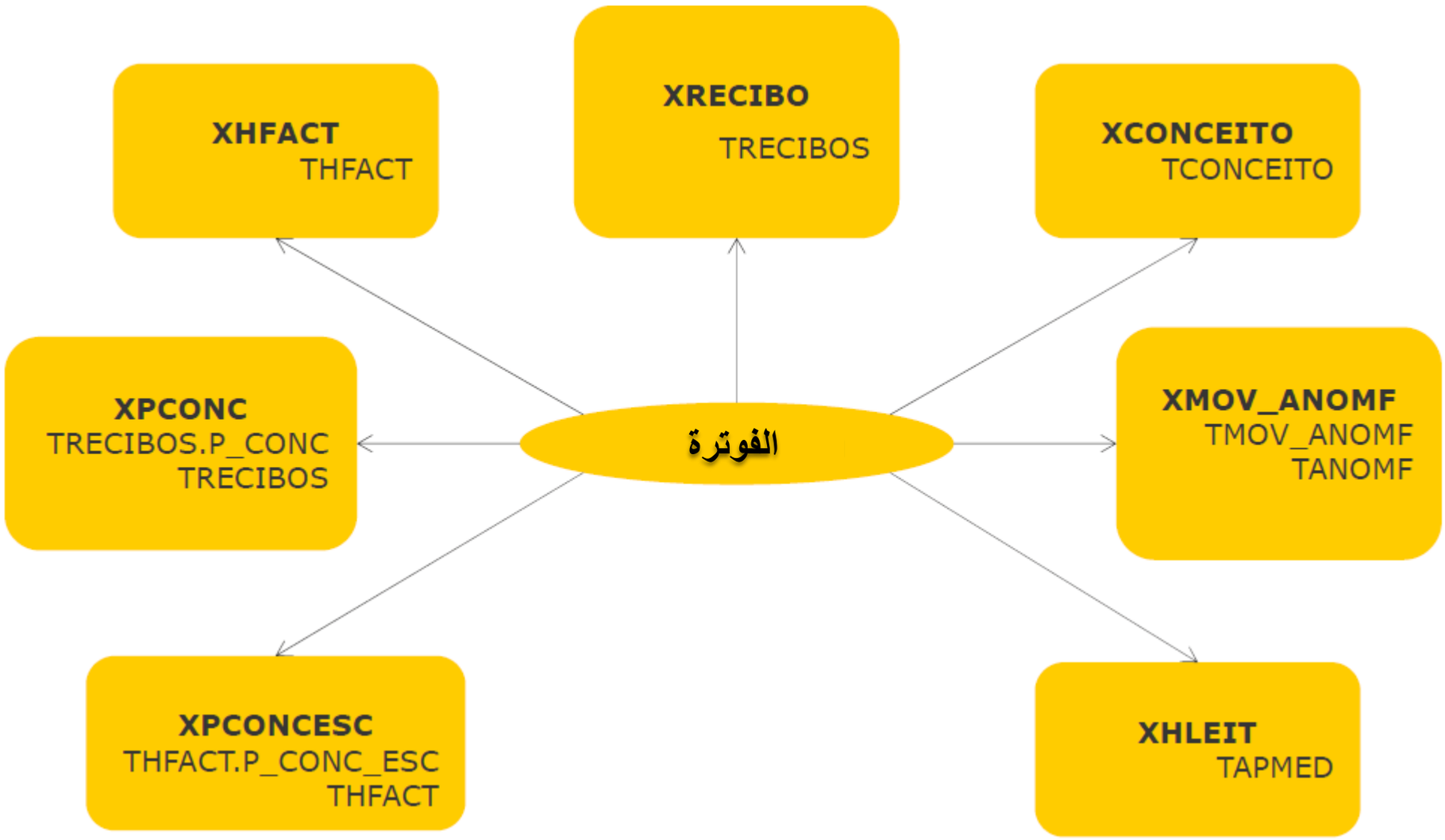
Logica is now part of CGI.

حالة عملية: قاعدة البيانات لتطبيق ELAG



Logica is now part of CGI.

حالة عملية: قاعدة البيانات لتطبيق ELAG



Logica is now part of CGI.

حالة عملية: أهم الملاحظات المسجلة –قطاع الماء والتطهير السائل-

- عدم شمولية رقم المعاملات السنوي الخاص بمبيعات السوائل ينعكس على صدقية الناتج الصافي المحاسبي
- اختلاف هيكل المبيعات المعتمد من طرف ريضال في تقييم الفواتير قبل الاعداد مع ذلك المستخرج من قاعدة المعطيات التجارية
- تناقض بين كميات استهلاك منتوج الماء والكميات المعتمدة في حساب إتاوات التطهير السائل
- فوترة استهلاك الإدارات العمومية عبر تقدير الكميات خلال فترات طويلة
- فوترة مصاريف إضافية من قبل ريضال في غياب موافقة السلطة المفوضة
- فرض مصاريف وضع وإزالة العداد في غياب الخدمة المنجزة

حالة عملية: أهم الملاحظات المسجلة –قطاع الكهرباء-

- استرجاع قيمة كميات تفوق تلك التي تم استهلاكها بصورة غير مشروعة
- فرض غير مستحق لعائدات مستخلصة لفائدة الغير
- خفض مبالغ الضريبة على القيمة المضافة المستحقة للدولة نتيجة اعتماد تقديرات غير صحيحة
- فرض مبلغ جزافي عن عقود الاشتراك للحصول على عدادات الكهرباء على هامش المقتضيات التعاقدية وفي غياب مصادقة السلطة المفوضة
- تحويل ديون الوكالة المستقلة لتوزيع الماء والكهرباء لفائدة ريضال وإلغاء جزء منها لفائدة بعض الأغيار

حالة عملية: أهم التوصيات

- إعادة النظر في مراجعة التعريفات بناء على متوسط ثمن البيع الحقيقي مع الحرص على عدم تداخل الدورات المحاسبية
- التقيد في عملية فوترة المصاريف بالمقتضيات التعاقدية، وربط تطبيقها بالإنجاز الفعلي للخدمة خصوصا فيما يتعلق بوضع وإزالة العداد ورسائل الإشعار وقطع وإعادة الربط
- تسوية الفوترة المنجزة خارج الضوابط التعاقدية
- التوقف عن فرض المبلغ الجزافي المتعلق باستخلاص الكميات المستهلكة عبر الربط غير المشروع مع الأخذ بعين الاعتبار لمجموع الفواتير المستخلصة في إطار الاتفاقيات مع الجماعات المحلية ووزارة الداخلية وبرنامج الإيصال الاجتماعي
- إرجاع المبالغ التي تعود للوكالة المستقلة لتوزيع الماء وتسوية حسابات الأغيار

6. خلاصة

- بإعطاء الأولوية لعمليات تدقيق تكنولوجيا المعلومات، أصبح لدى المجلس الأعلى للحسابات بالمملكة المغربية الأدوات والموارد اللازمة للإشراف الفعال على أنظمة تكنولوجيا المعلومات والمساهمة في قطاع عام أكثر شفافية وفعالية
- ومن خلال العمل سويا بين مكونات المجلس الأعلى للحسابات و مديرية أنظمة المعلومات لديه، صار بإمكانه الاستفادة من عمليات تدقيق تكنولوجيا المعلومات لتحديد مخاطر تكنولوجيا المعلومات ومعالجتها
- ومع استمرار تطور التكنولوجيا، يتطور أيضًا نهجنا في الرقابة داخل المجلس الأعلى للحسابات. حيث تعد عمليات تدقيق تكنولوجيا المعلومات أداة أساسية بالنسبة لنا للتغلب على تعقيدات العصر الرقمي وضمان الاستخدام المسؤول لموارد تكنولوجيا المعلومات.

