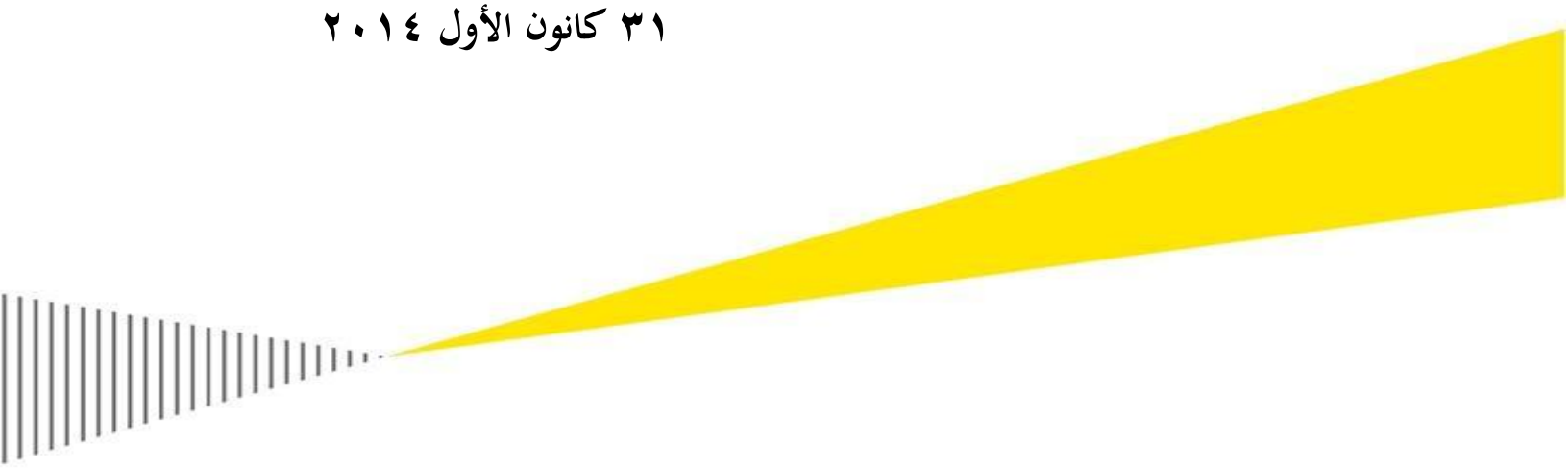
صندوق التنمية للعراق والحساب اللاحق

مذكرة متابعة الأمور الظاهرة من عملية تدقيق السنوات السابقة

نظام معلومات وزارة المالية والبنك المركزي

٣١ كانون الأول ٢٠١٤



EY

نبني عالماً أفضل للعمل

إرنست و يونغ
صندوق بريد ٦٠٠٤
منزل ٢٣، شارع ٣ (شارع الأميرات) حي ٦٠٩،
حي المنصور، بغداد، العراق

هاتف: ٠٣٥٧ ٥٤٣ ١ ٩٦٤+
فاكس: ٩٨٥٨ ٥٤٣ ١ ٩٦٤+
baghdad.iraq@iq.ey.com
ey.com/mena

١٥ كانون الأول ٢٠١٥

السادة رئيس وأعضاء لجنة الخبراء الماليين
صندوق التنمية للعراق والحساب اللاحق
بغداد – العراق

تحية طيبة وبعد،

لقد قمنا بتدقيق نظام المعلومات في وزارة المالية والمؤسسات التابعة لها. ويسرنا أن نبين ما يلي:
يوجد في قسم المحاسبة التابع لوزارة المالية نظامين تم تطويرهما داخليا من قبل مبرمجي الوزارة وذلك لتسجيل جميع العمليات المالية المتعلقة بصندوق التنمية للعراق والحساب اللاحق سواء كانت إيرادات أو نفقات.

١. **نظام الدينار العراقي**: وقد تم تطويره بإستخدام برنامج الفيجيوال فوكس برو، ويستخدم لتسجيل جميع الحركات المالية التي تتم بالدينار العراقي الخاصة بصندوق التنمية للعراق والحساب اللاحق.
٢. **نظام الدولار الأمريكي**: وقد تم تطويره بإستخدام برنامج مايكروسوفت أكسس، ويستخدم لتسجيل جميع الحركات المالية التي تتم بالدولار الأمريكي الخاصة بصندوق التنمية للعراق والحساب اللاحق.

إن قسم تكنولوجيا المعلومات في البنك المركزي العراقي يستخدم **نظام سويفت** وذلك لعمل التحويلات الإلكترونية الخاصة بصندوق التنمية للعراق والحساب اللاحق. وقد تم شراء هذا النظام من شركة مجموعة المهندسين المتحدين.
إن الأنظمة أعلاه تؤثر على البيانات المالية الخاصة بصندوق التنمية للعراق والحساب اللاحق، لذلك، فقد قررنا القيام بعملية مراجعتها وتدقيقها.

