دليل تدقيق تكنولوجيا المعلومات لأجهزة الرقابة العليا

- مجموعة عمل الإنتوساي لتدقيق تكنولوجيا المعلومات (WGITA) ومبادرة الإنتوساي للتنمية (IDI)

INTOSAI

IDI

DEVELOPMENT INITIATIVE

هذا الدليل تم نشره في فبراير 2014

وتم ترجمته من قبل ديوان المحاسبة الكويتي الى اللغة العربية في أغسطس 2014

دليل تدقيق تكنولوجيا المعلومات لأجهزة الرقابة العليا

WGITA – IDI HANDBOOK ON IT AUDIT FOR SUPREME AUDIT INSTITUTIONS

INTOSAI DEVELOPMENT INITIATIVE

تمهيـــــــــــد

أصبحت عملية تدقيق تكنولوجيا المعلومات (IT) أحد الموضوعات الرئيسية لعمليات التدقيق التي تجريها أجهزة الرقابة العليا (SAIs) في جميع أنحاء العالم. وتعتبر هذه استجابة طبيعية على عمليات الحوسبة المتزايدة في الجهات الحكومية والقطاع العام، يجب ان تكون أنظمة تكنولوجيا المعلومات المستخدمة قادرة على حماية المعلومات والأصول في الجهة وتدعم رسالتها وأهدافها المالية وأهدافها الأخرى. في حين أن الاستخدام المتزايد لتكنولوجيا المعلومات قد أدى إلى تحسين من فعالية وكفاءة الأعمال والخدمات التي يتم تقديمها، إلا أنها جلبت معها أيضاً مخاطر ونقاط ضعف مرتبطة مع قواعد البيانات وتطبيقات الأعمال التي تحدد بيئة العمل الآلية. يعتبر دور تدقيق تكنولوجيا المعلومات في ضمان أنه يتم إجراء العمليات المناسبة لإدارة المخاطر ونقاط الضعف ذات الصلة بتكنولوجيا المعلومات أمراً بالغ الأهمية في حال إعداد جهاز الرقابة الأعلى لتقرير هادف حول فعالية وكفاءة أعمال الحكومة والقطاع العام. في بيئة تدقيق تكنولوجيا المعلومات، يشار إلى العمليات، والأدوات، والرقابة، والطرق الأخرى لإدارة الوظائف بالضوابط.

وقد عملت كل من مجموعة عمل الإنتوساي المعنية بتدقيق تكنولوجيا المعلومات (WGITA) ومبادرة الإنتوساي للتنمية (IDI) على إصدار دليل حديث حول تدقيق تكنولوجيا المعلومات بهدف تزويد مدققي أجهزة الرقابة العليا بمعايير وممارسات معترف بها عالمياً للتدقيق على تكنولوجيا المعلومات. يتضمن هذا الدليل شرحاً شاملاً للمجالات الرئيسية التي يحتاج مدقق تكنولوجيا المعلومات إلى الاطلاع عليها عند ممارسة التدقيق.

يتبع دليل مجموعة عمل الإنتوساي المعنية بتدقيق تكنولوجيا المعلومات ومبادرة الإنتوساي للتنمية المبادئ العامة للتدقيق على النحو المنصوص عليه بموجب المعايير الدولية لأجهزة الرقابة العليا(ISSAI)*. كما أن الدليل قد أخذ أيضاً من أطر عمل تكنولوجيا المعلومات المعترف بها دولياً، مشتملا على إطار جمعية التدقيق والرقابة على نظم المعلومات (ISACA) المسمى (COBIT)، ومعايير منظمة المعايير الدولية(ISO) ، وإرشادات وأدلة تكنولوجيا المعلومات من بعض أجهزة الرقابة العليا، وذلك في محاولة لتزويد مدققي تكنولوجيا المعلومات بمجموعة كاملة من الإرشادات حول تدقيق تكنولوجيا المعلومات.

الهدف الرئيسي من هذا الدليل هو تزويد المستخدمين بالمعلومات والأسئلة الأساسية اللازمة للتخطيط الفعال لتدقيق تكنولوجيا المعلومات، ونأمل بأن يعود هذا الدليل بالفائدة على أجهزة الرقابة العليا بحيث يصبح مرجعا شاملا ودليل إرشاد عملي لإجراء عمليات تدقيق تكنولوجيا المعلومات.

وقد تم إدارة هذا المشروع بشكل مشترك من قبل رئيس مجموعة عمل الإنتوساي المعنية بتدقيق تكنولوجيا المعلومات (WGITA) وهو جهاز الرقابة الأعلى الهندي، ومبادرة الإنتوساي للتنمية (IDI) وقامت أجهزة الرقابة العليا الأعضاء في مجموعة عمل الإنتوساي وهي الأجهزة التابعة لكل من البرازيل واندونيسيا والهند وبولندا والولايات المتحدة الأمريكية بالعمل معاً على تطوير هذا الدليل، ترغب كل من مجموعة عمل الإنتوساي المعنية بتدقيق تكنولوجيا المعلومات (WGITA) ومبادرة الإنتوساي للتنمية (IDI) أن تتقدم بالشكر بشكل خاص إلى أفراد الفريق الذين عملوا بلا كلل في تطوير هذا الدليل، والشكر موصول أيضاً إلى أجهزة الرقابة العليا التي قدمت ملاحظاتها وتعليقاتها القيمة على الدليل.

شاشي كانت شارما	إينار ج. غوريسين
المراقب والمراجع العام للهند	المدير العام
رئيس مجموعة عمل الإنتوساي المعنية	مبادرة الإنتوساي للتنمية
بتدقيق تكنولوجيا المعلومات	

* www.issai.org

أعضاء فريق المشروع

1. **السيد/ مادهاف اس بانوار**

موظف تقني على مستوى متقدم (مدير)، مكتب مساءلة حكومة الولايات المتحدة الأمريكية.

2. **السيد/ باول باناس**

مستشار رئيس مكتب الجهاز الرقابي البولندي (NIK)، مكتب الجهاز الرقابي البولندي.

3. **السيد/ نيلش كومار ساه**

المحاسب العام، مكتب المراقب والمراجع العام للهند.

4. **السيد/أنينديا داسجوبتا**

مدير، مكتب المراقب والمراجع العام للهند.

5. **السيد/ماركو رودريجو براز**

مدقق، المحكمة البرازيلية للتدقيق.

6. **السيدة/شيفالي اس انداليب**

مساعد المدير العام، مبادرة الإنتوساي للتنمية (IDI).

7. **السيد/نوفس برامانتيا بودي**

نائب المدير، مجلس التدقيق في جمهورية إندونيسيا.

8. **السيدة/ريا انوجرياني**

نائب المدير، مجلس التدقيق في جمهورية إندونيسيا.

قائمة الاختصارات

BCP	Business Continuity Plan/ Business Continuity Planning	خطة استمرارية العمل
BIA	Business Impact Assessment	تقييم التأثير على العمل
CAATs	Computer Assisted Audit Techniques	تقنيات التدقيق بمساعدة الحاسوب
COBIT	Control Objectives for Information and related Technology	أهداف الرقابة على المعلومات والتكنولوجيا ذات الصلة
CMMI	Capability Maturity Model Integration	لتكامل نموذج نضوج المقدرة
CM	Configuration management	إدارة الاعداد
CVV	Card Verification Value	رقم التحقق من البطاقة
DRP	Disaster Recovery Plan/ Disaster Recovery Planning	خطة استعادة الأوضاع بعد الكوارث
EUROSAI	European Organization of Supreme Audit Institutions	المنظمة الأوروبية للأجهزة العليا للرقابة
EDP	Electronic Data Processing	معالجة البيانات الإلكترونية
ERP	Enterprise resource planning	التخطيط لموارد الجهة
GAO	Government Accountability Office, United States of America (USA)	جهاز الرقابة لحكومة الولايات المتحدة الأمريكية (USA)
GRC	governance, risk, and compliance	الإطار العام لحوكمة المخاطر
ISACA	Information Systems Audit and Control Association	جمعية الرقابة وتدقيق نظم المعلومات
IS	Information System	نظم المعلومات
ISSAI	International Standards for Supreme Audit Institutions, sometimes, especially in older documents referred also as INTOSAI Standards	المعايير الدولية للأجهزة العليا للرقابة، في بعض الأحيان، خصوصا في الوثائق القديمة كانت تسمى معايير الإنتوساي
ISP	Information Security Policy	سياسة أمن المعلومات
IT	Information Technology	تكنولوجيا المعلومات
ITIL	Information Technology Infrastructure Library	مكتبة البنية التحتية لتكنولوجيا المعلومات
IDI	INTOSAI Development Initiative	مبادرة الإنتوساي للتنمية
KPIs	key performance indicator	مؤشرات أداء القياس