شكرا لكم

المجلس الأعلى للحسابات بالمملكة المغربية

تجربة المجلس في الرقابة على الأنظمة المعلوماتية

2024

الدكتور محمد عساوي
قاضي مستشار مشرف
رئيس فرع

السيد جواد البيش
رئيس قسم
مديرية الأنظمة المعلوماتية

الجهاز المركزي للرقابة المالية
سورية

الطرق الحديثة للرقابة على الأنظمة المعلومات

إعداد
حسن فارس – محمد ناعسة

الأسلوب والمنهجية المتبعة في الرقابة والتدقيق

- تم تصميم ستة مصفوفات :مصفوفة لكل من (الضوابط العامة- أمن المعلومات- المدخلات- المعالجة – المخرجات – أمن التطبيق) ترتكز هذه المصفوفات بشكل اساسي على المصفوفات الواردة في دليل تدقيق تكنولوجيا المعلومات لأجهزة الرقابة كما تمت الاستعانة والمقارنة بأدلة الرقابة الموجودة لدى الأجهزة العليا للرقابة لبعض الدول العربية بحيث نحصل على اطار متكامل قدر الإمكان حيث تم تلخيص وترجمة الاسئلة الواردة فيها مع بعض الاضافات على شكل مخاطر وإدارة للمخاطر بغية تحقيق رقابة أداء على تقنية وأمن المعلومات والوصول لاستنتاج وإجابة مرتبط برقابة الاداء على تقنية المعلومات وأن الاجراءات المتبعة تحقق أفضل استراتيجية لإدارة المخاطر المتعلقة بامن وتقنية المعلومات ولا يوجد مجال للتحسين. على سبيل المثال:

الأسلوب والمنهجية المتبعة في الرقابة والتدقيق

التدقيق موضوع	الإجراء	احتمالية الخطر(1)	الخطر تأثير (2)	الخطر درجة (3)=(1)* (2)	الخطر إدارة(4) فعال غير(0-1) متوسط الفاعلية(1-2) فعال(4)	Performance (4-3)
المادي الدخول	العمل موافق إلى فقط لهم المصرح الموظفين دخول الجهة تضمن	2	2	4	3	1-
الدفاع	بها العمل يتم وأنه الاقتحاممحاولات لكشف الجهة في سياسة وجود من التأكد.	2	1	2	0	2-
الدخول سياسة	بالدخول للتحكم وفعالة واضحة سياسة الجهة لدى	1	1	1	1	0

- حيث :
- درجة الخطر = حاصل ضرب (احتمالية الخطر * تأثير الخطر)
- تتحدد احتمالية الخطر باحد القيم (0,1,2,) بحسب درجة احتمال الحدوث
- تتحد قيمة تأثير الخطر بأحد القيم (0,1,2,) بحسب تاثير الخطر على المؤسسة.
- وبالتالي تتحدد درجة الخطر باحد القيم (0-4)
- بعد تحديد درجة الخطر يتم تحديد قيمة لادارة هذه الخطر تتراوح بين (0-4)
- اما مقياس درجة الأداء فيقاس بحاصل طرح (درجة الخطر – إدارة الخطر).

الأسلوب والمنهجية المتبعة في الرقابة والتدقيق

- إن مقياس درجة الأداء هو مقياس يتيح ملائمة الإجراءات والضوابط المتخذة من قبل الشركة لإدارة مخاطر تقنية وامن المعلومات ويقاس بالتفاضل بين درجة الخطر للضابط و ودرجة ملائمة الإجراء المتخذ لتفادي الخطر ويكون بحالته المثلى يساوي الصفر .

- ثم يؤخذ المتوسط الحسابي لكل اجراءات المصفوفة الواحدة وبحسب نتيجة المتوسط الحسابي للاداء يتراوح بين (0) و (-4) نستطيع أن نجيب على فرضية الدراسة ان مستوى أداء نظم وأمن المعلومات في المؤسسة العامة جيد ولا يوجد مجال للتحسين وأن نقيم مكان هذا الاداء على هذا السلم بحسب المتوسط الحسابي لكامل المصفوفات

الأسلوب والمنهجية المتبعة في الرقابة والتدقيق

- مع وجود توصيات لكل مايلي:

- اجراءات التدقيق الواجبة والتي كانت نتيجة تقيم اداءها اقل من (-2,-3,-4) بحيث يوصى بإدارة مخاطر افضل لها

- اجراءات التدقيق الواجبة والتي كانت نتيجة تقييم أداءها أكبر من الصفر بحيث يتم التوصية بتخصيص مواردها للاجراءت ذات المخاطر المرتفعة وبذلك نحصل على افضل المجالات للتحسين.

-

الأسلوب والمنهجية المتبعة في الرقابة والتدقيق

- أما إدارة الخطر فقد تم استبدال الإجابة على أسئلة المصفوفات بنعم او لا بمقياس ليكرت الرباعي حيث استخدم الأوزان النوعية التالية.

  - الرقم (0-1) إذا كانت نتيجة إدارة الخطر غير فعالة.
  - الرقم (2-3) إذا كانت نتيجة إدارة الخطر متوسطة الفاعلية.
  - الرقم (4) إذا كانت نتيجة إدارة الخطر فعالة..

- وتم استخدام وسائل التحليل المقترحة في الدليل لتحديد مستوى قياس الأداء لكل اجراء مدروس

- **هـ** ـ تم تلخيص النتائج والإجابات بجدول يبين اسم المصفوفة وأهداف التدقيق الرئيسية والمتوسط الحسابي لمستوى الأداء لكل مصفوفة

- **و**ـ تم تلخيص النتائج (تقرير التدقيق على نظم المعلومات وأمن المعلومات) يبين مستوى فاعلية ضوابط تقنية معلومات وتسليط الضوء على أهم نقاط الضعف في الضوابط العامة وضوابط التطبيق وضوابط امن المعلومات. ووضع جدول يوصف أهم نقاط الضعف ومستوى الخطر الخاص به والتوصيات لمعالجته.

مصفوفات التدقيق

1. مصفوفة الضوابط العامة
2. مصفوفة أمن المعلومات
3. مصفوفة مدخلات التطبيق
4. مصفوفة معالجة التطبيق
5. مصفوفة مخرجات التطبيق
6. مصفوفة امن التطبيق.

نتائج عملية الرقابة على نظم المعلومات (تقرير تدقيق نموذجي)

- **إلى : الشركة السورية للاتصالات**

- **الرأي:**

- برأينا تفتقر ضوابط نظم المعلومات إلى الفاعلية المطلوبة في تحقيق أهداف ضوابط تقنية نظم المعلومات وأمن المعلومات إذ أظهرت نتائج تقييم الضوابط العامة وضوابط التطبيق وامن المعلومات درجة أداء دون المتوسط وتراوحت متوسط درجة الأداء بين 1.29- (لضوابط الأمن السيبراني) و 0.88- لضوابط التطبيقات, إذ أن الضوابط تكون فعالة عندما تكون درجة الأداء صفر او أكبر من الصفر.
- إن مقياس درجة الأداء هو مقياس يتيح ملائمة الإجراءات والضوابط المتخذة من قبل الشركة لإدارة مخاطر تقنية وامن المعلومات ويقاس بالتفاضل بين درجة الخطر للضابط و ودرجة ملائمة الإجراء المتخذ لتفادي الخطر ويكون بحالته المثلى يساوي الصفر .