المذكرة المرفقة تتضمن اقتراحات لتحسين تكنولوجيا المعلومات ومحددات السرية المتعلقة بها والتي لفتت إنتباهنا أثناء مراجعتنا لنظم المعلومات المختارة والمتعلقة بصندوق التنمية للعراق والحساب اللاحق للسنة المنتهية في ٣١ كانون الأول ٢٠١٤.
إن مراجعتنا للأنظمة التي قمنا بإختيارها يهدف إلى مساعدتنا في إبداء رأينا حول البيانات المالية وليس للكشف عن عمليات الاحتيال التي قد تحدث. إن عملية المراجعة والتدقيق التي نقوم بها ليس من الضرورة أن تشمل جميع التحسينات الممكنة لكافة نقاط الضعف القائمة.

سيكون من دواعي سرورنا أن نقوم بمناقشة هذه التوصيات معكم و كذلك مساعدتكم في تنفيذها.

ختاماً، نشكركم على إتاحة هذه الفرصة لنا لتقديم خدماتنا ونشكر كافة العاملين في جميع دوائر ومؤسسات الدولة لما أبدوه من تعاون لتسهيل مهمتنا، راجين لكم دوام التقدم والازدهار.

وتفضلوا بقبول فائق الاحترام ، ، ، ،

Ernst + Young

إرنست ويونغ/ العراق

مفتاح الرموز

يحتوي هذا التقرير على الرموز التالية:

الرمز	البيان
درجة المخاطرة عالية	تتعلق الملاحظة بضعف جوهري يؤثر في تحقيق الأهداف الأساسية أو النتائج المالية أو تؤثر في السمعة المهنية. نوصي بضرورة إتخاذ إجراءات معالجة فورية.
درجة المخاطرة متوسطة	تتعلق الملاحظة بالأمور متوسطة الخطورة و التي قد تؤدي إلى ضعف في نظام الرقابة الداخلي و/أو كفاءة الأنشطة التشغيلية والتي يجب أن يتم الأفصاح عنها. نوصي باتخاذ إجراءات معالجة خلال فترة قصيرة.
درجة المخاطرة منخفضة	تتعلق الملاحظة بأمور قمنا بملاحظتها قد لا تؤثر على نظام الرقابة الداخلي و/أو فاعلية وكفاءة الأنشطة التشغيلية، ولكن يجب الإهتمام بها من قبل الإدارة. نوصي بإتخاذ إجراءات معالجة خلال فترة معقولة.

ملخص الملاحظات

التسلسل	المؤسسة	الملاحظة	درجة المخاطرة
١.	وزارة المالية	صلاحيات المبرمج لتعديل البيانات – أنظمة الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية
٢.	وزارة المالية	توثيق تعديلات النظام – أنظمة الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية
٣.	وزارة المالية/ البنك المركزي	إجراءات طلب تعديل النظام – أنظمة الدينار العراقي، والدولار الامريكي، والمدفوعات والمقبوضات	درجة المخاطرة عالية
٤.	وزارة المالية	الدخول إلى برامج الأنظمة – أنظمة الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية
٥.	وزارة المالية/ البنك المركزي	تحديثات نظم التشغيل – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة متوسطة
٦.	وزارة المالية/ البنك المركزي	سياسات وإجراءات تقنية المعلومات – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية
٧.	وزارة المالية/ البنك المركزي	الوصف الوظيفي – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة متوسطة
٨.	وزارة المالية/ البنك المركزي	التدقيق الداخلي لتقنية المعلومات – انظمة الدينار العراقي، والدولار الأمريكي، والمدفوعات والمقبوضات، والسويفت	درجة المخاطرة متوسطة
٩.	وزارة المالية/ البنك المركزي	تعديل البرامج – انظمة الدينار العراقي، والدولار الامريكي، المدفوعات والمقبوضات	درجة المخاطرة عالية
١٠.	وزارة المالية	فصل المهام – نظامي الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية
١١.	وزارة المالية	فصل بيئات التطوير والاختبار للأنظمة – نظامي الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية
١٢.	وزارة المالية/ البنك المركزي	مراجعة سجلات التدقيق – انظمة الدينار العراقي، والدولار الامريكي، المدفوعات والمقبوضات	درجة المخاطرة متوسطة
١٣.	وزارة المالية/ البنك المركزي	ضوابط كلمة السر للأنظمة – أنظمة الدينار العراقي، والدولار الامريكي، والمدفوعات والمقبوضات	درجة المخاطرة عالية
١٤.	وزارة المالية/ البنك المركزي	ضوابط الخروج التلقائي – أنظمة الدينار العراقي، والدولار الامريكي، والمدفوعات والمقبوضات، والسويفت	درجة المخاطرة متوسطة
١٥.	وزارة المالية/ البنك المركزي	ضوابط اغلاق حساب مستخدم – أنظمة الدينار العراقي، والدولار الامريكي، والمدفوعات والمقبوضات	درجة المخاطرة متوسطة
١٦.	وزارة المالية/ البنك المركزي	برامج مكافحة الفايروسات – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية
١٧.	وزارة المالية/ البنك المركزي	الشبكات المحلية و الواسعة (LAN/WAN) – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة متوسطة
١٨.	وزارة المالية/ البنك المركزي	إدارة النسخ الاحتياطية – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية
١٩.	وزارة المالية/ البنك المركزي	واجهات أنظمة صندوق التنمية للعراق – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية
٢٠.	وزارة المالية/ البنك المركزي	أمنية الحواسيب – انظمة الدينار العراقي، والدولار الأمريكي، والمدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية

الملاحظات

١. صلاحيات المبرمج لتعديل البيانات – أنظمة الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية

الملاحظة:

لاحظنا أن مبرمجي الأنظمة لهم الصلاحية المطلقة في الوصول إلى وتعديل قاعدة بيانات نظامي الدينار العراقي والدولار الامريكي لصندوق التنمية للعراق، حيث تمكنهم الصلاحيات الممنوحة على النظام من تغيير كافة المعطيات في قاعدة البيانات دون وجود محددات لذلك.

إن غياب الفصل الكافي بين الواجبات على الأنظمة يزيد من احتمالية حدوث تغييرات غير مصرح بها على بيانات الأنظمة دون أن يتم اكتشافها في الوقت المناسب مما يؤدي الى تعريض أمن وسرية البيانات للخطر.

التوصية:

نوصي بضرورة فصل المهام ما بين عمليات الإدخال، إدارة قاعدة البيانات، والبرمجة. بحيث يتم حفظ نسخة من قاعدة البيانات في جهاز منفصل لإجراء عملية الفحص والاختبار من قبل مدير قاعدة البيانات وذلك لمزيد من إجراءات الضبط والرقابة.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال سنة ٢٠١٤.

٢. توثيق تعديلات النظام – أنظمة الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية

الملاحظة:

لاحظنا من خلال مراجعتنا عدم وجود نظام لتوثيق التعديلات التي يتم إجراؤها على نظامي الدينار العراقي والدولار الامريكي. إضافة إلى ذلك فإن عملية توثيق المعلومات الخاصة بعملية برمجة الانظمة غير فعالة.

التوصية:

نوصي بضرورة توثيق جميع التغييرات التي تتم على برمجة النظام بشكل مفصل مما يسهل عملية مراجعة جميع التفاصيل المتعلقة بالتعديلات التي تتم على النظام، وبالتالي زيادة كفاءة عملية كتابة البرنامج.

إضافة إلى ذلك نوصي باستخدام نماذج خاصة لتوثيق برمجة النظام، وعرض تاريخ التعديلات التي يتم إجراؤها على النظام، وينبغي أن يحتوي هذا النموذج على اسم المبرمج، رقم البرنامج، التاريخ، الغرض من التعديل، رقم طلب التعديل والمستخدم المتعلق به، بالإضافة إلى وصف لعملية التعديل وذلك لمزيد من إجراءات الضبط والرقابة.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

٣. إجراءات طلب تعديل النظام – أنظمة الدينار العراقي، والدولار الامريكي، والمدفوعات والمقبوضات	درجة المخاطرة عالية

الملاحظة:

لاحظنا عدم وجود إجراءات موحدة يتبعها مستخدمي أنظمة الدينار العراقي والدولار الامريكي والمدفوعات والمقبوضات لصندوق التنمية للعراق فيما يختص بطلبات تعديل وصيانة وتطوير الأنظمة. وفي أغلب الأحيان تكون تلك الطلبات شفهية.

بدون طلب رسمي لعمل التعديل والتطوير على برنامج النظام، يصبح النظام معرض للمخاطر، حيث أن بعض التعديلات قد لا تكون صحيحة، أو لم يتم اختبارها بشكل كافي قبل تطبيقها.

وللمساعدة في ضمان الحصول على هذه الأهداف، يجب تطوير وتطبيق عملية توثيق التعديلات المطلوبة من قبل المستخدم.

التوصية:

نوصي بضرورة استخدام نماذج خاصة لتوثيق كافة طلبات التعديل المستلمة من مستخدمي النظام، على أن تكون هذه النماذج مرقمة وتشتمل على التفاصيل التالية على الأقل :

- اسم المستخدم طالب التعديل.
- تاريخ الطلب.
- وصف للتعديلات المطلوبة.
- التاريخ المطلوب لإنجاز الطلب.
- موافقة مدير الدائرة على التعديل.

كما نوصى بضرورة حفظ طلبات التعديل المنجز وفقاً لتسلسلها مع مراعاة المراجعة الدورية لاكتمال هذا التسلسل مما يسهل تحديد الطلبات التي لم يتم انجازها والعمل على متابعتها.

إن عملية التوثيق تتطلب اهتمامًا كافياً لما لها من اهمية في إثبات عمليات طلبات التعديل والموافقات المتعلقة بها.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

٤. الدخول إلى برامج الأنظمة – أنظمة الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية

الملاحظة:

لاحظنا من خلال مراجعتنا أن مبرمجي الأنظمة لهم السيطرة الكاملة على برامج نظامي الدينار العراقي والدولار الامريكي لصندوق التنمية للعراق. حيث يقوم المبرمج بكافة عمليات إدارة وتطوير ودعم النظام.