NIST	National Institute of Standards and Technology, US Department of Commerce	المعهد الوطني للمعايير والتكنولوجيا، وزارة التجارة الأمريكية
RPO	Recovery Point Objective	هدف مرحلة استعادة الأوضاع بعد الكوارث
RTO	Recovery Time Objective	هدف الوقت المستغرق لاستعادة الأوضاع بعد الكوارث
SLA	Service Level Agreement	اتفاقية مستوى الخدمة
SAIs	Supreme Audit Institutions	أجهزة الرقابة العليا
SRS	System Requirement Specifications	وثيقة مواصفات متطلبات النظام
SDLC	systems development life cycle	دورة حياة تطوير البرمجيات
URS	User Requirement Specifications	وثيقة مواصفات متطلبات المستخدم
UPS	uninterruptible power supply	إمدادات الطاقة غير المنقطعة
Wi-Fi	Wireless Fidelity	أمن الشبكة اللاسلكية
WGITA	Working Group on IT Audit	مجموعة عمل الإنتوساي المعنية بتدقيق تكنولوجيا المعلومات

قائمة المحتويات

المقدمـــــــــــــة

ساهم ظهور تقنية المعلومات في تغيير الطريقة التي نعمل بها جميعنا في العديد من المجالات، ويتضح هذا التغيير في مهنة التدقيق دون استثناء. فقد أصبح الحاسوب مستخدما في كل مكان تقريباً، حيث إنه وبلا شك أحد أكثر أدوات العمل فعالية، إلا أن ذلك صاحبه ظهور نقاط ضعف ذات علاقة وثيقة ببيئة الأعمال الآلية. حيث يجب أن يتم تحديد كل نقطة من نقاط الضعف الجديدة وتقليل أثرها والتحكم بها من خلال تقييم مدى دقة كل العمليات الرقابية باستخدام أساليب تدقيق جديدة[1].

لقد تطور استخدام أجهزة الكمبيوتر من كونها مجرد نظم لمعالجة البيانات لتصل إلى وضعها الحالي حيث تجمع وتخزن وتسهل الوصول إلى كم هائل من البيانات. ويتم استخدام هذه البيانات في عملية صنع القرار، وإدارة الأعمال الأساسية في الجهات. حاليا، تتواصل أجهزة الكمبيوتر مع بعضها البعض ويتم تبادل البيانات عبر شبكات الحاسوب – على المستويين العام والخاص على حد سواء.

في الواقع، مع ظهور ونمو أنظمة شبكات الكمبيوتر، أصبحت معها الآن نظم الحاسوب أكثر فعالية. وانعكاساً لهذا التطور، تم استبدال مصطلح " معالجة البيانات الإلكترونية – EDP" بمصطلحات أخرى مثل "تدقيق تكنولوجيا المعلومات" و"تدقيق نظم المعلومات".

مع زيادة الاستثمار في النظم الحاسوبية والاعتماد عليها من قبل الجهات الخاضعة للتدقيق، أصبح لزاماً على مدقق تكنولوجيا المعلومات اعتماد طرق ومنهجيات مناسبة حتى يمكن لعملية التدقيق أن تحدد وبشكل مؤكد المخاطر التي تواجه سلامة البيانات والخصوصية وسوء الاستخدام، وكذلك لضمان وجود الضوابط الخاصة

[1] دليل تدقيق تكنولوجيا المعلومات، المجلد الأول، مراجع ومراقب عام الهند

بتقليل أثر هذه المخاطر في مكانها الصحيح، في نظام تكنولوجيا المعلومات الاعتيادي، وبخاصة عندما يتم التنفيذ في بيئة لا تتوفر فيها الضوابط الكافية، تواجه الجهة الخاضعة للتدقيق العديد من المخاطر التي يجب على المدقق أن يقوم بالتعرف عليها وتحديدها، وحتى عندما تكون الجهة الخاضعة للتدقيق قد اتخذت بعض التدابير للحد من المخاطر، فيجب القيام بعملية تدقيق مستقلة لضمان وضع وتنفيذ ضوابط كافية (ضوابط عامة للكمبيوتر[2] وضوابط التطبيق[3]) لتقليل التعرض لمختلف المخاطر.

محتوى وهيكل الدليل

يهدف هذا الدليل إلى تزويد مدققي تكنولوجيا المعلومات بإرشادات تصف مختلف مجالات تدقيق تكنولوجيا المعلومات، وكذلك الإرشاد حول كيفية التخطيط لعمليات التدقيق بنحو فعال.

في الفصل الأول من هذا الدليل، سوف يجد القراء لمحة عامة حول تعريف تدقيق تكنولوجيا المعلومات، والتفويضات الممنوحة لأجهزة الرقابة العليا، ونطاق وأهداف تدقيق تكنولوجيا المعلومات، كما يوضح ماهية الضوابط العامة لتكنولوجيا المعلومات وضوابط التطبيقات والعلاقة التي تربط فيما بينهم، وقد تم تناول مجالات هذه الضوابط بمزيد التفصيل في الفصول اللاحقة، ويصف الفصل الأول أيضاً عملية تدقيق تكنولوجيا المعلومات ومنهجية التقييم على أساس المخاطر لاختيار عمليات تدقيق تكنولوجيا المعلومات، تم وضع القائمة الشاملة لتقييم المخاطر في الملحق الأول. يعتبر وصف عملية تدقيق تكنولوجيا المعلومات وصفاً شاملاً، وذلك وفق أساليب التدقيق المعيارية المطبقة في التدقيق النموذجي لتكنولوجيا المعلومات، يجب على مستخدمي الدليل الرجوع إلى الأدلة والإرشادات التوجيهية لإجراءات التدقيق في أجهزة الرقابة العليا التي يعملون بها للتخطيط والقيام بعمليات تدقيق محددة.

---

[2] لا تقتصر الضوابط العامة لنظم المعلومات على تطبيقات معينة أو معاملات فردية بل هي ضوابط على عمليات المعالجة في بيئة تكنولوجيا المعلومات والتي تدعم تطوير وتنفيذ وتشغيل نظام تكنولوجيا المعلومات، وعادة ما تتعلق بضوابط حوكمة وتنظيم وهيكل تكنولوجيا المعلومات، والضوابط البيئية والمادية، وعمليات تكنولوجيا المعلومات، وأمن نظم المعلومات، واستمرارية الأعمال.

[3] ضوابط التطبيق هي ضوابط خاصة لنظام تكنولوجيا المعلومات، وتشمل تطبيق قواعد العمل في البرنامج وبالتالي توفير الضوابط للمدخلات وعملية المعالجة والمخرجات والبيانات الرئيسية.

تتناول الفصول من الثاني إلى الثامن وصفاً مفصلاً لمجالات تكنولوجيا المعلومات المختلفة التي من شأنها أن تساعد مدققي تكنولوجيا المعلومات في تحديد المجالات المحتملة القابلة للتدقيق، وقد تم إدراج مخاطر المستوى التنظيمي المتعلقة بمجال تكنولوجيا المعلومات في نهاية كل فصل، والتي سوف تساعد مدققي تكنولوجيا المعلومات في تحديد مجالات المخاطر العالية القابلة للتدقيق، وسوف تساعد التوجيهات المقدمة في كل مجال مدققي تكنولوجيا المعلومات في التخطيط لعمليات التدقيق، وذلك إما في مجال معين أو في مجموعة من المجالات بناءً على نطاق عملية تدقيق تكنولوجيا المعلومات التي تم التخطيط لها والهدف منها (تدقيق مالي أو تدقيق أداء)، على سبيل المثال، يمكن استخدام الارشادات لتدقيق حوكمة تكنولوجيا المعلومات في التخطيط لعملية التدقيق على آلية حوكمة تكنولوجيا المعلومات في الجهة، أو في التخطيط للتدقيق على بيئة الضوابط العامة والتي تعتبر حوكمة تكنولوجيا المعلومات جزءاً مهماً منها.

