

صندوق التنمية للعراق والحساب اللاحق

مذكرة متابعة الأمور الظاهرة من عملية تدقيق السنوات السابقة

نظام معلومات وزارة المالية والبنك المركزي

٣١ كانون الأول ٢٠١٥

The logo consists of the letters 'EY' in a bold, black, sans-serif font. The 'E' and 'Y' are connected at the top and bottom. The 'E' has a horizontal bar that extends to the right, overlapping the 'Y'.

EY

نبني عالمأ
أفضل للعمل

٣٠ ايلول ٢٠١٦

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

تحية طيبة وبعد،

نتيجة لعملية التدقيق التي قمنا بها لقيود وسجلات صندوق التنمية للعراق والحساب اللاحق للسنة المنتهية في ٣١ كانون الاول ٢٠١٥، وجدنا بعض الملاحظات حول الحسابات وأسلوب العمل ونظام الرقابة الداخلية والتي نوردنا راجين أن تال عنايتكم ومتابعتم.

عند التخطيط والقيام بعملية التدقيق، والتي قمنا بها ضمن نطاق العمل لتدقيق حسابات صندوق التنمية للعراق والحساب اللاحق، قمنا بمراجعة وتقييم أنظمة الرقابة الداخلية لغرض تحديد إجراءات التدقيق اللازمة لغرض إبداء رأينا حول القوائم المالية وليس لتقديم ضمانات بشأن أنظمة الرقابة الداخلية، وبناءً عليه لا يمكن الاعتماد على هذا التقرير للكشف عن جميع هذه المسائل. قد لا يحدد تدقيقنا كافة نقاط الضعف داخل أنظمتكم. إن الملاحظات والتوصيات المدرجة في جدول المحتويات المرفق قد لا تكون سجلاً شاملاً لكافة نقاط الضعف التي قد تكون قائمة.

إن الهدف من إعداد هذا التقرير هو فقط لمعلومات واستخدامات لجنة الخبراء الماليين وحكومة العراق وليس الهدف من إعداده ليستخدم من قبل أي جهة أخرى بخلاف هذه الجهات المحددة. ونظراً لأن الجهات الأخرى قد تسعى إلى استخدامه لأغراض مختلفة، فإنه يجب عدم الاقتباس من هذا التقرير أو الإشارة إليه أو عرضه على أي جهة أخرى (باستثناء المستشارين المهنيين للجهة المقدم إليها هذا التقرير الذين يتصرفون بهذه الصفة شريطة ان يقبلوا بأننا لا نتحمل أي مسؤولية أو التزام من أي نوع اتجاهاً فيما يتعلق بمضمون هذا التقرير) إلا إذا تم طلب ذلك بأمر من المحكمة أو السلطة التنظيمية من دون موافقتنا الخطية المسبقة. إننا لا نتحمل أي مسؤولية من أي نوع تتعلق أو تنتج عن أو تتصل بمحتويات هذا التقرير لجهات أخرى غير الجهة المقدم إليها هذا التقرير. إذا قامت أي جهة أخرى بإختيار الاعتماد بأي شكل من الاشكال على مضمون هذا التقرير، فإنه يمكنهم القيام بذلك بشكل كامل على مسؤوليتهم الخاصة.

سيكون من دواعي سرورنا أن نقوم بمناقشة هذه التوصيات معكم وكذلك 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.

EY

وتفضلوا بقبول فائق الاحترام

إرنست ويونغ / العراق

رقم الصفحة

أ

ب

١

مفتاح الرموز

ملخص الملاحظات

الملاحظات

يحتوي هذا التقرير على الرموز التالية:

البيان	الرمز
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 عالية
تتعلق الملاحظة بالأمر متوسطة الخطورة و التي قد تؤدي إلى ضعف في نظام الرقابة الداخلي و/أو كفاءة الأنشطة التشغيلية والتي يجب أن يتم الإفصاح عنها. نوصي بإتخاذ إجراءات معالجة خلال فترة قصيرة.	درجة المخاطرة متوسطة
تتعلق الملاحظة بأمر 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.	درجة المخاطرة منخفضة