إن هذه العمليات تقع ضمن اختصاصات مختلفة وبالتالي فإن إمكانية عمل تعديلات غير موافق عليها مسبقاً بدون أن يتم اكتشاف ذلك تصبح عالية.

التوصية:

نوصي بضرورة مراجعة مستوى الصلاحيات الممنوحة للمبرمج، بحيث تمنع هذه الصلاحيات المبرمج من تعديل برامج الأنظمة وذلك لتقليل احتمالية حدوث تعديلات غير موافق عليها مسبقاً.

إن تعديل برامج الأنظمة يجب أن يتم تحت الإشراف المباشر لإدارة الصندوق وذلك لإعطاء مزيد من إجراءات الضبط والرقابة.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

٥. تحديثات نظم التشغيل – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة متوسطة

الملاحظة:

لاحظنا أن نظم التشغيل المتعلقة بأنظمة صندوق التنمية للعراق لا يتم تحديثها بشكل دوري حسب آخر التحديثات التي تصدر على شبكة الانترنت من قبل شركة مايكروسوفت.

إن ذلك يزيد من مخاطر إمكانية استغلال نقاط الضعف في نظم الحماية الخاصة بنظام التشغيل.

التوصية:

نوصي بمتابعة آخر التحديثات الخاصة بنظام التشغيل والتي تصدر من قبل شركة مايكروسوفت على شبكة الانترنت واختبارها وتطبيقها على أنظمة التشغيل المتعلقة بأنظمة بصندوق التنمية للعراق بشكل دوري وذلك لمزيد من إجراءات الضبط والرقابة .

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

6. سياسات وإجراءات تقنية المعلومات – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية

الملاحظة:

من خلال مراجعتنا، لاحظنا عدم وجود دليل سياسات وإجراءات موثق لتقنية المعلومات وذلك لإدارة نظم المعلومات والبنية التحتية لتقنية المعلومات.

بدون تطوير سياسات وإجراءات شاملة لتقنية المعلومات، ستجد المؤسسة أنه من الصعوبة أن تدير بشكل فعال ومستمر نشاطات تقنية المعلومات وتسيطر على مخاطر الأعمال المتعلقة بها وتطوير عملياتها اللازمة لتحقيق الأهداف الداخلية والخارجية.

التوصية:

نوصي بتطوير سياسات وإجراءات لتقنية المعلومات وتوثيقها وجعلها متاحة بأيدي الموظفين.

يجب على الإدارة الموافقة على السياسات والإجراءات لضمان مايلي:

- توافق مهام تقنية المعلومات مع أهداف المؤسسة.
- يتم تنفيذ الوظائف التكنولوجية حسب الممارسات المنهجية.

إن السياسات والإجراءات يجب أن تركز وبشكل غير محدد على ما يلي:

- المستخدمين وصلاحيات الدخول.
- اجراءات تعديل البرامج.
- العمليات اليومية والتقارير.
- حل المشاكل التقنية والبرمجية ومحاولة تجنبها.
- صيانة ومراقبة ملفات الدخول.
- التدريب والتعليم.
- عمل النسخة الاحتياطية.
- طرق اختيار وتطوير وصيانة البرمجيات والاجهزة.
- مراقبة الأداء والقدرة على التخطيط.

أن المراجعة المستقلة هي عملية ضرورية لضمان الفهم والتطبيق الصحيح للسياسات والإجراءات.

مراقبة ومتابعة الأعمال المنجزة وذلك لضمان أن العمل المنجز قد تم حسب السياسات والإجراءات الموضوعة.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

٧. الوصف الوظيفي – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة متوسطة

الملاحظة:

من خلال مراجعتنا، لاحظنا عدم وجود دليل رسمي وموثق للتوصيف الوظيفي، والذي يشرح بصورة واضحة مسؤوليات ومهام كل وظيفة وكذلك المؤهلات والمهارات التقنية التي يجب توافرها في الكادر.

بدون تطوير دليل للتوصيف الوظيفي بحيث يتم تحديثه بشكل دوري، سيكون من الصعب على الإدارة توزيع حمل العمل على الأشخاص أو الموظفين المناسبين لتلك الأعمال والذي يؤدي الى التداخل غير المناسب في تنفيذ المهام. بإستمرار عملية تعيين الكوادر من الممكن أن تزيد المشكلة بسبب كون الكادر الجديد لا يمتلك الدراية الكافية بماهو متوقع منه أو المخاطر الناتجة من كونهم ليسو ملائمين للأعمال المناطة بهم، حيث أن ذلك يؤدي الى عدم كفائتهم في تنفيذ المهام.

التوصية:

على الإدارة الأخذ بعين الإعتبار تطوير دليل توصيف للوظائف خاص بدائرة تقنية المعلومات بحيث يشتمل على المهام والمسؤوليات لكل كادر من كوادر الدائرة بالإضافة الى الصلاحيات والمهارات التقنية والمؤهلات العلمية لكل وظيفة وضمان التحديث الدوري للدليل.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

٨. التدقيق الداخلي لتقنية المعلومات – انظمة الدينار العراقي، والدولار الأمريكي، والمدفوعات والمقبوضات، والسويفت	درجة المخاطرة متوسطة

الملاحظة:

من خلال مراجعتنا، لاحظنا بأنه لايوجد تدقيق داخلي لتقنية المعلومات وذلك لمراجعة النشاطات التي تقوم بها بالإضافة الى ضمان وجود السيطرة الفعالة.