نتائج عملية الرقابة على نظم المعلومات (تقرير تدقيق نموذجي)

- **أساس الرأي.**

- لقد استندنا في رأينا إلى منهجية مركبة تستند على الاصدارات المهنية المتمثلة بدليل تدقيق تكنولوجيا المعلومات لأجهزة الرقابة العليا و وتستند على تقييم المخاطر المرتبطة بنظم المعلومات والأمن السيبراني وتستند على معايير رقابة الأداء بحيث قمنا بتخطيط وتنفيذ هذه المهمة استنادا إلى هذه المعايير وتم قياس درجة الأداء وتوصلنا إلى هذه الدرجة وفق ما هو مبين أعلاه.
- لقد قمنا بإبداء رأينا في ضوء الاستنتاجات والنتائج التي توصلنا لها وهو استنتاج معقول وليس مطلق لكافة المخاطر التي من الممكن أن تتعرض لها الشركة في هذا المجال.

- ولقد التزمنا بقواعد السلوك المهني للشركة وللجهاز الأعلى للرقابة اثناء تنفيذنا للمهمة

نتائج عملية الرقابة على نظم المعلومات (تقرير تدقيق نموذجي)

- **وتركزت معظم نقاط الضعف في كل مما يلي:**
- **بالنسبة للضوابط العامة:**

- ✓ لا يتواجد سياسات لاستخدامات الانترنيت والبريد الداخلي الكترونيا
- ✓ لا يتم تقييم الجهة للثغرات الأمنية واختبار الاختراق بصفة دورية حسب سياسة موثقة ومعتمدة
- ✓ لا يتواجد خطة لاستمرارية العمل معتمدة وموثقة لدى الجهة
- ✓ ل**بالنسبة لضوابط امن المعلومات:**

- ✓ لا يوجد آلية فعالة وموثقة بشكل جيد لتقييم المخاطر المرتبطة بأمن معلومات والامن السيبراني
- ✓ لا يتم الحد من أثر المخاطر الهامة بصورة كافية وفعالة؟
- ✓ الموظفين ليسو على وعي وادراك بأدوارهم ومسئولياتهم فيما يتعلق بمهامهم ومسئولياتهم الأمنية؟
- ✓ لم تضمن الشركة دخول الموظفين المصرح لهم فقط إلى مرافق العمل

- **بالنسبة لضوابط التطبيقات:**

- ✓ لا يتم مراجعة سجل التدقيق دورياً لمراقبة أي نشاط غير عادي
- ✓ عدم تأمين معلومات التطبيق بشكل ملائم ضد سوء الاستغلال .

نتائج عملية الرقابة على نظم المعلومات (تقرير تدقيق نموذجي)

الوصف	المخاطر ذات الصلة	التوصيات
لا يتواجد سياسات لاستخدامات الانترنيت والبريد الداخلي الكترونيا. ولايتم مراقبة الدخول الفعلي المصرح للموظفين بصورة دورية	إمكانية اجراء معاملات مالية غير قانونية وشبه فساد من خلال الدخول غير المصرح به. وهذا ما حصل بالفعلو وهذا ما سجل 11 حالة فيروسات بالاجهزة تم تلافي معظمها بمضاد الفيروسات وبعضها الحق ضررا بباقي الاجهزة وبتاخير انجاز المعاملات.	وضع سياسات لاستخدامات الانترنيت والبريد الداخلي الكترونيا. مراجعة صلاحيات الموظفين باستمرار بما يتماشى مع القرارات الداخلية
لا تقوم الشركة باختبار وتنفيذ خطة استمرارية العمل حسب سياسة موثقة ومعتمدة	تسرب العديد من زبائن الشركة نتيجة توقف الشبكة المستمر او الانترنيت او انقطاع الكهرباء المستمر وفق ما أظهرت إدارة التسويق	وضع الخطة المطلوبة لاستمرارية العمل في الظروف الطارئة بما يضمن عدم توقف العمل
عدم تأمين معلومات التطبيق بشكل ملائم ضد سوء الاستغلال و لا يوجد مراجعة للسجلات الالكترونية بصفة منتظمة	سوء استغلال المخرجات والمعلومات بشكل غير مناسب ينطوي على شبه بالفساد , وهذا ما حصل بالفعل عند اتاحة السماح بطباعة بعض بيانات العملاء قبل إتمام تخزينها مما رتب اجراء بعض العمليات دون ارشفتها وادخالها النظام ودون معرفة الشخص القائم بها	التغذية العكسية لجميع المخالفات والآثار المحتلمة على قواعد التحقق من الصحة وضوابط تسجيل دخول الموظفين والاحتفاظ بالسجل اللكتروني للعمليات لفترة مناسبة وتوثيق ذلك ضمن ساسة معتمدة

التوصيات

- لابد للأجهزة العليا للرقابة من البدء وبأسرع وقت في مجال رقابة نظم المعلومات وأمن المعلومات لما لذلك دور من تعزيز دورها في حماية وتدقيق المال العام وتحقيق الأهداف والغاية من وجودها.

- يجب على الأجهزة العليا للرقابة تطوير قدرات الموظفين وتدريبهم وزيادة كفاءتهم وحثهم على على الحصول على الشهادات المهنية المتعلقة بالرقابة على نظم المعلومات وأمن المعلومات ولا سيما في في اهداف التدقيق المشار إليها في نتائج الدراسة.

- زيادة المستوى العام للاجور والموارد الاقتصادية للعاملين في نظم المعلومات والأمن السيبراني بما يزيد من الاهتمام بتفادي المخاطر المرتبطة بمجال نظم وأمن المعلومات ويستقطب المهارات والكفاءات بهذا الخصوص. إذ غالبا ما يتطلب استدراك هذه المخاطر كفاءات ومهارات خاصة غير متوفرة بامكانيات الموظف العام وخارج اهتماته.

- السعي لتأطير الضوابط العامة لنظم وامن العلومات ضمن قواعد وانظمة ملزمة يتم التقرير عنها ضمن رقابة الالتزام أو الامتثال

- افراد فقرات خاصة بتقارير التدقيق سواء (تقارير الرقابة المالية او رقابة الالتزام او رقابة الاداء يتم التطرق بموجبها إلى نقاط الضعف في الضوابط ذات العلاقة.

التوصيات

- الحاجة إلى إنشاء مركز تعلم مخصص لفريق تدقيق تكنولوجيا المعلومات الإقليمي.

- تشجيع الأجهزة العليا للرقابة في زيادة البحث العلمي وتكثيف الدورات التدريبية للرقابة على نظم المعلومات والأمن السيبراني .

- العمل على وضع إطار عمل أو دليل رقابة خاص بالرقابة على نظم المعلومات وامن المعلومات يشتمل على منهجية وادلة تدقيق للتعامل مع نظم المعلومات, مع مراعاة أنواع التدقيق وان تكون هذه المنهجية مبنية على تقييم المخاطر.

- دعوة الأجهزة العليا لتنفيذ مهمات تعاونية إقليمية بالتعاون مع المنظمات ذات الخبرة , وتقاسم قصص النجاح والدروس المستفادة من الرقابة على نظم المعلومات , والاستفادة من كفاءات ومهارات فريق تقنية المعلومات في الأجهزة العليا للرقابة المالية والمحاسبة التي تركز على علوم البيانات والإحصاءات ومهارات تكنولوجيا المعلومات وذكاء الأعمال.