رقم الصفحة	المؤسسة	الملاحظة	درجة المخاطرة
٢	وزارة المالية/ البنك المركزي	تقنية شبكة تكنولوجيا المعلومات - أنظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية
٣	البنك المركزي	دعم خدمات نظام التشغيل - نظام السويفت	درجة المخاطرة عالية
٤	وزارة المالية/ البنك المركزي	الضوابط البيئية والمادية في غرف السيرفرات - أنظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية
٦	البنك المركزي	سرية قاعدة البيانات - نظام المدفوعات والمقبوضات	درجة المخاطرة عالية
٧	البنك المركزي	ضوابط الدخول المتزامن للنظام - نظام المدفوعات والمقبوضات	درجة المخاطرة متوسطة
٨	البنك المركزي	مشاركة حساب المستخدم - نظام المدفوعات والمقبوضات	درجة المخاطرة عالية
٩	وزارة المالية/ البنك المركزي	ضوابط كلمة السر لنظام التشغيل ويندوز - أنظمة الدينار العراقي، والدولار الامريكي، المدفوعات والمقبوضات، سويفت	درجة المخاطرة عالية
١٠	وزارة المالية	صلاحيات المرجم لتعديل البيانات - أنظمة الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية
١١	وزارة المالية	توثيق تعديلات النظام - أنظمة الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية
١٢	وزارة المالية	إجراءات طلب تعديل النظام - أنظمة الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية
١٣	وزارة المالية	الدخول إلى برامج الأنظمة - أنظمة الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية
١٤	وزارة المالية/ البنك المركزي	تحديثات نظم التشغيل - أنظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة متوسطة
١٥	وزارة المالية/ البنك المركزي	سياسات وإجراءات تقنية المعلومات - أنظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية
١٦	وزارة المالية/ البنك المركزي	الوصف الوظيفي - أنظمة الدينار العراقي، الدولار الأمريكي، والسويفت	درجة المخاطرة متوسطة
١٧	وزارة المالية/ البنك المركزي	التدقيق الداخلي لتقنية المعلومات - أنظمة الدينار العراقي، والدولار الأمريكي، والسويفت	درجة المخاطرة متوسطة
١٨	وزارة المالية/ البنك المركزي	تعديل البرامج - أنظمة الدينار العراقي، والدولار الامريكي، المدفوعات والمقبوضات	درجة المخاطرة عالية
١٩	وزارة المالية	فصل المهام - نظامي الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية
٢٠	وزارة المالية	فصل بيئات التطوير والاختبار للأنظمة - نظامي الدينار العراقي والدولار الامريكي	درجة المخاطرة عالية
٢١	وزارة المالية/ البنك المركزي	مراجعة سجلات التدقيق - أنظمة الدينار العراقي، والدولار الامريكي، المدفوعات والمقبوضات	درجة المخاطرة متوسطة
٢٢	وزارة المالية/ البنك المركزي	ضوابط كلمة السر للأنظمة - أنظمة الدينار العراقي، والدولار الامريكي، المدفوعات والمقبوضات	درجة المخاطرة عالية
٢٤	وزارة المالية/ البنك المركزي	ضوابط الخروج التلقائي - أنظمة الدينار العراقي، والدولار الامريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة متوسطة

درجة المخاطرة متوسطة	ضوابط اغلاق حساب مستخدم - أنظمة الدينار العراقي، والدولار الامريكى، والمدفوعات والمقبوضات	وزارة المالية/ البنك المركزي	٢٥
درجة المخاطرة عالية	برامج مكافحة الفيروسات - أنظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	وزارة المالية/ البنك المركزي	٢٦
درجة المخاطرة متوسطة	الشبكات المحلية و الواسعة (LAN/WAN) - أنظمة الدينار العراقي والدولار الأمريكي والسويفت	وزارة المالية/ البنك المركزي	٢٧
درجة المخاطرة عالية	إدارة النسخ الاحتياطية - أنظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	وزارة المالية/ البنك المركزي	٢٨
درجة المخاطرة عالية	واجهات أنظمة صندوق التنمية للعراق - أنظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	وزارة المالية/ البنك المركزي	٢٩
درجة المخاطرة عالية	أمنية الحواسيب - أنظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	وزارة المالية/ البنك المركزي	٣٠

الملاحظات

الملاحظة:

لقد لاحظنا أن كل الحواسيب مرتبطة بالسيرفر عن طريق تقنية شبكة مجموعة العمل (Workgroup Network Technology) بدلاً من إستخدام تقنية وحدة التحكم بالشبكة (Domain Controller Technology) للسيطرة وإدارة المستخدمين المخولين والحواسيب المرتبطة بالسيرفر من خلال بناء وتفعيل الدليل النشط (Active Directory). الإدارة قد تجد صعوبة في تطبيق السياسات الأمنية على الأجهزة المرتبطة بالشبكة، مثل سياسة كلمة المرور وسياسة تدقيق حواسيب المستخدمين بسبب إستخدام تقنية شبكة مجموعة العمل اللامركزية (Workgroup Network Technology). وعلاوة على ذلك، قد تجد الإدارة صعوبة في تتبع ومعرفة الأنشطة الغير مصرح بها وذلك لأن تقنية شبكة مجموعة العمل (Workgroup Network Technology) ليس لديها سيرفر مخصص لها لتتبع أنشطة المستخدمين وأي عمل يتم عبر جهاز المستخدم بواسطة الشبكة المحلية (LAN)، وهذا يشمل مشاركة الملفات وسجلات الدخول للمستخدمين.

التوصية:

يجب على الإدارة ضمان عدم تشغيل الحواسيب والسيرفرات في بيئة شبكة مجموعة العمل (Workgroup Network)، والعمل على تطبيق تقنية وحدة التحكم بالشبكة (Domain Controller Technology) وذلك لإدارة جميع الحواسيب السيرفرات وحسابات المستخدمين بشكل فعال.

رد الإدارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

الملاحظة:

استناداً إلى مراجعتنا لحواسيب نظام سويفت، لاحظنا أن هذه الحواسيب تعمل على نظام التشغيل ويندوز أكس بي المنتهي الصلاحية (Windows XP)، والذي هو حالياً خارج الدعم من قبل شركة مايكروسوفت ولا يتم تسويقه. لا يمكن للمؤسسة الحصول على دعم من أي موزع لمايكروسوفت في السوق في حالة حدوث مشاكل فنية في نظام التشغيل. وعلاوة على ذلك، قد تتعرض المؤسسة إلى مخاطر إستغلال الثغرات الأمنية المعروفة في الأنظمة الغير محمية بشكل كاف من خلال تحديث وتصحيح نظام التشغيل أو الأنظمة الغير محمية.

التوصية:

ينبغي على قسم تكنولوجيا المعلومات التوقف عن إستخدام تقنيات غير معتمدة أو منتهية الصلاحية تسويقياً. أيضاً، يجب على قسم تكنولوجيا المعلومات التأكد من تحديث أنظمتهم بأحدث الإصدارات.

رد الإدارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

الملاحظة:

من خلال مراجعتنا لغرف السيرفرات المخصصة لأنظمة صندوق التنمية للعراق، لاحظنا الأمور التالية:

- فيما يتعلق بنظامي الدينار العراقي والدولار الأمريكي:
 - السيرفرات موضوعة في غرف مكاتب الموظفين، حيث أن الوصول إليها متاح من قبل أي موظف أو زائر.
- فيما يتعلق بأنظمة المدفوعات والمقبوضات وسويقت:
 - لا يوجد جهاز لمراقبة الدخول الى غرفة السيرفرات.
 - لا يوجد سجل لزائري غرفة السيرفرات او لأرشفة معلومات الزوار.
 - الباب والجدران من الزجاج المضلل.
 - لا يوجد نظام للتنبيه عن وجود المياه.
 - لا يوجد جهاز لقياس درجة حرارة الغرفة ونسبة الرطوبة.

إن وجود السيرفرات على نفس المستوى من الأرض تزيد من احتمالية تعطلها في حال حدوث فيضانات أو تسريب مياه. إن عدم وجود أنظمة كشف الحرائق داخل مركز البيانات تزيد من خطورة الإصابة التي قد يتعرض لها الأفراد في الداخل وبالإضافة الى الخطورة على أجهزة الحاسوب.

قد لا تكون الإدارة قادرة على التأكد من أن طفايات الحريق ستعمل بصورة صحيحة في حال عدم اجراء فحص دوري عليها. في حال عدم وجود كاميرات متصلة في غرفة السيرفرات، فإن الإدارة لن تكون قادرة على مراقبة وتسجيل أي حركات مشبوه أو أضرار قد تحدث على موجودات غرفة السيرفرات.