تم تزويد كل فصل بإرشادات تشرح خطوة بخطوة طريقة إعداد مصفوفة التدقيق المنصوص عليها في الملاحق من الثاني إلى الثامن، تشتمل مصفوفة التدقيق على موضوعات التدقيق، والمعايير، والمعلومات المطلوبة، وطرق التحليل، يجب على المستخدمين ملاحظة أن الموضوعات المتعلقة بالتدقيق والمدرجة في المصفوفات هي عامة وليست شاملة، ويفضل أن يقوم المستخدمون بإعداد المصفوفات وفق المتطلبات المحددة لعمليات التدقيق الخاصة بهم، يعتبر نموذج المصفوفة نموذجاً عاماً يمكن أن تستخدمه أجهزة الرقابة العليا كأوراق عمل، أو أن يتم تعديله وفقاً لمعايير أجهزة الرقابة العليا.

بالإضافة إلى ذلك، يتضمن هذا الدليل لمحة عامة حول الأمور المستجدة في تدقيق تكنولوجيا المعلومات. ويتناول الفصل التاسع بعض المجالات التي قد تهم مدققي تكنولوجيا المعلومات، مثل المواقع الالكترونية، والبوابات، والحوكمة الإلكترونية، وعمليات التدقيق القضائي القائمة على أساس الكمبيوتر، والحوسبة المتنقلة. كما يحتوي هذا الفصل قائمة إرشادية لمجالات التدقيق ويقدم المراجع للاطلاع الاضافي للمستخدمين المهتمين.

تعتبر الإرشادات الفنية حول استخدام تقنيات التدقيق باستخدام الكمبيوتر (CAATS) خارج نطاق هذا الدليل، ويفضل أن تقوم أجهزة الرقابة العليا بتدريب موظفيها على استخدام هذه التقنيات، كما وقد تأخذ في الاعتبار ترشيح موظفيها لبرنامج مبادرة الإنتوساي للتنمية (IDI) لتدقيق تكنولوجيا المعلومات.

لمزيد من المعلومات حول البرامج التدريبية المستقبلية، يرجى زيارة المواقع الالكترونية لكل من مجموعة عمل الإنتوساي المعنية بتدقيق تكنولوجيا المعلومات (WGITA) ومبادرة الإنتوساي للتنمية (IDI).

WGITA: http://www.intosaiitaudit.org

IDI: http://www.idi.no

نأمل أن تجد أجهزة الرقابة العليا وموظفيها في مجال تدقيق تكنولوجيا المعلومات هذا الدليل أداة مفيدة في تعزيز معرفتهم وفهمهم لموضوعات تدقيق تكنولوجيا المعلومات، وأنها سوف تساعدهم في تخطيط وإجراء عمليات تدقيق تكنولوجيا المعلومات.

الفصل الأول

تدقيق تكنولوجيا المعلومات

المقدمة

في ضوء الفرص المتاحة للتحول للنظم المعلوماتية في جميع أنحاء العالم، أصبحت الجهات تتوسع في ميكنة أنشطتها وإدارة المعلومات، وأصبح المدققين أكثر اطمئنانا لهذه الآليات والمعلومات التي تتوفر من خلالها للتوصل إلى ملاحظات صحيحة.

يقدم هذا الفصل لمحة عامة عن عملية تدقيق تكنولوجيا المعلومات، ويمكن اعتباره مقدمة وملخص للفصول من الثاني إلى الثامن، وبذلك يختلف هذا الفصل عن جميع الفصول الأخرى من حيث التصميم والمحتوى، لم يتم توثيق عملية تدقيق تكنولوجيا المعلومات المبينة في هذا الفصل في المعايير الدولية، ولكنها تعكس منهجية التدقيق في المعايير الدولية وممارسات التدقيق المقبولة التي تتبعها وتطبقها أجهزة الرقابة العليا (ISSAIs).

I. ما هو تدقيق تكنولوجيا المعلومات

إن التدقيق على تكنولوجيا المعلومات يضمن أن تحقق عمليات تطوير وتطبيق وصيانة أنظمة تكنولوجيا المعلومات أهداف العمل، ويحمي أصول المعلومات ويحافظ على نزاهة البيانات، وبعبارة أخرى، فإن التدقيق على تكنولوجيا المعلومات يعتبر اختبارا لكيفية تنفيذ نظم تكنولوجيا المعلومات والضوابط المطبقة عليها لضمان تلبية هذه النظم لاحتياجات العمل في الجهة دون المساس بالأمن، والخصوصية، والتكلفة، وغيرها من محاور العمل الهامة.

I.1 التفويض لعمليات تدقيق تكنولوجيا المعلومات

إن التفويض الممنوح لجهاز الرقابة الأعلى لإجراء تدقيق لنظم تكنولوجيا المعلومات موجود ضمن المعايير الدولية لأجهزة الرقابة العليا ISSAI في إعلان ليما[4]. حيث ان التفويض الممنوح لجهاز الرقابة الأعلى لتدقيق تكنولوجيا المعلومات مستمد من التفويض العام الممنوح لجهاز الرقابة الأعلى للقيام بالتدقيق المالي، وتدقيق الالتزام، وتدقيق الأداء أو المزج فيما بينهم[5]، وقد يكون لبعض أجهزة الرقابة العليا تفويضات محددة للقيام بتدقيق تكنولوجيا المعلومات، على سبيل المثال، في حال حصول جهاز الرقابة الأعلى على تفويض بالتدقيق على عملية الإيرادات الضريبية، فيجب عليه تدقيق الجزء الآلي من هذه العملية بناء على تفويض يستمد من التفويض الأصلي.

I.2 أهداف تدقيق تكنولوجيا المعلومات

إن الهدف من عمليات تدقيق تكنولوجيا المعلومات هو التأكيد على أن موارد تكنولوجيا المعلومات تؤدي إلى تحقيق الأهداف التنظيمية بفعالية واستخدام الموارد بكفاءة، وقد يشمل تدقيق تكنولوجيا المعلومات أنظمة تخطيط موارد المؤسسات، وأمن 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 وأمنه، على سبيل المثال، نظم الحجز في السكك الحديدية.
- فحص عملية تطوير النظام والإجراءات.

---

[4] INTOSAI Lima Declaration, Part VII Section 22

[5] ISSAI 100 Fundamental Principles of Public Sector Auditing

I.3 مجال تدقيق تكنولوجيا المعلومات

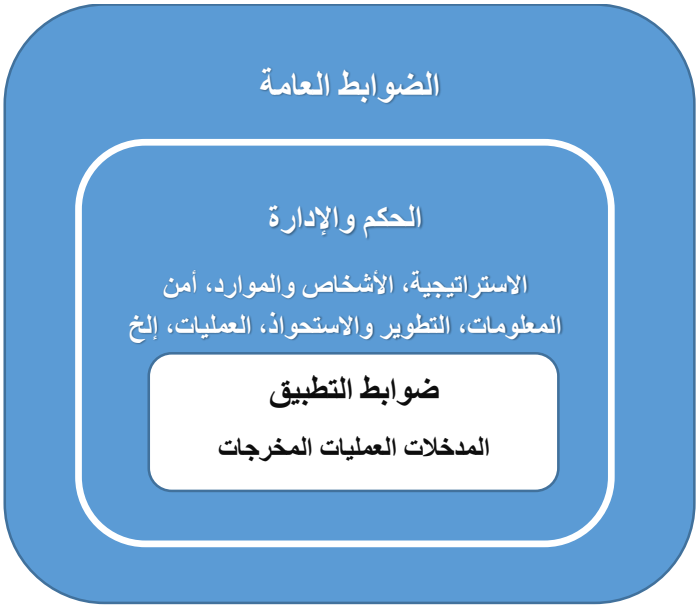
عادة ما تقوم أجهزة الرقابة العليا (SAIs) بعمليات التدقيق على تكنولوجيا المعلومات مقترنةً مع التدقيق على البيانات المالية، ومراجعة الضوابط الداخلية، وعمليات تدقيق الأداء لنظم وتطبيقات تكنولوجيا المعلومات، بتعبير آخر، فإن عمليات تدقيق تكنولوجيا المعلومات تغلغلت في عمليات التدقيق المالي (لتقييم صحة البيانات المالية للجهة)؛ وفي تدقيق الالتزام والتدقيق التشغيلي (تقييم الضوابط الداخلية)؛ وفي تدقيق الأداء (بما في ذلك مواضيع نظم المعلومات)؛ وفي عمليات التدقيق المتخصصة (تقييم الخدمات المقدمة من خلال طرف ثالث كالاستعانة بمصادر خارجية)؛ وفي التدقيق القضائي والتدقيق على مشاريع تطوير نظم المعلومات (IS)[6].