- الاستفادة من نقاط الضعف المحددة في الضوابط الرقابية لنظم وامن المعلومات بحيث تتحول إلى ضوابطة وقائية بدلا من ضوابط استنتاجية تساعد على التغذية العكسية لرقابة الالتزام والرقابة المالية ورقابة الأداء

التوصيات

- تخصيص إدارة مستقلة في كل جهاز أعلى تتعلق بالرقابة والتدقيق على نظم المعلومات والأمن السيبراني يكون من مهامها:

  - الرقابة على نظم المعلومات وأمن المعلومات لبعض الجهات الخاضعة للتدقيق ضمن خطة سنوية

  - مختصة بالتدقيق على تكنولوجيا المعلومات والأمن السيبراني

  - متابعة المستجدات في تدقيق نظم المعلومات والأمن السيبراني وخاصة من خلال متابعة الأدوات المستخدمة في الرقابة.

  - تكون بمثابة مختبر يزود باقي إدارات التدقيق بأماكن الضعف والمخاطر العالية واجبة التدقيق وتساعد في وضع الخطة الاستراتيجية للجهاز الأعلى للرقابة من خلال مهاراتها في تدقيق نظم وأمن المعلومات

- العمل على تعديل نطاق التدقيق ليشمل الوصول إلى بيئة تكنولوجيا المعلومات للجهات الخاضعة للتدقيق بما في نظم المعلومات في رقابة الالتزام

- ضرورة متابعة الأجهزة العليا للرقابة للإصدارات المهنية الدولية المتعلقة بالرقابة في ظل بيئة تقنية المعلومات أو البيانات الضخمة أو الحكومة الإلكترونية أو الأمن السيبراني أو ذكاء الاعمال ....

التوصيات

1. الترويج لأهمية الدور الرقابي للأجهزة العليا للرقابة من أجل التغلب على الصورة النمطية للرقابة والتدقيق الموجودة لدى بعض الجهات الحكومية من خلال وضع التشريعات والقوانين لتمكين الجهاز الأعلى من أداء العمل المطلوب منه.

2. توفير التقنيات المناسبة لمساعدة الجهاز الأعلى على نظم وأمن المعلومات لأي جهة عامة حكومية

3. تطوير وحدة خاصة في الجهات الحكومية للتعامل مع خطة نظم المعلومات لضمان جودة نظم المعلومات والأمن السيبراني

4. تفعيل التعاون والتنسيق والتكامل مع الجهات الحكومية المعنية بالأمن السيبراني والجهات الناظمة للخطة الاستراتيجية للامن السيبراني والجهات المقررة لضوابط نظم وامن المعلومات في القطاع العام بحيث يتحقق التكامل بالاعمال دون ازدواجية او تعارض.

5. السعي لتطبيق حوكمة تكنولوجيا المعلومات بفعالية ـ سواء في منظمات الأعمال أو المنظمات والجهات الحكومية أو الأجهزة العليا للرقابة ـ للاستفادة من مزاياها في زيادة كفاءة أنظمة المعلومات الإلكترونية والحد من المخاطر التي تتعرض لها.

•

التوصيات

1. ضرورة تطوير أنظمة الرقابة والمراجعة الداخلية فى ظل حوكمة تكنولوجيا المعلومات لكي تتلاءم مع أهداف وسياسات المنظمات، وحماية البيانات والمعلومات، ومن ثم الحد من مخاطر نظم المعلومات الإلكترونية.

2. التأهيل المناسب للمدققين، والأعضاء الفنيين في الأجهزة العليا للرقابة المالية والمحاسبة من الناحية العلمية والعملية فى مجال تكنولوجيا المعلومات لتجنب القصور فى التكنولوجيا الموجودة والتى تتيح الغش والتلاعب والاحتيال فى النواحى المالية، وكذلك لتحسين كفاءة وفعالية المدققين.

3. التوصية بتضمين مخرجات الرقابة المالية ورقابة الالتزام وتقارير التدقيق بمختلف أوضاعها تقييم للضوابط الرقابية لنظم المعلومات وامن المعلومات بالعموم وتوصيات بهذا الخصوص.

شكرا لحسن استماعكم

تقرير ديوان الرقابة المالية والادارية

حــول

التدقيق على البريد الإلكتروني الحكومي

(2021)

تقرير ديوان الرقابة المالية والادارية

حــول

التدقيق على البريد الإلكتروني الحكومي

(2021)

أعد\د
محمد نخلة

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

دوافع التدقيق

قام ديوان الرقابة المالية والإدارية بإجراء رقابة حول "منظومة البريد الإلكتروني الحكومي وسياسة استخدامه في الجهات الخاضعة" نتيجة لبعض الأسباب والدوافع :-

- أهمية وجود قناة اتصال آمنة وموحدة بين الموظفين وبين المؤسسات، وعدم الاعتماد على البريد الشخصي والذي قد يؤدي لضياع الوثائق والبيانات
- التأكد من الامتثال للتشريعات والسياسات الالخاصة والمتصله بالبريد الالكتروني

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

نطاق التدقيق

الأمان

- التشفير:- التأكد من استخدام التشفير اثناء النقل الرسائل (TLS)
- التحقق من استخدام تقنيات منع التزوير والاحتيال (DMARC,SPF,DKIM)
- التأكد من وجود أنظمه حمايه خاصة بالبريد الالكتروني
- فحص سياسات التحكم والمصادقة الثنائية
- التحقق من وجود إجراءات لانشاء وحذف الحسابات
- اداره كلمات المرور

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

نطاق التدقيق

الإدارة والسياسات(الامتثال)

- التأكد من الالتزام بالقرارات الصادره عن مجلس الوزراء المتعلقة باستخدام البريد الالكتروني الحكومي
- مراجعة وتقييم السياسات والإجراءات المتعلقة البريد الالكتروني الحكومي

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

نطاق التدقيق

التوافر والاداء

- التحقق من وجود وتنفيذ النسخ الاحتياطي
- التحقق من قابليه وصحه استعادة البيانات في حالات الطوارئ

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

هدف التدقيق

- تقييم مدى الالتزام بالسياسات والإجراءات
- تقييم كفائه وفاعلية إدارة البريد
- تقييم الضوابط الداخلية المتبعة لتقيد الوصول وحماية النظم
- تحسين الأداء والفاعلية

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

اسئله التدقيق

اسئله حول امان البريد الالكتروني

- هل يتم تشفير رسائل البريد الالكتروني اثناء الارسال؟
- هل يتم استخدام تقنيات منع التزوير والاحتيال (DMARC,SPF,DKIM)؟
- هل هنالك وجود انظمه خاصة لفحص المرفقات وحماية البريد من البرمجيات الخبيثة
- هل يتم استخدام المصادقة الثنائية؟
- هل يتم فرض سياسات قويه لكلمات المرور؟
- هل هنالك إجراءات لتغيير كلمات المرور بانتظام ؟

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

اسئله التدقيق

السياسات والاجراءات

- **هل يوجد سياسه خاصة في كيفية استخدام بالبريد الاكتروني ؟**
- **هل يوجد سياسات ذات صله بالبريد الالكتروني** (سياسه اداره الحساب وسايسة النسخ الاحتياطي ....) ؟