في حال عدم وجود ضوابط للسيطرة على دخول الزوار إلى مركز البيانات، قد يحدث دخول غير مصرح به إلى أنظمة المؤسسة، بالإضافة إلى احتمالية حدوث عمليات احتيال وعبث في بيانات ومعلومات سرية. عدم وجود جهاز كشف تسرب المياه قد يؤدي إلى تعطل وتلف الاجهزة الموجودة في غرفة السيرفرات.

التوصية:

- ينبغي على الإدارة تعزيز الضوابط المادية والبيئية في مركز البيانات وأن تأخذ بعين الاعتبار توفير الأمور التالية:
- التأكد من أن أرضية غرفة السيرفرات مرتفعة بشكل صحيح.

- تركيب الإضاءة الاحتياطية.
- تركيب جهاز كشف الحرائق وأنظمة إخماد الحريق.
- عمل فحص دوري لطفايات الحريق.
- تركيب كاميرات مراقبة داخل غرفة السيرفرات.
- عمل سجل دخول لمركز البيانات بحيث يتم تسجيل جميع الزيارات التي تتم للمركز. وينبغي الإحتفاظ السجل ومراجعته بشكل دوري.
- تركيب جهاز تسرب المياه.
- ضمان عدم وجود أي شبائيك زجاجية في غرفة السيرفرات.
- يجب أن تكون وحدة الطاقة الاحتياطية (UPS) كافية لإعطاء الوقت اللازم لإغلاق الأجهزة بشكل سليم في حال حدوث انقطاع في التيار الكهربائي.
- التأكد من نظام التكييف الهوائي يعمل في جميع الأوقات وذلك للحفاظ على درجة حرارة مناسبة في غرفة السيرفرات.

رد الإدارة:

المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

الملاحظة:

خلال عملية مراجعتنا لمحددات قاعدة بيانات نظام المدفوعات والمقبوضات، لاحظنا بأن الـ "Database Listener" غير محمية بكلمة سر، وكذلك الرقم الأساسي الأولي الخاص بالـ "Listener Port" لم يتم تغييره، حيث أن ذلك من الممكن أن يؤدي إلى تعريض قاعدة بيانات إلى الإختراق والخطر.

التوصية:

نوصي بأن يتم حماية الـ "Database Listener" وذلك بأن يتم عليها تطبيق كلمة سر وتشفيرها وكذلك تغيير الرقم الأساسي الخاص بالـ "Listener Port".

رد الإدارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

الملاحظة:

خلال مراجعتنا لنظام المدفوعات والمقبوضات، لاحظنا أنه لا يوجد محددات للسيطرة على دخولهم الى النظام من خلال أكثر من حاسوب من قبل نفس المستخدم وفي نفس الوقت.

إن قدرة المستخدم على الدخول الى النظام من خلال أكثر من حاسوب وفي نفس الوقت من الممكن أن يزيد من خطورة مشاركة استخدام اسم المستخدم والذي يؤدي إلى تعريض سلامة البيانات وسريتها الى الخطر.

التوصية:

على الإدارة منع مشاركة اسم المستخدم من قبل المستخدمين وكذلك منع فتح النظام بنفس اسم المستخدم من خلال أكثر من حاسوب في نفس الوقت إلا في الحالات الضرورية التي يفرضها العمل.

رد الإدارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

الملاحظة:

من خلال مراجعتنا لنظام المدفوعات والمقبوضات، لاحظنا وجود بعض المستخدمين الذين يتشاركون بنفس اسم المستخدم وكلمة السر للدخول للعمل على النظام. بدون وجود مسؤولية وملكية واضحة لحساب كل مستخدم للنظام فقد تجد الإدارة صعوبة في مساءلة المستخدمين الغير مصرح لهم بالدخول.

التوصية:

من أجل إقامة المساءلة، ينبغي للإدارة إنشاء حسابات منفصلة لكل موظف بحاجة لإستخدام النظام.