الإدارة قد لا تكون متأكدة من فعالية أداء التدقيق الداخلي في المناطق التي تعتمد على وجود انظمة المعلومات. وكذلك عدم وجود عملية تقييم مستقلة يؤدي الى عدم قدرة الإدارة على ضمان أن برامج ومعدات تقنية المعلومات يتم استخدامها بشكل فعال بحيث يتم المحافظة على سرية البيانات.

التوصية:

يجب ان تأخذ الإدارة بعين الإعتبار تعيين مدقق داخلي لتقنية المعلومات لكي يؤدي مايلي:

- التأكد من التعديلات التي تنفذ على البرامج وعملية الدخول الى البيانات والملفات تتم بصورة مناسبة ومسيطر عليها.
- استخدام نظام متخصص لبيان كفاية وكفاءة المحددات الداخلية.
- مراجعة محددات الدخول المستخدمة لجميع أنظمة تقنية المعلومات وبصورة دورية.
- المشاركة في مراجعة معايير المحددات الداخلية خلال مرحلة تصميم الأنظمة الجديدة، هذه المشاركة تساعد على ضمان تطبيق محددات مناسبة لتلك الأنظمة وكذلك ضمان فحصها وتعديلها بطرق مناسبة وموافق عليها.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

٩. تعديل البرامج – انظمة الدينار العراقي، والدولار الامريكي، المدفوعات والمقبوضات	درجة المخاطرة عالية

الملاحظة:

فيما يتعلق بتعديل البرامج، لاحظنا ما يلي:

- لا يتم تسجيل التعديلات التي تتم على الانظمة.
- لا يوجد وصف لماهية التعديل.
- لا يوجد معايير لتسمية متغيرات الانظمة.
- لا يتم عمل إصدارات للبرامج.

من دون وجود منهجية لتسجيل التعديلات فإن الإدارة لن تكون قادرة على ضمان ان التعديلات التي تجرى على الانظمة موافق عليها وتم اعتمادها. بألاضافة الى ذلك، مع عدم وجود معايير لتسمية المتغيرات واصدارات للبرامج فإن قسم تكنولوجيا المعلومات سيجد صعوبة في تحديد آخر تعديل أو تحديث تم على الأنظمة.

التوصية:

نوصي بوضع وصف كامل ودقيق فوق كل تعديل يتم على برامج الأنظمة، وهذا سوف يساعد في تسريع عملية تحديد التعديلات. بالأضافة الى ذلك، ينبغي لقسم تكنولوجيا المعلومات أن يأخذ بنظر الاعتبار وضع آلية يتم اتباعها في تسمية متغيرات البرامج وكذلك لعمل إصدارات للبرامج والأنظمة.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

١٠. فصل المهام – نظامي الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية

الملاحظة:

من خلال مراجعتنا لاحظنا أن نفس الشخص الذي يدير قاعدة بيانات ونظام التشغيل هو / هي نفس الشخص الذي يقوم بعمل وطوير الأنظمة.

إن الخطر الموجود من كون كادر تقنية المعلومات من الممكن أن يقوم بعمل تعديلات على الأنظمة غير مصرح لهم القيام بها، حيث أنه من الممكن أن يؤدي الى تعريض أمن وسرية البيانات للخطر.

التوصية:

نوصي الإدارة أن تعمل على ضمان الفصل بين مهام وواجبات مبرمجي الأنظمة والمشرفين على نظم التشغيل ومديري قاعدة البيانات.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

١١. فصل بيئات التطوير والاختبار للأنظمة – نظامي الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية

الملاحظة:

من خلال مراجعتنا لنظامي الدينار العراقي والدولار الأمريكي، لاحظنا أنه لا يتم فصل بيئات التطوير والاختبار ، حيث انه يتم تطوير البرامج الجديدة وفحصها على نفس الجهاز.

من دون الفصل الفعلي لبيئات التطوير والاختبار للأنظمة، البرامج الجديدة من الممكن أن يتم نسخ برامج قديمة عليها بالخطأ بحيث يتم الغاؤها بعد أن تم فحصها واعتمادها، وهذا قد يؤدي الى النتائج التالية:

- وضع وادخال برامج غير معتمدة على الأنظمة.
- ظهور اخطاء في الأنظمة من الصعوبة حلها.

التوصية:

ينبغي على الإدارة إنشاء بيئتين منفصلتين لتطوير البرامج وفحصها، وذلك لضمان الفصل في الأدوار والمسؤوليات بين مطوري الأنظمة ومديري قاعدة البيانات ونظم التشغيل.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

١٢. مراجعة سجلات التدقيق - انظمة الدينار العراقي، والدولار الامريكي، المدفوعات والمقبوضات	درجة المخاطرة متوسطة

الملاحظة:

من خلال مراجعتنا لأنظمة الدينار العراقي والدولار الامريكي والمدفوعات والمقبوضات، لاحظنا أنه لم يتم تفعيل خاصية التدقيق الخاصة بقاعدة البيانات ونظام التشغيل والمتعلقة بالأنظمة وذلك لتسجيل الحركات التي تتم عليها.