بغض النظر عن نوع التدقيق، يجب على مدقق تكنولوجيا المعلومات أن يقوم بتقييم السياسات المطبقة والإجراءات المتبعة في بيئة تكنولوجيا المعلومات بصورة شاملة في الجهة الخاضعة للتدقيق، وذلك للتأكيد على وجود الضوابط والآليات المناسبة في الموضع الصحيح، ويحدد نطاق التدقيق مدى دقة الفحص، ونظم المعلومات التي سيتم تغطيتها وأي وظائف منها، وعمليات تكنولوجيا المعلومات التي ستخضع للتدقيق، ومواقع نظم تكنولوجيا المعلومات[7] والفترة الزمنية التي سيتم تغطيتها، أي أنه شيء أساسي أن يتم تحديد مجال التدقيق.

[6] طالع قاعدة بيانات اليوروساي في مجال تقارير التدقيق على نظم المعلومات لأنواع التدقيق المختلفة – http://egov.nik.gov.pl/

[7] يشمل الموقع أماكن تواجد الخوادم، المستخدمين، والشبكات، سواء كانت موزعة على مباني، أو مدن أو حتى دول مختلفة.

I.4 ضوابط تكنولوجيا المعلومات



الضوابط هي مزيج من الأساليب والسياسات والإجراءات التي تكفل حماية أصول الجهة، ودقة وموثوقية سجلاتها، والالتزام التشغيلي بمعايير الإدارة.

تنقسم ضوابط تكنولوجيا المعلومات إلى قسمين: الضوابط العامة وضوابط التطبيق، وتعتمد نوعية هذه الضوابط على مدى تأثيرها وهل هي مرتبطة بأي تطبيق محدد.

تعتبر الضوابط العامة أساس ضوابط تكنولوجيا المعلومات، وهي المعنية بالبيئة العامة التي يتم فيها تطوير نظم تكنولوجيا المعلومات وتشغيلها وإدارتها وصيانتها، تضع الضوابط العامة لتكنولوجيا المعلومات إطار عمل للرقابة الشاملة على أنشطة تكنولوجيا المعلومات وتقدم الضمان بتحقيق مستوى مرضي من أهداف الرقابة.

يتم تطبيق الضوابط العامة باستخدام عدد من الأدوات كالسياسات والإجراءات والتوجيه وكذلك بوضع هيكل إداري ملائم، بما في ذلك هيكل إدارة نظم تكنولوجيا المعلومات في الجهة، وتشمل الأمثلة على الضوابط العامة تطوير وتنفيذ استراتيجية نظم المعلومات، والسياسة الأمنية لنظم المعلومات، وتشكيل لجنة توجيهية لتكنولوجيا المعلومات، وتنظيم موظفي نظم المعلومات لفصل المهام المتعارضة، والتخطيط للوقاية من الكوارث واستعادة الاوضاع.

ضوابط التطبيق هي ضوابط معينة تختلف باختلاف التطبيق، ولها علاقة بالمعاملات والبيانات الموجودة، وتشمل ضوابط التطبيق التحقق من صحة إدخال البيانات، تشفير البيانات المراد إرسالها، وضوابط المعالجة، الخ، على سبيل المثال، من ضوابط المدخلات في تطبيق الدفع عبر الإنترنت، أن يكون تاريخ انتهاء بطاقة الائتمان أكبر من تاريخ المعاملة، وأن يتم تشفير المعلومات التي تم إدخالها.

I.5 الضوابط العامة لتكنولوجيا المعلومات وضوابط التطبيق والعلاقة فيما بينهما

الضوابط العامة لتكنولوجيا المعلومات ليست محددة لمعاملات أو سلسلة إجراءات محاسبية معينة أو للتطبيقات المالية، إنما الهدف من الضوابط العامة لتكنولوجيا المعلومات هو ضمان تطوير وتنفيذ التطبيقات والبرامج بشكل صحيح، وكذلك صحة ملفات البيانات وعمليات الكمبيوتر[8].

إن طريقة تصميم الضوابط العامة لتكنولوجيا المعلومات وطريقة تطبيقها لهما تأثير كبير على فعالية ضوابط التطبيق، تزود الضوابط العامة التطبيقات بالموارد التي تحتاجها للتشغيل وضمان عدم حدوث أي تغييرات غير مصرح بها على التطبيقات أو على قواعد البيانات الأساسية.

فيما يلي أكثر الضوابط العامة لتكنولوجيا المعلومات شيوعاً والتي تعزز ضوابط التطبيق[9]:

- ضوابط الدخول المنطقي على البنية التحتية والتطبيقات والبيانات.
- ضوابط دورة حياة تطوير النظام.
- ضوابط إدارة تغيير البرنامج.
- ضوابط الدخول المادي على مركز البيانات.
- ضوابط الاحتياطات الخاصة بالنظام والبيانات واسترجاع الأوضاع الطبيعية.
- ضوابط عمليات الكمبيوتر.

تعمل ضوابط التطبيق على مستوى المعاملات بحيث تضمن صحة إدخالها ومعالجتها ومخرجاتها، تؤثر فعالية تصميم وتشغيل الضوابط العامة لتكنولوجيا المعلومات بصورة كبيرة على مدى اعتماد الإدارة على ضوابط التطبيق في إدارة المخاطر.

[8] من وثائق IS Auditing Guidelines – Application Systems Review – ISACA

[9] من دليل التدقيق التكنولوجي العالمي – (GTAG) التدقيق على ضوابط التطبيق

I.6 لماذا تعتبر ضوابط تكنولوجيا المعلومات مهمة لمدقق تكنولوجيا المعلومات؟

بصورة عامة، يتم الاستعانة بمدقق تكنولوجيا المعلومات لفحص ضوابط الرقابة المتعلقة بالتكنولوجيا، في حين يفحص المدققون الضوابط المالية والتنظيمية والالتزام، و بما أن المزيد من الجهات أصبحت تعتمد على تكنولوجيا المعلومات لميكنة عملياتها، فإن الحد الفاصل ما بين دور مدقق تكنولوجيا المعلومات والمدقق قد اضمحل بشكل سريع أيضاً، وأصبح المطلوب من جميع المدققين فهم بيئة الرقابة في الجهة الخاضعة للتدقيق وذلك لتقديم ضمانات بشأن نظم الرقابة الداخلية المعمول بها في الجهة، وفق المعايير الدولية لأجهزة الرقابة العليا (ISSAI) حول المبادئ الأساسية للتدقيق في القطاع العام: "يجب على المدققين فهم طبيعة الجهة/البرنامج الذي سيخضع للتدقيق"[10]. وهذا يشمل فهم نظم الرقابة الداخلية، إضافة إلى الأهداف والعمليات والبيئة التنظيمية والأنظمة وطريقة سير العمل، ويستند كل نوع من أنواع الرقابة على مجموعة من الأهداف الرقابية التي تضعها الجهة لتخفيف مخاطر الرقابة، دور المدقق هو فهم المخاطر المحتملة للعمل ولتكنولوجيا المعلومات التي تواجه الجهة الخاضعة للرقابة، وبعد ذلك يقوم بتقييم ما إذا كانت الضوابط المطبقة مناسبة لتحقيق الهدف، في حالة الضوابط العامة لتكنولوجيا المعلومات، يجب على المدقق فهم فئاتها الرئيسية وكذلك مدى تطبيقها، وتقييم رؤية الإدارة ووعي الموظفين في الجهة لها، ومعرفة مدى فعالية هذه الضوابط لتقديم ضمان بها، فبينما يشير المعيار الدولي ISSAI 1315 إلى أنه حتى في الجهات الصغيرة التي تكون فيها نظم المعلومات وطريقة سير العمل لإعداد التقارير المالية أقل تطوراً، إلا أن الدور الذي تلعبه يعتبر دوراً هاماً، وفي حال كون الضوابط العامة ضعيفة، فإنها تقلل وبصورة كبيرة من مصداقية الضوابط المرتبطة بتطبيقات تكنولوجيا المعلومات.