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

اسئله التدقيق

اسئله التوافر وألاداء

- هل يتم اخذ نسخه الاحتياطي وفق نظام متبع وموثق؟
- هل يتم اجراء عمليه استرجاع للنسخ الاحتياطي والتاكد من سلامتها؟
- هل هنالك موقع بديل لنقل مسؤوليه إدارة البريد في حال حدوث كوارث؟
- هل يوجد إجراءات موثقة لادارة المخاطر الناتجه عن التغيرات والتطورات الحاصة على البريد الالكتروني؟
- هل هنالك مساحة تخزينية محددة للمستخدمين ؟
- كيف يتم التعامل مع البريد الممتليء؟

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

النتائج

نتائج امان البريد

- تشفير البيانات:- تم تشفير جميع الرسائل البريد الالكتروني اثناء الارسال والتخزين
- تم استخدام تقنيات منع التزوير والاحتيال (DMARC,SPF,DKIM)
- وجود قصور في أنظمة فحص المرفقات وحماية البريد من البرامج الخبيثة
- عدم استخدام المصادقه الثنائيه
- اداره كلمات المرور: وجود قصور في اداره كلمات المرور

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

النتائج

نتائج السياسات والإجراءات

- وجود قصور في السياسه المعتمده لاستخدام البريد الالكتروني
- قصور – في سياسه الينسخ الاحياطي واستعاده البيانات

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

النتائج

نتائج الأداء

- عدم جود إجراءات موثقة لادارة المخاطر الناتجه عن التغيرات والتطورات الحاصة على البريد الالكتروني
- عدم وجود موقع بديل يضمن نقل مركز المسؤوليه اليه في حال حدوث كوارث
- عدم توثيق الاحداث ذات العلاقه بامن المعلومات كالاعطال والهجمات

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

المعايير

المعيار	المصدر أو التشريع
❑ اعتماد البريد الحكومي حصريا لنقل بريد المؤسسات والدوائر الحكومية داخل فلسطين	❑ قرار مجلس الوزراء (03/66/17) لعام 2015 م
❑ سياسة استخدام الانترنت والبريد الإلكتروني الحكومي في الدوائر الحكومية	❑ قرار مجلس الوزراء (07/17/18)
❑ وثيقة ونظام أمن المعلومات المعدة من قبل الفريق الوطني الأنظمة والمعلومات والمصادق عليها بقرار من مجلس الوزراء في عام 2012	❑ قرار مجلس الوزراء (08/127/13) لعام 2012 م

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

المعايير

المعيار	المصدر أو التشريع
❑ المنهجية المعتمدة في ديوان الرقابة المالية والإدارية للرقابة على تكنولوجيا المعلومات ❑ معايير التدقيق وقياس بيئة الضوابط الرقابية: ❑ أولا: حوكمة تكنولوجيا المعلومات (1A.) ❑ ثانيا: إدارة ومتطلبات التطوير (2A.) ❑ ثالثا: إدارة عمليات تكنولوجيا المعلومات (3A.) ❑ رابعا: الاستعانة بمصادر خارجية (4A.) ❑ خامسا: خطة استمرارية العمل (BCP) وخطة التعافي من الكوارث (PRD) (5.A) ❑ سادسا: أمن المعلومات (6A.) ❑ سابعا: ضوابط التطبيق (7A.)	❑ توصيات وتعليمات الممارسات الفضلى لمهنة تدقيق أنظمة المعلومات الصادرة عن جمعية التدقيق والرقابة على أنظمة المعلومات (ISACA) الواردة ضمن إطار عمل وتعليمات أهداف ضوابط المعلومات والتكنولوجيا المصاحبة (COBIT) وإطار عمل ضمان ومراجعة تكنولوجيا المعلومات (ITAF) وكافة المعايير والتوجيهات الواردة فيها ذات العلاقة بالتكنولوجيا ومعايير وتوجيهات تدقيق أنظمة المعلومات والتي تشمل المعايير الدولية للمؤسسات العليا للتدقيق ISSAI 1210 والمعايير الدولية للتدقيق ISA 210) ومعايير الإنتوساي: مجموعة عمل الإنتوساي للرقابة على تقنية المعلومات (WGITE) ومبادرة تنمية الإنتوساي (IDI)

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

التوصيات

- ضرورة وضع سياسات وخطط لإدارة ومعالجة وتقييم المخاطر. .
- ضرورة وضع إجراءات للاستجابة للأحداث الأمنية ورفع تقارير دورية تشمل الأدلة وتقييم هذه الأحداث والتعلم من الأحداث الأمنية السابقة.
- ضرورة وجود جهة إدارية تشرف على التغييرات وتقوم بفحصها واختبارها واعتمادها قبل إدخالها في بيئة العمل الفعلية.
- ضرورة توفير موقع بديل يضمن تشغيل الخدمات منه كخدمة البريد الإلكتروني في حالة حدوث أي كارثة في الموقع الرئيسي والاستثمار بتقنيات تضمن ال HIGH AVAILABILITY.

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

التوصيات

- ضرورة تحديث سياسة البريد الإلكتروني لتشمل الإجراءات المتعلقة بالأجهزة النقالة وتوزيع نموذج "التعهد الأمني بعدم الكشف" واتخاذ تدابير أمنية داعمة للحماية من المخاطر الناجمة عن استخدام الأجهزة النقالة.
- ضرورة تصنيف المعلومات باستخدام أدوات تقنية مخصصة لذلك وربط هذه الأدوات بالبريد الإلكتروني وبأنظمة المراقبة والتدقيق.
- ضرورة تعزيز الضوابط الأمنية للبريد الإلكتروني المرتبطة بالكشف، والوقاية وذلك للحماية من البرمجيات الخبيثة.

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

تقرير ديوان الرقابة المالية والادارية

حـول

التدقيق على البريد الإلكتروني الحكومي

(2021)

شكرا لحسن استماعكم

ديـــوان المحاسبـــة
State Audit Bureau
State of Qatar • دولـــة قطـــر

الطرق الحديثة للرقابة على تكنولوجيا المعلومات

الموضوعات الرئيسية

- مقدمة تعريفية عن مراجعة تكنولوجيا المعلومات
- معايير مراجعة تكنولوجيا المعلومات
- مخاطر تكنولوجيا المعلومات
- حوكمة تكنولوجيا المعلومات
- استمرارية الاعمال والتعافي من الكوارث
- تحليل البيانات

2

تعريف الرقابة على تكنولوجيا المعلومات

التدقيق على تكنولوجيا المعلومات هو ضمان تطوير وتطبيق وصيانة ألانظمة لأهداف العمل، وحماية أصول المعلومات والمحافظة على نزاهة البيانات، واختبار تنفيذ مشاريع تكنولوجيا المعلومات او الضوابط المطبقة على النظم لضمان تلبية احتياجات العمل في الجهة دون المساس بالأمن، والخصوصية، والتكلفة، وغيرها من محاور العمل الهامة.