إن تفعيل هذه الخاصية يساعد على كشف التغييرات الغير معتمدة والتي من الممكن أن تحدث على البرامج بحيث تبين من الذي قام بعملية التغيير والتاريخ الذي تمت فيه هذه العملية.

التوصية:

ينبغي للإدارة التأكد من تفعيل خاصية التدقيق الخاصة بقواعد البيانات ونظم التشغيل وذلك لتسجيل التغييرات والأنشطة على التي تتم على الأنظمة.

يعتبر تفعيل التدقيق طريقة فعالة لمراقبة التغييرات وتحديد الغير معتمد منها ومتابعة حالتها.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

١٣. ضوابط كلمة السر للأنظمة – أنظمة الدينار العراقي، والدولار الامريكي، والمدفوعات والمقبوضات	درجة المخاطرة عالية

الملاحظة:

من خلال مراجعتنا لأنظمة الدينار العراقي والدولار الامريكي والمدفوعات والمقبوضات، لاحظنا الأمور التالية فيما يتعلق بالضوابط المتعلقة بكلمة السر:

- المستخدمين ليس لديهم الحق في اختيار كلمات السر الخاصة بهم.
- يتم حفظ كلمات السر في قاعدة بيانات بنص واضح.
- كلمات السر غير معقدة.
- كلمة السر غير قابلة للتغيير.
- لا يتم الاحتفاظ بأرشيف كلمة السر.
- ليس هناك تحديد أدنى لطول كلمات السر.

بمرور الزمن، اذا لم يتم تغيير كلمات السر من فترة لأخرى يؤدي ذلك الى فقدانها لفاعليتها وسريتها وبالتالي الى زيادة الفرص لإختراق قاعدة البيانات من قبل أشخاص غير مسموح لهم بدخولها بحيث يصبحوا قادرين على الدخول الى النظام والإطلاع على البيانات.

إن إستخدام كلمات سر بسيطة ومستخدمة سابقاً يؤدي الى السهولة النسبية في معرفتها مما يؤثر على فعالية ضوابط الدخول الى النظام والإطلاع على البيانات السرية.

أن عدم تشفير كلمة السر عند تخزينها في قاعدة البيانات قد يعرض المؤسسة الى مخاطر الكشف عنها من قبل اشخاص غير مخولين بمعرفتها والذي يؤدي بدوره الى الحصول على بيانات ومعلومات سرية واحتمالية التلاعب فيها.

التوصية:

على الإدارة أن تسعى الى تطبيق ما يلي:

- إجبار المستخدمين تغيير كلمات سرهم الإساسية عند دخولهم الأول الى النظام.
- عمر كلمات السر يجب أن يكون ملائماً (شهر أو شهرين) وأن يكون هذا التحديد مقياس لكل المستخدمين.
- تحديد الحد الأدنى لطول كلمات السر (لا يقل عن ستة أحرف، يفضل أن يكون ثمانية أحرف).
- يجب أن تكون كلمات السر معقدة (متكونة من أحرف وأرقام).

- حفظ كلمات السر القديمة في ملف تاريخي في قاعدة البيانات (مثال: كلمات السر الثلاثة الأخيرة)، وذلك لمنع إعادة إستخدام نفس الكلمات السابقة.

بالإضافة الى ذلك، يجب أن يتم لفت انتباه الموظفين من خلال برامج توجيهة أمنية الى الحاجة الى تغيير كلمات السر بشكل فوري في حال اصبحت معروفة من قبل الآخرين.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

١٤. ضوابط الخروج التلقائي – أنظمة الدينار العراقي، والدولار الامريكي، والمدفوعات والمقبوضات، والسويفت	درجة المخاطرة متوسطة

الملاحظة:

من خلال مراجعتنا للأنظمة صندوق التنمية للعراق، لاحظنا عدم وجود ضوابط للخروج التلقائي من الأنظمة في حال تركها من دون استخدام فتره معينه من الزمن.

أن عملية ترك النظام مفتوح وفعال من دون استخدام يمكن أن يؤدي الى استخدامه من قبل اشخاص غير مصرح لهم بالدخول الى معلومات النظام مما يعرض سرية المعلومات وسلامتها الى الخطر.

التوصية:

على الإدارة أن تضع ضوابط ملائمة على واجهات النظام، وهذه الضوابط يجب أن تتضمن انهاء تفعيل الواجهات الفعالة بعد فترة محددة من عدم الإستخدام (مثلا ٥ دقائق).

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

١٥. ضوابط اغلاق حساب مستخدم – أنظمة الدينار العراقي، والدولار الامريكي، والمدفوعات والمقبوضات	درجة المخاطرة متوسطة

الملاحظة:

من خلال مراجعتنا لأنظمة الدينار العراقي والدولار الامريكي والمدفوعات والمقبوضات، لاحظنا بأن حساب المستخدم لا يتم إيقافه بعد عدد محدد من المحاولات الغير ناجحة للدخول الى النظام.