في الفصول اللاحقة، سيتم مناقشة بعض أهم الضوابط العامة وضوابط التطبيقات الخاصة بتكنولوجيا المعلومات بالتفصيل، تم وضع مصفوفات التدقيق المقترحة لكل نوع من هذه الضوابط في الملاحق.

[10] ISSAI 100 paragraph 49

II. سير عملية تدقيق تكنولوجيا المعلومات

التخطيط لعمليات تدقيق تكنولوجيا المعلومات

يعتبر التخطيط لعملية التدقيق المفتاح الأساسي لأي عملية تدقيق، بما في ذلك تدقيق تكنولوجيا المعلومات، في معظم أجهزة الرقابة العليا، يتم التخطيط لعملية التدقيق على ثلاثة مستويات –التخطيط الاستراتيجي، والتخطيط ذو النطاق العام (Macro) أو السنوي، والتخطيط التفصيلي (Micro) أو على مستوى الجهة.

II.1 التخطيط الاستراتيجي

إن الخطة الاستراتيجية لجهاز الرقابة الأعلى عبارة عن خطة طويلة الأجل (من 3 إلى 5 سنوات) للوصول إلى أهداف التدقيق، شاملة في ذلك نظم تكنولوجيا المعلومات في الجهات المعنية الخاضعة لسلطة الجهاز الرقابي.

في بعض أجهزة الرقابة العليا، يتم فقط ضم المجالات الجديدة في تكنولوجيا المعلومات إلى خطة التدقيق الاستراتيجية، وهذا قد يشمل ذلك دراسة اقتناء أساليب جديدة لتطوير النظم (على سبيل المثال، البرمجة الذكية) والاستحواذ، أو استخدام الحوسبة السحابية في القطاع العام.
في كلتا الحالتين، توضح عملية التخطيط الاستراتيجي اسلوب واتجاه جهاز الرقابة الأعلى نحو تحقيق أهداف التدقيق في مجال تكنولوجيا المعلومات في المستقبل.

II.2 التخطيط العام:

عادة ما يتم القيام بالتخطيط السنوي للتدقيق على مستوى جهاز الرقابة الأعلى[11] لاختيار مجالات التدقيق، مع الانتشار السريع لنظم المعلومات الحديثة في الحكومات والموارد المحدودة لأجهزة الرقابة العليا، فإن **النهج المبني على أساس المخاطر** لاختيار المواضيع المناسبة وتحديد الأولوية لها يكون ملائماً، علاوة على ذلك، يجب على جهاز الرقابة الأعلى دمج عمليات التدقيق الالزامية، مثل تلك التي يلزم بها القانون أو التي يطلبها البرلمان أو الكونغرس أو الجهات الرقابية الأخرى.

خطوات النهج المبني على أساس المخاطر للتخطيط لعمليات التدقيق:

1. التعرف على عالم التدقيق الذي يشمل جميع الجهات الملزمة بالخضوع للتدقيق من قبل جهاز الرقابة الأعلى لوقوعها تحت سيطرة سلطته.
2. إعداد قائمة بنظم المعلومات المستخدمة في الجهة الخاضعة للتدقيق.
3. تحديد العوامل التي تؤثر على مدى أهمية النظام بالنسبة للجهة لتتمكن من القيام بمهامها وتقديم خدماتها.
4. تحديد درجة أهمية هذه العوامل، يمكن أن يتم ذلك بالتشاور مع الجهة الخاضعة للتدقيق.
5. تصنيف المعلومات لجميع النظم في جميع الجهات، وبناء على المجموع التراكمي، يتم ترتيب أولويات التدقيق للنظم/الجهات.
6. إعداد خطة تدقيق سنوية، والتي ينبغي أن يتم فيها تحديد الأولويات والنهج والجدول الزمني لعمليات تدقيق تكنولوجيا المعلومات، ويمكن تكرار هذا النهج سنويا، وبالتالي يصبح جزءا من الخطة السنوية.

i. النهج القائم على أساس المخاطر

عادة ما تستخدم الجهات الخاضعة لرقابة أجهزة الرقابة العليا نظم معلومات مختلفة، وتملك تطبيقات مختلفة لمهام وأنشطة مختلفة، كما قد تكون أنشطتها متوزعة على مواقع جغرافية مختلفة.

[11] إن أجهزة الرقابة العليا في جميع أنحاء العالم لها هياكل تنظيمية مختلفة، تشير المرحلة الأولى هنا إلى الجهاز الرقابي ذو الهيكل التنظيمي الاعتيادي، أما التخطيط على المستوى العالمي فإن القيام به واعتماده يتم في مقار الأجهزة الرقابية، على أن يتم التدقيق الفعلي (المرحلة الثانية للتخطيط) على المستوى الميداني.

هناك العديد من المخاطر الملازمة لنظم المعلومات، وهذه المخاطر تؤثر على النظم المختلفة بطرق مختلفة، فمثلا عواقب خطر عدم توافر نظام الفواتير في متجر تجزئة مزدحم بالعمل حتى لمدة ساعة يمكن أن تكون جدية، كما يمكن أن يتسبب خطر التعديل غير المصرح به على نظام الخدمات المصرفية عبر الإنترنت بالاحتيال والخسائر المحتملة، قد يكون نظام معالجة مجموعة من البيانات أو نظام توحيد البيانات أقل عرضة لبعض من هذه المخاطر، أيضاً البيئات التقنية التي تعمل بها نظم المعلومات قد تؤثر على المخاطر المرتبطة بهذه النظم[12]، إن النهج المبني على أساس المخاطر يساعد المدقق في تحديد الأولويات عند اختيار أنظمة تكنولوجيا المعلومات ليتم التدقيق عليها، ولاستخدام إطار عمل تقييم المخاطر، يحتاج جهاز الرقابة الأعلى لوجود حد أدنى من المعلومات عن الجهات، وعادة ما يتم تجميعها من خلال الاستبيانات.

في حين تعتبر عملية تقييم المخاطر أحد الطرق لتحديد الجهة التي ستخضع لتدقيق تكنولوجيا المعلومات، فإن أجهزة الرقابة العليا أيضاً تحدد الجهات التي سيتم التدقيق عليها بشكل دوري، أو بناء على طلب محدد من الجهات الرقابية (الكونغرس، البرلمان، السلطة التشريعية، الخ).

II.3 التخطيط التفصيلي:

التخطيط الجزئي ينطوي على وضع خطة تفصيلية للتدقيق على جهة معينة، ابتداءً من تحديد أهداف التدقيق، وتساعد هذه الخطة المدقق في إعداد برنامج لتدقيق تكنولوجيا المعلومات، يسبق ذلك فهم المدقق العميق للجهة الخاضعة للتدقيق ونظم المعلومات الخاصة بها، ويهدف هذا الدليل إلى مساعدة المدقق أنه بمجرد إعداد الخطة لتعميم مصفوفة التدقيق ذات أهداف التدقيق المحددة لكل مجال (الحوكمة، وأمن المعلومات، وغيرها) من المجالات التي سيتم التدقيق عليها، يتطلب التخطيط التفصيلي للتدقيق فهم الجهة وعمل تقييم أولي للضوابط لتسهيل هذه العملية.