أهمية الرقابة على تكنولوجيا المعلومات

تقييم مستوي المخاطر وادارتها

ضمان الكفاءة والفعالية التشغيلية

أمن المعلومات وحماية البيانات

الامتثال والمتطلبات القانونية

ثقة أصحاب المصلحة

استمرارية الأعمال والتعافي من الكوارث

الهدف:

الهدف الرئيسي للرقابة على تكنولوجيا المعلومات هو الحفاظ على المال العام من خلال مراجعة أنظمة وبرامج وتطبيقات تكنولوجيا المعلومات بالجهات الخاضعة لرقابة الديوان. وتقييم أدائها والتأكد من مدى كفاءتها وفعاليتها، من خلال التأكيد على أن موارد تكنولوجيا المعلومات تؤدي لتحقيق الأهداف التنظيمية بفعالية واستخدام الموارد بكفاءة، وقد يشمل تدقيق تكنولوجيا المعلومات أنظمة تخطيط موارد المؤسسات، و أمن نظم المعلومات، والحصول على حلول للأعمال، وتطوير الأنظمة، واستمرارية الأعمال والتي تعتبر كلها من مجالات تطبيق نظم المعلومات، أو يمكن أن تكون للنظر في القيمة المفترضة التي وفرتها النظم المعلوماتية.

فيما يلي بعض الأمثلة على أهداف التدقيق:

- مراجعة ضوابط نظم تكنولوجيا المعلومات للتأكيد على دقتها وفعاليتها.
- تقييم العمليات المرتبطة بعمليات مجال معين مثل نظام الرواتب، أو نظام المحاسبة المالية.
- تقييم أداء النظام ، على سبيل المثال، التدقيق على نظام الحجز في السكك الحديدية.
- فحص عملية تطوير النظام والإجراءات.

ديـــوان المحاسبـــة
State Audit Bureau
State of Qatar • دولـــة قطـــر

معايير مراجعة تكنولوجيا المعلومات

معايير مراجعة تكنولوجيا المعلومات

توجد العديد من الأطر والمعايير والمبادئ التوجيهية والأدوات لتوفير التوجيه للمدققين في استكمال تدقيق أنظمة المعلومات. يجب أن يكون المدققون على دراية بتلك المعايير عند التدقيق ويمكنهم استخدامها كأدوات مرجعية.

المعايير:

هي مجموعة من التدابير أو الإجراءات أو الممارسات التشغيلية أو الفنية. توفر المعايير معلومات أكثر تفصيلاً حول الكيفية التي يُتوقع بها من المديرين والمتخصصين الوظيفيين إجراء جوانب معينة من واجباتهم. يجب على المدققين الالتزام بهذه المعايير عند إجراء التدقيق.

معايير مراجعة تكنولوجيا المعلومات

معايير مراجعة تكنولوجيا المعلومات

- **GUID 5100**
- سلسلة الإرشادات حول الرقابة على نظم المعلومات

- **المعايير العامة** : المبادئ التوجيهية التي تعمل بموجبها مهنة ضمان تكنولوجيا المعلومات.
- **معايير الأداء** : تتعامل مع سلوك المهمة، مثل التخطيط والإشراف، وتحديد النطاق، والمخاطر والأهمية النسبية، وتعبئة الموارد، والإشراف وإدارة المهام، وأدلة التدقيق والتأكيد، وممارسة الحكم المهني والعناية الواجبة.
- **معايير إعداد التقارير** "تتناول أنواع التقارير ووسائل الاتصال والمعلومات المرسلة.

- آيزو 20000 :عمليات تكنولوجيا المعلومات.
- آيزو 27000: أمن تكنولوجيا المعلومات.
- آيزو 31000: المخاطر آيزو 38500: الحوكمة

مخاطر تكنولوجيا المعلومات

مخاطر تكنولوجيا المعلومات

- هي المخاطر التقنية التي تشير إلى أي تهديد لسلامة البيانات، أو توافر النظام، أو سرية المعلومات التي يمكن أن تؤثر على عمليات الجهة . هذه المخاطر تنشأ من مصادر متعددة مثل الهجمات الإلكترونية، وخروقات البيانات، وأعطال النظام، أو غيرها

كيفية تحديد المخاطر:

- تقييم المخاطر
- تحليل الحوادث السابقة
- مراقبة التهديدات الناشئة
- استشارة أفضل الممارسات والأطر في القطاع المتعلق بالجهة

المعادلة الحسابية للمخاطر

- **الخطر = الاحتمالية * الأثر**

امثلة على الضوابط المتعلقة بالمخاطر:

- **ضوابط وقائية**: تهدف إلى منع حدوث المخاطر (مثل جدران الحماية، ضوابط الوصول).
- **ضوابط كشفية:** مصممة لتحديد وكشف المخاطر مبكرًا (مثل أنظمة كشف التسلل).
- **ضوابط تصحيحية:** يتم تنفيذها للتخفيف من الضرر بعد تحقق المخاطر (مثل أنظمة النسخ الاحتياطي).

ديـــوان المحاسبـــة
State Audit Bureau
State of Qatar • دولـــة قطـــر

حوكمة تكنولوجيا المعلومات

حوكمة واستراتيجية تكنولوجيا المعلومات
IT Governance and Strategy

هي الإطار الذي يضمن أن الاستثمارات التقنية تدعم أهداف الأعمال. وهي تشمل القيادة، والهياكل التنظيمية، والعمليات التي تضمن أن تقنية المعلومات للمؤسسة تدعم وتوسع استراتيجيات وأهداف المؤسسة عن طريق

- التأكد من تناسب الأهداف الاستراتيجية لتكنولوجيا المعلومات مع آليات حوكمة مناسبة
- التأكد من تصميم أعمال وأنشطة تكنولوجيا المعلومات بالجهة للحصول على أفضل عائد ممكن من تكنولوجيا المعلومات
- التأكد من الالتزام الاستراتيجي

أمثلة:

- التأكد من وضع هيكل لحوكمة تكنولوجيا المعلومات
- التأكد من إعداد سياسات وإجراءات تكنولوجيا المعلومات وأمن المعلومات لإدارة العمليات ذات العلاقة
- التأكد من إعداد استراتيجية لتكنولوجيا المعلومات وفقاً لاستراتيجية النشاط

استمرارية العمل والتعافي من الكوارث :
IT Business Continuity & Disaster Recovery

استمرارية الأعمال هي التخطيط والاستعداد لضمان قدرة المؤسسة على الاستمرار في العمل في حالة وقوع حوادث خطيرة أو كوارث وقدرتها على التعافي إلى حالة تشغيلية في فترة قصيرة نسبيًا. عن طريق

- **التأكد من تضمين استمرارية خدمات تكنولوجيا المعلومات في أنظمة إدارة استمرارية تكنولوجيا المعلومات المتبعة من قبل الجهة**
- **التأكد من استمرارية خدمات تكنولوجيا المعلومات في أوقات الكوارث**
- **الالتزام باتفاقيات مستوى الخدمة والقوانين والتشريعات ذات العلاقة**

أمثلة:

- مراجعة خطط استمرارية تكنولوجيا المعلومات والتعافي من الكوارث
- التأكد من اختبار هذه الخطط بصورة دورية
- التأكد من النسخ الاحتياطية