في غياب عملية إغلاق حساب المستخدم بطريقة تلقائية بعد عدد من محاولات الدخول الغير ناجح للنظام، من الممكن أن يؤدي ذلك الى الدخول غير مسموح به الى الأنظمة.

التوصية:

يجب أن تسعى الإدارة الى التعاون مع قسم تكنولوجيا المعلومات على وضع ضوابط لإغلاق حسابات المستخدمين الذين تجاوزوا العدد المحدد من محاولات الدخول الغير ناجح الى النظام. ويجب أن يشمل هذا التحديد عدد المرات المسموحة للإدخال الخاطىء لكلمة السر (٣ مرات مثلا).

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

١٦. برامج مكافحة الفايروسات – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية

الملاحظة:

خلال مراجعتنا للحواسيب المخصصة لأنظمة صندوق التنمية للعراق، لاحظنا أن برامج مكافحة الفيروسات في الحواسيب لا يتم تحديثها مع أحدث تعريفات الفيروسات. وعلاوة على ذلك، كلا من الخادم وحواسيب السويفت ونظام المدفوعات والمقبوضات غير محمية ببرامج مكافحة الفيروسات.

هنالك خطورة في إدارة الأعمال بدون برامج مكافحة الفيروسات وذلك لحماية المعدات الحاسوبية من البرامج الغير المرغوب والذي قد يؤدي الى احتمال حصول خسائر مادية، بالإضافة الى احتمالية حصول سرقة في البيانات بسبب عدم وجود الحماية المناسبة بحيث يصبح العمل عرضة للأشخاص المختصين في سرقة البيانات، حيث أنه من الممكن أن يؤدي ذلك اتخاذ إجراءات قانونية توقف العمل.

التوصية:

يجب على الإدارة التأكد من أن جميع أجهزة الكمبيوتر المحمولة وحواسيب الانظمة والخوادم محمية بالبرامج المضادة للفيروسات وجعل التحديث لهذه البرامج يتم بشكل تلقائي بالإضافة الى وضع جدول زمني منتظم يتم بشكل تلقائي لتنفيذ فحص أجهزة الحاسبات وبشكل دوري.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

١٧. الشبكات المحلية و الواسعة (LAN/WAN) – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة متوسطة

الملاحظة:

من خلال مراجعتنا لأنظمة الدينار العراقي والدولار الأمريكي والسويفت، لاحظنا عدم وجود شبكات محلية وواسعة لربط الأنظمة الخاصة بصندوق التنمية للعراق.

في غياب الشبكة المحلية والواسعة، سيؤدي ذلك الى التأخير في تنفيذ العمل بسبب الترحيل اليدوي للحركات المالية. بالإضافة الى ذلك، قد تواجه المؤسسة زيادة تكلفة نقل البيانات والمخاطرة بسرية البيانات بسبب الوضع الحالي في العراق.

التوصية:

ينبغي للإدارة أن تأخذ بنظر الاعتبار إنشاء شبكات محلية وواسعة لتوفير الاتصال بين دوائر المؤسسة وفروعها، حيث أن ذلك يساعد على تناقل المعلومات بصورة سريعة.

إن إنشاء هذه الشبكة سيزيد من فعالية عملية الرقابة والسيطرة وكذلك تقليل الوقت المستهلك لنقل وتجميع البيانات المالية.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

١٨. إدارة النسخ الاحتياطية – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية

الملاحظة:

عند فحص الضوابط لتي تحيط بعملية إجراء النسخ الاحتياطية من الأنظمة الخاصة بصندوق التنمية للعراق، لاحظنا ما يلي:

- لا يوجد إجراء رسمي موثق يتم إتباعة للقيام بعملية اجراء النسخ الاحتياطية.
- لا يوجد جدول زمني محدد للقيام بعملية عمل النسخ الاحتياطية.
- فيما يخص نظامي الدينار العراقي والدولار الامريكي، لا يتم نقل النسخ الاحتياطية الى مواقع خارجية وأمينة معتمدة من قبل الإدارة، وعوضا عن ذلك يتم حفظها على ذاكرات فلاش بحيث تبقى مع مستخدمي الأنظمة.
- فيما يخص نظام سويفت، يتم عمل النسخ الاحتياطية بشكل اسبوعي على قرص صلب بحيث يتم الاحتفاظ به مع الشركة التي طورت النظام..
- عدم الاحتفاظ بسجل تاريخي للنسخ الاحتياطية
- لا يتم تشفير بيانات النسخ الاحتياطية.

عدم وجود فحص دوري للنسخ الاحتياطية وذلك لضمان سلامة البيانات.