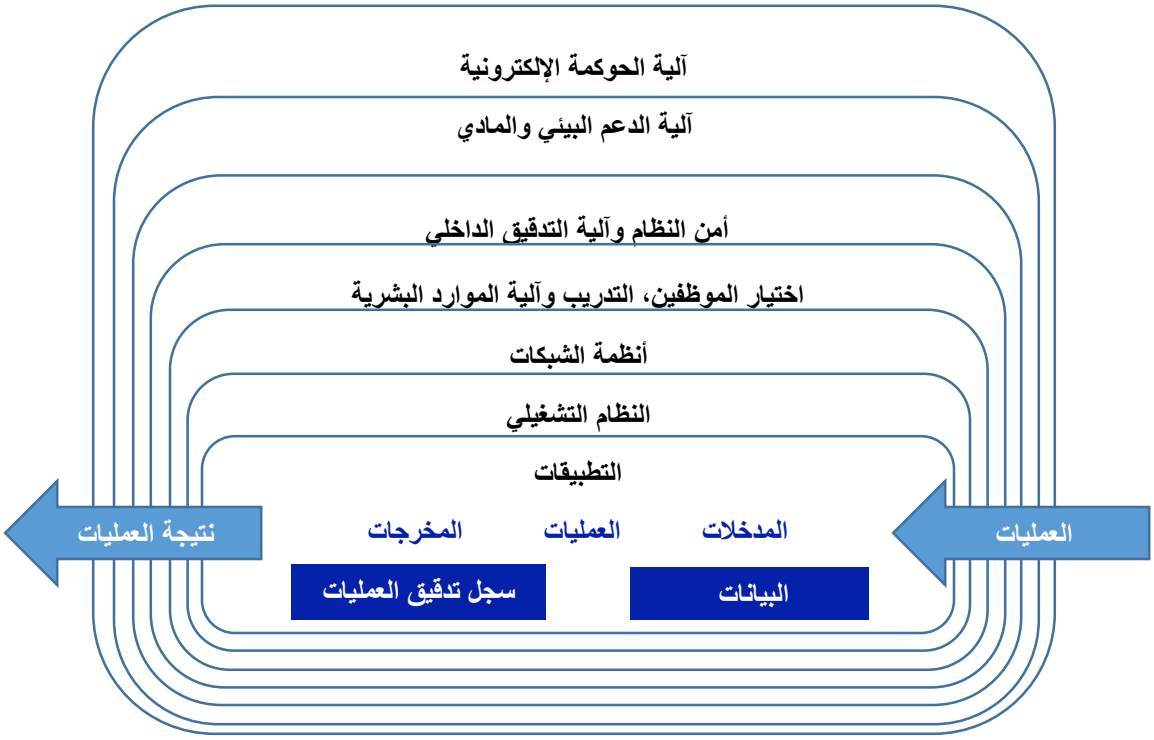
---

12 S. Anantha Sayana–ISACA

i. فهم الجهة

إن مدى المعرفة المطلوبة من مدقق نظم المعلومات حول الجهة والعمليات التي تقوم بها يعتمد بشكل كبير على طبيعة الجهة ومستوى الدقة المطلوبة في مهمة التدقيق، إن المعرفة المطلوبة حول الجهة يجب تشمل المخاطر المتعلقة بأعمالها، والمخاطر المالية، والمخاطر الكامنة التي تواجهها وتواجه نظم تكنولوجيا المعلومات فيها، وينبغي أن تشمل أيضاً مدى اعتماد الجهة على الاستعانة بمصادر خارجية لتحقيق أهدافها، وإلى أي مدى تم اختصار أعمالها إلى بيئة تكنولوجيا المعلومات[13]، يجب على المدقق استخدام هذه المعلومات في تحديد المشاكل المحتملة، وصياغة الأهداف ومجال العمل، وتنفيذ العمل، والأخذ بالاعتبار الإجراءات الإدارية التي يجب أن ينتبه لها مدقق نظم المعلومات.

فيما يلي الشكل الاعتيادي لنظام المعلومات في أي جهة:



الشكل 1.2: تخطيط نموذجي لتكنولوجيا في الجهة

[13] إن الجهات التي تتحول من البيئة اليدوية إلى البيئة الحاسوبية عادة ما تقوم بإعادة هندسة العمليات الوظيفية (BPR) لديها، قد يكون من الممكن أن يتم القيام ببعض العمليات يدوياً جنباً إلى جنب أنظمة تكنولوجيا المعلومات.

إن أي تطبيق حاسوبي يتألف من مزيج من قواعد بيانات ونظام إدارة خاص بها وبرنامج يقوم بتطبيق قواعد العمل في النظام، وواجهة المستخدم الأمامية، وكل ذلك يكون مدعما بشبكة الحاسب في حال وجودها، يتم وضع قواعد البيانات وبرامج التطبيقات على الخوادم، والتي تعتبر أجهزة حاسوبية ذات قدرة عالية على استضافة التطبيقات وقواعد البيانات الكبيرة والمتعددة، ويمكن اقتصار عمل الخادم على متطلبات معينة مثل تخصيص خادم للبيانات، وخادم للتطبيق، وخادم الانترنت وخادم البروكسي.

يستطيع مدقق تكنولوجيا المعلومات أن يحدد منهج عملية التدقيق بناء على ما تم اكتسابه من معلومات حول الجهة الخاضعة للتدقيق ونظم المعلومات فيها، وسوف تتضمن عملية تدقيق تكنولوجيا المعلومات في النهاية الضوابط العامة وضوابط التطبيقات.

ii. الأهمية

يجب أن يتم تحديد أهمية[14] موضوعات تدقيق تكنولوجيا المعلومات وفق الإطار العام للسياسة التي يتم فيها تحديد الموضوعات الهامة في جهاز الرقابة الأعلى المسئول عن صياغة تقرير التدقيق، ويجب على المدقق أن يضع في عين الاعتبار أهمية الموضوع فيما يخص البيانات المالية (التدقيق على اللوائح التنظيمية) أو من حيث طبيعة الجهة الخاضعة للتدقيق أو نشاطها.

ينبغي على مدقق نظم المعلومات تحديد ما إذا كان هناك أي قصور عام في تكنولوجيا المعلومات قد يؤدي إلى خلل فعلي، يجب أن يتم تقييم أهمية القصور في الضوابط العامة لتكنولوجيا المعلومات بناء على تأثيرها على ضوابط التطبيق، أي ما إذا كانت ضوابط التطبيق المصاحبة غير فعالة أيضاً، في حال كان الخلل في التطبيق راجع إلى الضوابط العامة لتكنولوجيا المعلومات، إذا فهو قصور هام، على سبيل المثال إذا كان حساب الضريبة في التطبيق خاطئ وكان ناتجاً عن ضوابط ضعيفة للتغيير على الجداول الضريبية، قد يصبح قرار الإدارة بعدم اتخاذ إجراءات لتصحيح هذا القصور في الضوابط العامة لتكنولوجيا المعلومات والتأثير

[14] وضحت الفقرة 43 من ISSAI 100 ما يلي "غالباً ما يتم تحديد الاهمية بالقيمة، ولكن من الممكن أن تقوم طبيعة الشيء أو خصائصه بإكسابه قيمة".

المصاحب له على بيئة الرقابة قرارا هاما عندما يتم جمعه مع جوانب قصور أخرى في الضوابط والتي تؤثر بدورها على بيئة الرقابة[15].

iii. تخصيص الموارد

يتطلب تدقيق تكنولوجيا المعلومات تخصيص الموارد اللازمة، وخاصة القوى العاملة التي يجب أن تكون على معرفة حسنة بنظم وعمليات وآليات تكنولوجيا المعلومات التي تقود إلى تطبيق ناجح لتكنولوجيا المعلومات، وبالإضافة إلى الموارد البشرية المناسبة[16]، يجب أن يتم توفير الميزانية المناسبة، والبنية التحتية[17] وأية متطلبات أخرى يتم تحديدها، كما ينبغي أن يتم تحديد الجدول الزمني للتدقيق، وذلك بالتشاور مع الجهة الخاضعة للتدقيق إذا كان ذلك ممكناً.

iv. العمل مع الجهة الخاضعة للتدقيق

يجب أن يتم إطلاع الجهة الخاضعة للتدقيق على مجال التدقيق، وأهدافه، ومعايير التقييم الخاصة به والتي ستُناقش إذا تطلب الامر ذلك، ويمكن لجهاز الرقابة الأعلى إذا لزم الأمر، أن يخاطب الجهة الخاضعة للتدقيق وأن يصف أعمال التدقيق المطلوبة، يجب على جهاز الرقابة الأعلى التأكيد على ضرورة التعاون والدعم من الجهة الخاضعة للتدقيق لاستكمال عملية التدقيق، بما في ذلك الاطلاع على السجلات والمعلومات، سواء كانت يدوية أو إلكترونية.