رد الإدارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

الملاحظة:

من خلال مراجعتنا لأنظمة التشغيل ويندوز والخاصة بالحواسيب المتعلقة بأنظمة صندوق التنمية للعراق، لاحظنا الأمور التالية فيما يتعلق بضوابط كلمة السر:

- خيار إجبار المستخدم على تغيير كلمة السر خلال الدخول الأول غير مفعّل.
- خيار إجبار المستخدم على تغيير كلمة السر بشكل دوري غير مفعّل.
- كلمة السر غير معقدة.
- لم يتم تحديد الحد الأدنى لطول كلمة السر.
- خيار الاحتفاظ بأرشفة كلمات السر لمنع تكرار استخدام كلمة السر غير مفعّل.
- لم يتم تحديد الحد الأدنى لعمر كلمة السر.
- عدم توقيف الحساب الذي يقوم بعدد من المحاولات الفاشلة للدخول.

التوصية:

- يجب أن تسعى الإدارة إلى التعاون مع مزودي الأنظمة على تنفيذ ما يلي:
- إجبار المستخدمين على تغيير كلمات السر الأساسية عند دخولهم الأول إلى 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 استخدام نفس الكلمات السابقة.
 - إقفال الحساب بعد محدد من المحاولات الفاشلة للدخول (على سبيل المثال ٣ محاولات).
 - بالإضافة إلى ذلك يجب أن يتم لفت انتباه الموظفين من خلال برامج توجيهية أمنية إلى الحاجة إلى تغيير كلمات السر بشكل فوري في حال أصبحت معروفة من قبل الآخرين.

رد الإدارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الإجراءات اللازمة لحلها خلال السنة 2015.

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 الإدارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال سنة 2015.

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 2015.

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 شفوية. 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 إنجازها والعمل على متابعتها. إن عملية التوثيق تتطلب اهتماماً كافياً لما لها من أهمية في إثبات عمليات طلبات التعديل والموافقات المتعلقة بها.

رد الإدارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

الملاحظة:

لاحظنا من خلال مراجعتنا أن مبرمجي الأنظمة لهم السيطرة الكاملة على برامج نظامي الدينار العراقي والدولار الأمريكي 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 الإدارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

درجة المخاطرة متوسطة

١٢. تحديثات نظم التشغيل - أنظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويقت

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 الإدارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

الملاحظة:

من خلال مراجعتنا، لاحظنا عدم وجود دليل سياسات وإجراءات موثقة 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 ما يلي:

- 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 الموضوعية.

رد الإدارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

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 بما هو متوقع منه أو المخاطر الناتجة من كونهم ليسو ملائمين للأعمال المناطة بهم، حيث أن ذلك يؤدي الى عدم كفاءتهم في تنفيذ المهام.

التوصية:

على الإدارة الأخذ بعين الإعتبار تطوير دليل توصيف للوظائف خاص بدائرة تقنية المعلومات بحيث يشمل 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 2015.

١٥. التدقيق الداخلي لتقنية المعلومات – انظمة الدينار العراقي، والدولار الأمريكي والسويقت | درجة المخاطرة متوسطة

الملاحظة:

من خلال مراجعتنا، لاحظنا بأنه لا يوجد 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 2015.

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. بالإضافة 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. بالإضافة الى ذلك، ينبغي لقسم تكنولوجيا المعلومات أن يأخذ بنظر الاعتبار وضع آلية يتم اتباعها في تسمية متغيرات البرامج وكذلك لعمل إصدارات للبرامج والأنظمة.

رد الإدارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

الملاحظة:

من خلال مراجعتنا لاحظنا أن نفس الشخص الذي يدير قاعدة بيانات ونظام التشغيل هو / هي نفس الشخص الذي يقوم بعمل وتطوير 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 2015.

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 2015.

درجة المخاطرة متوسطة

١٩. مراجعة سجلات التدقيق - أنظمة الدينار العراقي، والدولار الامريكي، المدفوعات والمقبوضات

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 الإدارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

الملاحظة:

من خلال مراجعتنا لأنظمة الدينار العراقي والدولار الأمريكي 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.
- لا يتم الاحتفاظ بأرشفة كلمة السر.
- ليس هناك تحديد أدنى لطول كلمات السر.

ولاحظنا كذلك ان المستخدم لا يرغم على تحديث كلمة السر خلال فترة معينة في نظام المدفوعات والمقبوضات.