التوصية:

يجب على قسم تكنولوجيا المعلومات وضع سياسات وإجراءات موثقة بحيث تشتمل تعليمات عمل النسخ الاحتياطية بشكل دوري وبجدول زمني محدد، بالإضافة الى ما يلي:

- يجب أن يتم تخزين النسخ الاحتياطية في مكان آمن، ويجب أن يتم تخزين نسخة أخرى خارج المؤسسة الى منطقة آمنة ومعتمدة من قبل الادارة.
- عمل سجل تاريخي للنسخ الاحتياطية والاحتفاظ بها.
- التأكد من تشفير النسخ الاحتياطي.
- إجراء فحص دوري للنسخ الاحتياطية وذلك للتأكد من أن النسخ تم عملها بصورة صحيحة وسليمة.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

١٩. واجهات أنظمة صندوق التنمية للعراق – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية

الملاحظة:

من خلال مراجعتنا لأنظمة صندوق التنمية للعراق، لاحظنا عدم وجود وجهات تقوم بربط أنظمة الدينار العراقي والدولار الامريكي والمدفوعات والمقبوضات وسويفت مع بعضهم البعض وذلك لتبادل البيانات واستخراج التقارير.

المؤسسات المالية تميل إلى الاعتماد على واجهات الربط الآلي بين الأنظمة لتوفير التكامل التام بينها مع التقليل من التدخل اليدوي.

بدون وجود واجهات ربط الآلي ما بين الأنظمة، ربما تتعرض المؤسسة الى مخاطر الأخطاء البشرية الناجمة عن العمليات اليدوية. وعلاوة على ذلك، سيؤدي ذلك الى زيادة الوقت اللازم لتنفيذ العمل والكلفة والشكوك حول دقة البيانات المدخلة.

التوصية:

ينبغي على المؤسسة أن تأخذ بعين الإعتبار تطوير واجهات ربط آلية وذلك لربط جميع الأنظمة وذلك للتقليل من مخاطر الخطأ البشري وتوفير الوقت والتكلفة وتحسين فعالية العمل.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

20. أمنية الحواسيب – انظمة الدينار العراقي، والدولار الأمريكي، والمدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية

الملاحظة:

من خلال مراجعتنا للربط المباشر لحواسيب المستخدمين، لاحظنا ان مخارج الـ (USB) متاحة وفعالة، وكذلك ان المستخدم لديه صلاحيات ادارية على الحواسيب المتصلة بالنظام.

بالاستخدام الغير المنضبط لوسائل البيانات الخارجية فضلا عن امتلاك المستخدم للصلاحيات الادارية على الحاسوب يؤدي الى زيادة احتمالية انتشار الفيروسات. وعلاوة على ذلك، قد تحدث عملية تنصيب لبرامج غير مصرح بها وكذلك اخذ نسخ من المعلومات الحساسة والسرية.

التوصية:

نوصي بضرورة إيقاف تفعيل كافة وسائل الوصول المباشر إلى أجهزة الحاسوب الخاصة بأنظمة صندوق التنمية للعراق. بالإضافة إلى ذلك، نوصي بضرورة تقييد صلاحيات المستخدمين. في الحالات الخاصة والتي تستدعي تفعيل احد وسائل الوصول المباشر، يراعى الحصول على موافقة الإدارة المعنية بالإضافة إلى أن يكون ذلك تحت إشراف شخص مخول من قبل الإدارة.

رد الادارة:

المتابعة:
مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة ٢٠١٤.

إرنست ويونغ

خدمات التدقيق والضرائب والمعاملات والاستشارات

عن إرنست ويونغ

تعتبر إرنست ويونغ أحدى المؤسسات الرائدة على مستوى العالم في مجالات التدقيق والضرائب والمعاملات والاستشارات، حيث تضم إرنست ويونغ عدد كبير من الموظفين يصل الى ١٩٠,٠٠٠ تجمعهم مجموعة من القيم المشتركة والالتزام الشديد بالجودة.

تحدث إرنست ويونغ الفرق من خلال مساعدة كوادرها وعملائها والمجتمعات الأوسع نطاقاً على تحقيق أهدافهم وصقل إمكاناتهم .

تعتبر إرنست ويونغ عضواً في مؤسسة إرنست ويونغ العالمية المحدودة، ولكل منهما كياناً قانونية منفصلاً. ومؤسسة إرنست ويونغ العالمية المحدودة هي شركة محدودة بضمان وتعمل بالمملكة المتحدة ولا تقدم خدمات الى العملاء.لمزيد من المعلومات عن مؤسستنا يرجى زيارة موقعنا الالكتروني:www.ey.com.

تعود أعمال إرنست ويونغ في الشرق الأوسط إلى عام ١٩٢٣. على امتداد أكثر من ٨٥ سنة، نمت مؤسستنا وتطورت لتلبية الاحتياجات والتطورات القانونية والتجارية في المنطقة. لدينا عبر الشرق الأوسط أكثر من ٤,٢٠٠ فرد يتعاونون معاً من خلال ٢٠ مكتباً في ١٥ دولة عربية، يتقاسمون ذات القيم والالتزام الشديد بالجودة. نحن نحدث الفارق من خلال مساعدة فريقنا وعملائنا ومجتمعاتنا في تحقيق وتوظيف إمكاناتهم.

لمزيد من المعلومات يرجى زيارة الموقع الالكتروني:www.ey.com/me

هكذا نحدث الفرق في إرنست ويونغ