---

[15] Materiality Concepts for Auditing Information, ISACA Guidelines (G6)

[16] المقصود بالموارد البشرية المناسبة الموظفين الذين لديهم معرفة حول نظم المعلومات ويمكنهم تنفيذ عمليات استخراج البيانات وتحليلها إذا لزم الأمر، حيث تتطلب عمليات تدقيق تكنولوجيا المعلومات استخدام مهارات تكنولوجيا المعلومات للقيام بعمليات التدقيق. يجب على جهاز الرقابة الأعلى الرجوع إلى المعيار ISSAI 100 الفقرة 52 حول توفير الكفاءة اللازمة لموظفيها قبل الشروع في تدقيق تكنولوجيا المعلومات.

[17] وتشمل برامج الأجهزة، وأنظمة التشغيل، ونظام إدارة قواعد البيانات (RDBMS)، وكذلك أجهزة التخزين، والوسائل الحاسوبية كأجهزة الكمبيوتر، وأجهزة الكمبيوتر المحمولة وغيرها لتمكين استخراج وتحليل المعلومات.

٧. جمع أدلة التدقيق

1. التقييم الأولي لضوابط تكنولوجيا المعلومات

يجب على مدقق تكنولوجيا المعلومات إجراء تقييم أولي لضوابط تكنولوجيا المعلومات في النظام الخاضع للتدقيق لضمان أن الرقابة الحالية (الضوابط العامة وضوابط التطبيق) يمكن الاعتماد عليها، يشمل تقييم الضوابط في هذا المستوى ما يلي:

أ. تقييم استخدام آليات مناسبة لحوكمة تكنولوجيا المعلومات وأنها تؤدي مهامها.

ب. تقييم تماشي أهداف تكنولوجيا المعلومات مع أهداف العمل.

ج. تقييم وجود آليات مناسبة للحصول على حلول لتكنولوجيا المعلومات (والتي تشمل تطبيقات تكنولوجيا المعلومات، الأجهزة، البرامج، الموارد البشرية، الشبكة، حلول للخدمات الخ).

د. أن الضوابط على مستوى الجهة مضمنة في عمليات تكنولوجيا المعلومات اليومية، وإجراءات أمن المعلومات في الجهة، وإجراءات استمرارية الأعمال، والإجراءات احتياطية، وإدارة التغيير، وتقديم الخدمات، والملاحظات.

يمثل ما ورد أعلاه ضوابط تكنولوجيا المعلومات العامة التي لا تقتصر على تعاملات أو تطبيق معين، ولكنها تعني بمجمل بنية تكنولوجيا المعلومات التحتية في الجهة، شاملة بذلك السياسات المتعلقة بتكنولوجيا المعلومات، والإجراءات، وممارسات العمل، ينبغي أن يتم تصميم الاختبارات بشكل دقيق باستخدام طرق[18] مثل المقابلات الشخصية، والمسح من خلال الاستبيانات، والملاحظات، والدخول بالتفاصيل[19]، والحصول على البيانات وتحليلها، والبراهين، الخ.

---

[18] يمكن أن يتم استخدام هذه الطرق لكل من الاختبار المبدئي والاختبار الأساسي، ويمكن لمدقق تكنولوجيا المعلومات أن يختار واحدة أو أكثر من هذه الطرق أثناء إجراء أي من التقييمين.

[19] ويتم إجراء اختبارات الدخول بالتفاصيل للفهم ولبناء الثقة في نظم تكنولوجيا المعلومات الخاصة بالعميل وإجراءات الرقابة الداخلية، يستخدم هذا الاختبار إما لفهم نظم تكنولوجيا المعلومات أو للتحقق من النتائج المستخلصة من الاختبارات المبدئية أو الاختبارات الأساسية الأخرى، وبالتالي فإنه قد لا يكون مقتصرا على اختبار الضوابط.

2. الاختبار الأساسي

في الاختبار الأساسي يتم تصميم الاختبارات لتقديم أدلة اثبات على صحة الدوافع وفق أهداف التدقيق، ويشمل الاختبار الأساسي اختبار تفصيلي لضوابط تكنولوجيا المعلومات باستخدام مختلف التقنيات والأدوات اللازمة للاستعلام عن واستخلاص البيانات وتحليلها.

يشمل تحليل البيانات البنود المدرجة أدناه[20]:

- تحديد الغرض من التحليل أو المشروع.
- فهم العينات قيد الدراسة.
- إدراك نسق[21] البيانات وبنيتها (Layouts & Formats).
- وضع مفتاح رئيسي للبيانات في حال وجود ضرورة للمطابقة أو الدمج.
- تحديد أسئلة البحث / أهداف التدقيق.
- الطرق المستخدمة للإجابة على أسئلة البحث:
  * معايير التقييم
  * الأدلة
  * التحليل
  * الخلاصة
- إجراءات إعادة هيكلة الملف (تركيب الجُمل، إضافة متغيرات جديدة حسب الحاجة)
- إجراءات تنظيف البيانات (على سبيل المثال إزالة القيم المتطرفة).

---

[20] Jonathan Steinberg, *An Overview of Data Analysis*; Bruce A. Kaplan *Data Analysis Research*; Muhamad Jantan *Introduction to Data Analysis*

[21] تعتبر هذه واحدة من أهم الخطوات التي تسبق القيام بتحليل البيانات، أن إدراك نسق البيانات وبنيتها يعني فهم قواعد البيانات المختلفة وما تشمله من جداول، وأسلوب البرمجة المستخدم والعلاقات بين الجداول وقواعد البيانات، سيكون فهم الأنواع المختلفة لقواعد البيانات مفيداً في هذا الخصوص.

يمكن تنفيذ معظم عمليات التحليل من ملف البيانات التشغيلي مباشرة، قد تتطلب بعض عمليات التحليل تحويل نوع البيانات، أو جزء منها، أو بيانات مدخلة معينة لتتوافق مع البرامج الإحصائية، تستخدم نظم تكنولوجيا المعلومات أنواع متعددة من البيانات (رقمية، أحرف، سلسلة أحرف، الخ)، يجب أن يكون مدقق تكنولوجيا المعلومات واعياً لتلك الأمور ويستخدم الأدوات المناسبة للتحليل، يمكن أن يستخدم المدقق برامج تدقيق عامة أو متخصصة لتحليل المعلومات، من أمثلة برامج التدقيق العامة التي تسهل الحصول على البيانات وتحليلها برنامج مايكروسوفت اكسل، ومايكروسوفت أكسيس، وآيديا (IDEA)، واي سي ال (ACL) وغيرها.

بعد ذلك يمكن أن يعتمد مدققي تكنولوجيا المعلومات أي من الأساليب التالية وفقا للمتطلبات:

أ–القيام باستخراج البيانات عن طريق **الحصول على نسخة من البيانات** من الجهة الخاضعة للتدقيق، قد يضطر مدققي تكنولوجيا المعلومات إلى خلق بيئة مماثلة (نظام التشغيل، ونظام إدارة قواعد البيانات، والأجهزة وغيرها)، للموجود في الجهة الخاضعة للتدقيق وذلك لتحليل البيانات أو استخراجها من البيانات المنسوخة، قد يضطر مدقق تكنولوجيا المعلومات لتحويل البيانات من نوع إلى آخر لتسهيل قراءتها وتحليلها بصورة أفضل.

ب–استخدام برنامج التدقيق لاستخراج البيانات من أنظمة متعددة، سواء كانت أنظمة تشغيل، أنظمة إدارة قواعد البيانات، ونظم تطبيقات وغيرها، يمكن أن يستخدم مدققي تكنولوجيا المعلومات **برامج تدقيق عامة** أو **برامج تدقيق متخصصة**، يمكن استخدام برامج التدقيق العامة للتدقيق على صناعات معينة أو استخدامها كوسيلة يتم من خلالها تقييم أداء الوظائف المختلفة لأنظمة الكمبيوتر، ويعتمد استخدام أي من هذه البرامج أو لمزيج منها على أهداف التدقيق والنطاق الذي يجب أن تغطيه عمليات تدقيق تكنولوجيا المعلومات.