ديـــوان المحاسبـــة
State Audit Bureau
State of Qatar • دولـــة قطـــر

تحليل البيانات

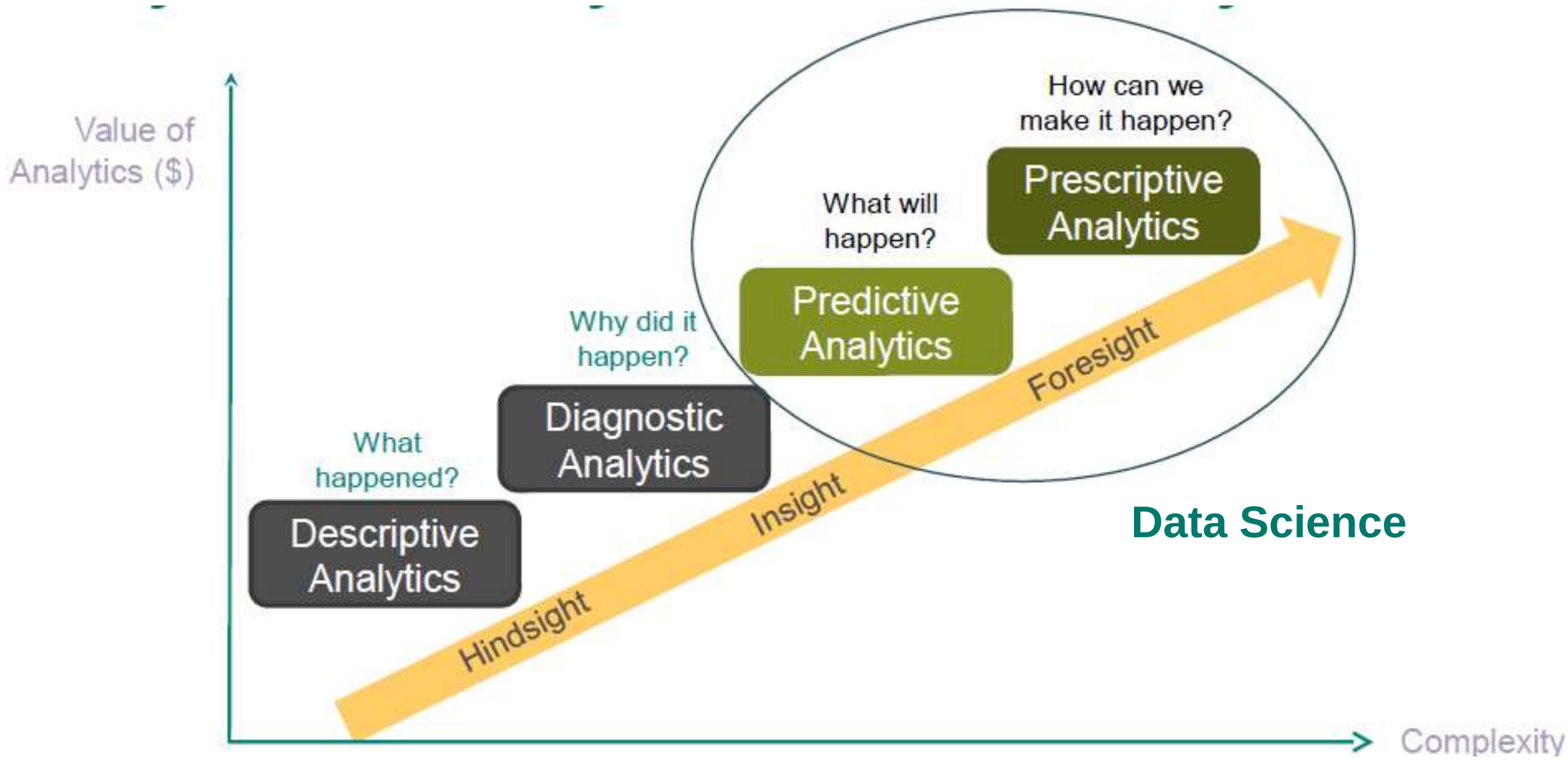
تحليل البيانات

- يعد تحليل البيانات جزءًا لا يتجزأ من الاتجاهات الحديثة في عمليات تدقيق تكنولوجيا المعلومات ، مما يمكّن المدققين من الاستفادة من الرؤى المستندة إلى البيانات لتقييم المخاطر واكتشاف المشكلات وتقديم توصيات مستنيرة لتحسين مستوى الجودة والكفاءة والامتثال بأنظمة تكنولوجيا المعلومات.
- يمكن استخدام نتائج تحليل البيانات في أي مرحلة من مراحل التدقيق، سواء كان ذلك في التخطيط أو التنفيذ أو إعداد التقارير، لاستخلاص الأفكار أو الأدلة أثناء عملية التدقيق.
  - **مرحلة التخطيط**، يمكن تحديد المشكلات وتخطيط الوحدة وتصميم العينة من خلال نتائج تحليل البيانات.
  - **مرحلة التنفيذ**، يمكن لنتائج تحليل البيانات تحديد الاستثناءات أو الانحرافات أو حتى وصف حالة موجودة والتي يمكن استخدامها كأدلة تدقيق.
  - **مرحلة إعداد التقارير**، يمكن عرض نتائج تحليل البيانات المرسومة في مرحلة التنفيذ للحصول على تقدير أفضل لنتائج التدقيق.

مزايا تحليل البيانات في عمليات التدقيق

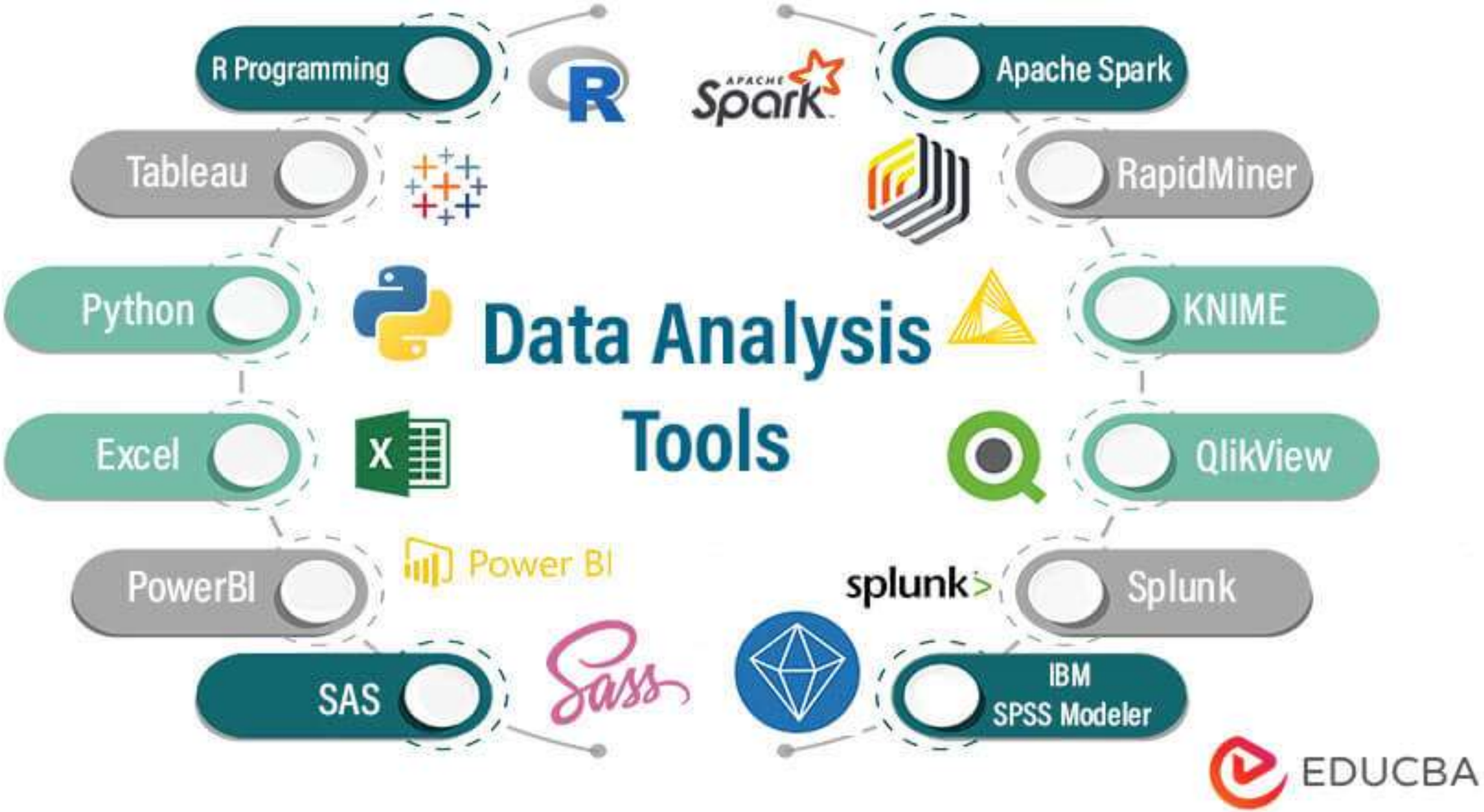
- تساهم أدوات وتقنيات تحليل البيانات على تعزيز سرعة وفعالية عمليات التدقيق والتي تلعب دورًا حاسمًا في مساعدة مدققي تكنولوجيا المعلومات في:
  - تحديد الحالات الشاذة.
  - تقييم المخاطر.
  - اكتشاف الاحتيال.
  - التحقق من الامتثال.
  - تحسين التكلفة.
  - تحليل الاسباب الجذرية للمشكلات.
  - تحليل الاتجاهات.
  - العرض والتلخيص