بمرور الزمن، اذا لم يتم تغيير كلمات السر من فترة لأخرى يؤدي ذلك الى فقدانها لفعاليتها 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 الأساسية 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 استخدام 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 2015.

درجة المخاطرة متوسطة

٢١. ضوابط الخروج التلقائي - أنظمة الدينار العراقي، والدولار الامريكى، والمدفوعات والمقبوضات، والسويقت

الملاحظة:

من خلال مراجعتنا للأنظمة صندوق التنمية للعراق، لاحظنا عدم وجود ضوابط للخروج التلقائي من الأنظمة في حال تركها من دون استخدام فترة 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 اثناء 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 2015.

درجة المخاطرة متوسطة

٢٢. ضوابط اغلاق حساب مستخدم – أنظمة الدينار العراقي، والدولار الامريكي، والمدفوعات والمقبوضات

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 الخاطيء لكلمة السر (٣ مرات مثلاً).

رد الادارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

درجة المخاطرة عالية

٢٣. برامج مكافحة الفيروسات - أنظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويقت

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 السويقت 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 والحوادم 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 2015.

درجة المخاطرة متوسطة

٢٤. الشبكات المحلية و الواسعة (LAN/WAN) - انظمة الدينار العراقي والدولار الأمريكي والسويقت

الملاحظة:

من خلال مراجعتنا لأنظمة الدينار العراقي والدولار الأمريكي والسويقت، 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 بسرقة 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 الإدارة:المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

الملاحظة:

- عند فحص الضوابط التي تحيط بعملية إجراء النسخ الاحتياطية من الأنظمة الخاصة بصندوق التنمية للعراق، لاحظنا ما يلي:
- لا يوجد إجراء رسمي موثق يتم إتباعه للقيام بعملية إجراء 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 وأمنية معتمدة من قبل الإدارة، وعضوا عن ذلك يتم حفظها على ذاكرات فلاش بحيث تبقى مع مستخدمي الأنظمة.
 - فيما يخص نظام سويقت، 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 تشمل 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 2015.

درجة المخاطرة عالية

٢٦. واجهات أنظمة صندوق التنمية للعراق - أنظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويقت

الملاحظة:

من خلال مراجعتنا لأنظمة صندوق التنمية للعراق، لاحظنا عدم وجود وجهات تقوم بربط أنظمة الدينار العراقي والدولار الامريكي والمدفوعات والمقبوضات وسويقت 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 الإدارة:

المتابعة:

مازالت الملاحظة قائمة. لم يتم اتخاذ الاجراءات اللازمة لحلها خلال السنة 2015.

الملاحظة:

من خلال مراجعتنا للربط المباشر لحواسيب المستخدمين، لاحظنا ان مخارج ال (USB) متاحة وفعالة في اغلب حواسيب المستخدمين لأنظمة الدينار العراقي والدولار الامريكى، 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 2015.

إرنست ويونغ
خدمات التدقيق والضرائب والمعاملات والاستشارات

عن إرنست ويونغ
تعتبر إرنست ويونغ إحدى المؤسسات الرائدة على مستوى العالم في مجالات التدقيق والضرائب والمعاملات والاستشارات، حيث تضم إرنست ويونغ عدد كبير من الموظفين يصل إلى ٢٣٠,٠٠٠ 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 إلى العملاء. لمزيد من المعلومات عن مؤسستنا يرجى زيارة موقعنا الإلكتروني: www.ey.com. تعود أعمال إرنست ويونغ في الشرق الأوسط إلى عام ١٩٢٣. على امتداد أكثر من ٩٠ سنة، نمت مؤسستنا وتطورت لتلبية الاحتياجات والتطورات القانونية والتجارية في المنطقة. لدينا عبر الشرق الأوسط أكثر من ٥,٠٠٠ فرد يتعاونون معاً من خلال ٢٠ مكتباً في ١٥ دولة عربية، يتقاسمون ذات القيم والالتزام الشديد بالجودة. نحن نحدث الفارق من خلال مساعدة فريقنا وعلماؤنا ومجتمعاتنا في تحقيق وتوظيف إمكاناتهم.

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

هكذا نحدث الفرق في إرنست ويونغ

© 2016 إرنست ويونغ
جميع الحقوق محفوظة