أنواع تحليل البيانات في عمليات التدقيق



Data Science

أدوات تحليل البيانات

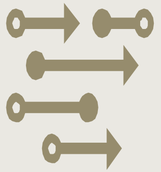


مزايا تحليل البيانات في عمليات التدقيق

Customization

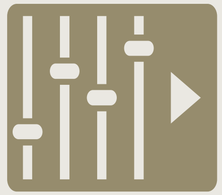
تعديل ادوات تحليل البيانات لدعم احتياجات العمل (مثل اختبار إدخال دفتر اليومية)

القدرة على التنبؤ



لقدرة على تكرار العمليات عبر نوع العمل وارتباطات العملاء

حجم الاختبارات

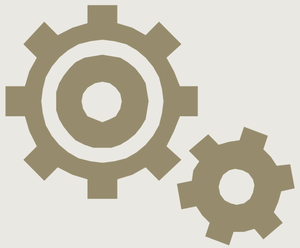


توفر القدرة على اختبار جميع السكان بدلاً من العينة

تفسير البيانات

تسمح أدوات العرض والتحليل برؤية أفضل للبيانات وتحديد المجالات التي تهم المدققين

الكفاءة



يؤدي استخدام تحليلات البيانات إلى زيادة الوقت المستغرق في تنظيم البيانات وتحويلها إلى معلومات

ديـــوان المحاسبـــة

State Audit Bureau

State of Qatar • دولـــة قطـــر

بسم الله الرحمن الرحيم

بالتعاون مع المجموعة العربية للأجهزة العليا للرقابة المالية والمحاسبة

المشارك سعيد سعيد دبوان

تجربة الجهاز المركزي للرقابة والمحاسبة

في استخدام نظم المعلومات الاليه

الطرق الحديثة للرقابة على الانظمة المعلوماتية

تميزت العقود الأخيرة من القرن العشرين بظهور تطورات في عالم المعلومات والاتصالات وتوسع كبير في استخدام الحاسوب والبرامج والتطبيقات المعلوماتية نتيجة للتوسع في حجم الأعمال والحاجة للمعلومات اللازمة لإدارتها.

أهمـــــــية تطوير وسائل المراجعة في الجهاز

تنبع أهمية تطوير وسائل وإجراءات المراجعة من الحاجة إلى الارتقاء بعملية المراجعة المحاسبية وأساليبها لتتلائم مع التطور التكنولوجي المستمر في المعالجة الآلية للمعلومات لدى الكثير من الجهات الخاضعة لمراجعة الجهاز.

أهم المحاور المتعلقة بتجربة الجهاز في الرقابة المعلوماتية

1) تطوير وتحديث البنية التحتية المعلوماتية.
2) التأهيل والتدريب الداخلي والخارجي.
3) الإقتناء أو التنفيذ للبرامج والتطبيقات.
4) التطبيق العملي لتلك البرامج والتطبيقات.

محاور تفصيلية بتجربة الجهاز في الرقابة المعلوماتية

1. إقتناء أجهزة الحاسوب اللازمة للعمل
2. تنفيذ أعمال الشبكات والربط الشبكي
3. تنفيذ برامج آلية لتسيير بعض الاعمال
4. تنفيذ برامج ألية للمراجعة
5. إقامة دورات تدريبية داخلية
6. التنسيق لإقامة دورات تدريبية خارجية
7. صرف أجهزة لابتوب لمراجعي الجهاز
8. جاري وضع خطط تطوير أداء مستقبلا

البرامج الألية المستخدمة في أعمال الجهاز:-

- ***نظام المرتبات والأجور الإضافية***
- ***نظام الشؤون المالية***
- ***نظام معلومات القروض***

علاوة على استخدام برامج وتطبيقات مايكروسوفت أوفس

نظام المرتبات والأجور الإضافية

يهدف هذا النظام الى توفير المعلومات اللازمة عن المرتبات والأجور الإضافية لموظفي الجهاز المركزي للرقابة والمحاسبة وقد تم تقسيم المعلومات فيه الى ملف المعلومات الثابتة وملف معلومات العهد والادخار ملف المعلومات الطارئة وملف المعلومات الرئيسية يتم من خلال التعامل مع هذه البيانات إنشاء ملف يحتوي على كافه تفاصيل المرتب وبحسب المعلومات المدخلة من قبل الموظف المختص ويتم بعد ذلك طباعه التفاصيل الخاصة بجميع الموظفين في الجهاز علاوة على كشوفات مرتبات الموظفين ويمكن إستخراج بعض التقارير من هذا النظام التي يتم استخدامها في إتخاذ القرارات وأرشفة البيانات

نظام الشؤون المالية

يهدف هذا النظام الى توفير المعلومات اللازمة عن النظام المحاسبي المعمول به في إدارة الحسابات في الجهاز وتم تقسيم المعلومات في هذا النظام الى سجل اليومية العامة وسجل المفردات حيث يتم إدخال جميع إستمارات الصرف والتسويات في دفتر اليومية العامة بشكل إجمالي ومن ثم يتم تفصيل مفردات الصرف في دفتر المفردات بحيث يتم توزيعها على مستوى الباب والفصل والبند والنوع كما هو الحال في جميع أنظمة المعلومات ويمكن من خلال البرنامج إستخراج بعض التقارير المطلوبة لدعم متخذي القرار وتقديرات إعداد الموازنات وغيرها

نظام معلومات القروض

يهدف هذا النظام لجمع المعلومات المتعلقة بالقروض ومصادرها وأوجه صرفها والمشاريع المخصصة لها والمشاريع المنفذة منها علاوة على عملة التمويل وتاريخ ومدة سريان القرض والجهة المختصة بالتنفيذ والتصرف بالقرض وغيرها من البيانات الهامة الي توفر قاعدة بيانات شاملة عن كافة القروض المحلية والخارجية المقدمة للدولة.

ارجو أن أكون قد وفقت في تقديم ما أمكن