ج–استخدام **بيانات للاختبار** في الحالات التي يراد بها اختبار جودة البرنامج، الافتراض هو أنه من الممكن تعميم الثقة في البرنامج في حال نجاحه في مجموعة معينة من الاختبارات، واستخدام بيانات الاختبار يتضمن على رسم خطة لبيانات الاختبار وتحضير البيانات قبل تشغيل البرنامج بها.

يجب على مدقق تكنولوجيا المعلومات اختيار تقييم مخاطر مناسب واستخدام تقنيات أخذ العينات للتوصل إلى استنتاجات مناسبة بناء على عمليات فحص إحصائية وافية تتم على بيانات محدودة. بصورة عامة، تعتبر الاستعانة بخبير أو إحصائي من الجهة لتحديد طريقة أخذ العينات ممارسة جيدة.

III. توثيق التدقيق

إن توثيق عمليات تدقيق نظم المعلومات ما هي إلا تسجيل لأعمال التدقيق التي تم القيام بها، وأدلة التدقيق التي تدعم نتائج التدقيق والاستنتاجات، يجب أن يضمن مدقق تكنولوجيا المعلومات المحافظة على نتائج التدقيق وأدلة التدقيق بطريقة تتوافق مع متطلبات الموثوقية والاكتمال، والكفاية، والصحة. من المهم أيضاً أن يؤكد مدققي تكنولوجيا المعلومات على حفظ عملية التدقيق لضمان إمكانية التحقق اللاحق من إجراءات التدقيق، ويشتمل هذا على طرق توثيق مناسبة.

يشتمل التوثيق على تسجيل ما يلي:

- التخطيط والإعداد لمجال التدقيق وأهدافه.
- برامج التدقيق.
- الأدلة التي تم جمعها والتي بناءً عليها تم التوصل للاستنتاجات.
- جميع أوراق العمل بما في ذلك الملف العام المتعلق بالجهة والنظام.
- النقاط التي تمت مناقشتها في المقابلات والتي تذكر بوضوح موضوع النقاش، الشخص الذي تمت مقابلته، ومنصبه ومهامه والوقت والمكان.
- ملاحظات المدقق حيث أنه قد راقب تنفيذ العمل، ويمكن أن تشتمل هذه الملاحظات على المكان والوقت، وسبب الملاحظة والأشخاص المعنيين.
- التقارير والبيانات التي حصل عليها المدقق من النظام مباشرة أو التي قدمها له موظفي الجهة الخاضعة للتدقيق، يجب على مدقق نظم المعلومات التأكيد على أن هذه التقارير تشير إلى مصدر التقرير، والتاريخ والوقت والشروط التي تم تغطيتها.

- يمكن أن يضيف المدقق تعليقاته وتوضيحاته حول مخاوفه وشكوكه والحاجة للحصول على معلومات إضافية في مختلف مراحل عملية التوثيق، يجب على المدقق أن يرجع إلى هذه التعليقات في وقت لاحق لإبداء رأيه وتوصياته حول طريقة حل هذه الأمور وموضعها من التقرير.
- للحفاظ على البيانات الإلكترونية، ينبغي على الأجهزة الرقابية العليا توفير نسخة احتياطية من البيانات الواردة من الجهة الخاضعة للتدقيق وكذلك من نتائج الاستفسارات والتحليل، ويجب المحافظة على سرية وثائق التدقيق والاحتفاظ بها لفترة من الزمن وفق قرار جهاز الرقابة الأعلى أو كما يفرضه القانون.
- عندما تتم مراجعة أعمال التدقيق من قبل أحد النظراء أو الإدارة الأعلى، ينبغي أيضاً تسجيل الملاحظات الناشئة عن المراجعة في الوثائق.
- ينبغي أن يكون كل من مسودة تقرير التدقيق والتقرير النهائي جزءاً من وثائق التدقيق.

IV. الإشراف والمراجعة

ينبغي أن يتم الاشراف على عمل موظفي التدقيق بشكل صحيح أثناء التدقيق[22]، وينبغي أن تتم مراجعة العمل الموثق من قبل أحد كبار موظفي التدقيق[23]، يجب أن يقدم كبير موظفي التدقيق الإرشادات اللازمة والتدريب والتوجيه أثناء إجراء التدقيق، والذي يعد أمرا حاسما في هذا المجال الجديد – تدقيق تكنولوجيا المعلومات.

V. إعداد التقارير

ينبغي تطبيق نظام إعداد التقارير المتبع في جهاز الرقابة الأعلى على تقارير تدقيق تكنولوجيا المعلومات، يجب أن تقيم تقارير تدقيق تكنولوجيا المعلومات التقنيات التي تم فحصها بناء على مستوى الدقة المطلوبة من قبل المهتمين بالتقرير .

---

22 ISSAI 100 paragraphs 39, 41

23 ISSAI 100 paragraph 54

يجب على مدققي تكنولوجيا المعلومات تقديم تقرير حول النتائج التي توصلوا إليها في حينه، وينبغي أن تكون النتائج بناءة ومفيدة للجهة الخاضعة للتدقيق وللمعنيين بالأمر، يمكن تقديم التقرير إلى السلطات المختصة وفقاً للتفويضات الممنوحة لجهاز الرقابة الأعلى وتدقيق تكنولوجيا المعلومات.

VI. مراحل إعداد التقارير

هناك عدة طرق للوفاء بمتطلبات المعايير الدولية لأجهزة الرقابة العليا ISSAI والتي تتعلق بالمرحلة الختامية من عملية التدقيق، وهي تعتمد على العادات المتبعة في أجهزة الرقابة العليا وبيئتها القانونية، وأحد هذه الطرق تتكون من ثلاث مراحل للتقرير في عملية التدقيق، وهي كما يلي:

VI.1 ورقة المناقشة

تبدأ عملية إعداد التقرير بمناقشة المسودة الأولى (ورقة المناقشة)، يتم إرسال هذه المسودة إلى الإدارة الوسطى للعميل قبل الجلسة الختامية، ثم يتم تضمين المسودة كأحد بنود المناقشة في الجلسة الختامية، ويتيح هذا الاجراء التعرف على وتصحيح أو إزالة أي صيغة تحريضية، أو أخطاء فعلية أو تناقضات في مرحلة مبكرة، حالما يناقش العميل والمدقق محتويات مسودة المناقشة، يقوم المدقق بالتعديلات اللازمة ويرسل للعميل النسخة الرسمية الأولى.

VI.2 كتاب الإدارة

كتاب الإدارة هو المسودة الرسمية التي يتم تقديمها للجهة الخاضعة للتدقيق حتى تتمكن من الرد على الملاحظات التي أثيرت، وهذا يسمح للإدارة بالتركيز على الملاحظات والاستنتاجات والتوصيات الواردة في المسودة الرسمية التي استلمتها، عند هذه المرحلة يجب على الإدارة أن تكتب رسمياً الملاحظات والردود للمدقق ومعالجة كافة الملاحظات.

VI.3 تقرير التدقيق النهائي

عندما يتم استلام ملاحظات العميل، يعد المدقق بعدها الردود مشيرا إلى رأيه الفني، ويتحقق ذلك عن طريق الجمع بين ملاحظات المدقق وردود الجهة في تقرير واحد، وهو تقرير التدقيق (تقرير التدقيق النهائي).

عند إعداد التقارير حول المخالفات أو حالات عدم الالتزام بالقوانين أو اللوائح، يجب على المدققين الاهتمام بوضع الملاحظات التي توصلوا إليها في المنظور الصحيح، فالتقارير حول المخالفات يمكن أن يتم إعدادها بغض النظر عن رأي المدقق.

بطبيعتها، تميل تقارير التدقيق إلى النقد الهام، ولكن من أجل أن تكون بناءة ينبغي أن تتناول أيضاً الإجراءات التصحيحية المستقبلية المستقاة من إفادة الجهة الخاضعة للتدقيق أو من قبل المدقق، بما في ذلك الاستنتاجات أو التوصيات[24].

VI.4 صياغة النتيجة والتوصيات

يجب أن تستند الملاحظات ونتائج التدقيق والتوصيات إلى الأدلة، وعند صياغة نتيجة أو تقرير التدقيق، ينبغي أن يأخذ مدقق تكنولوجيا المعلومات في الاعتبار الأهمية النسبية للموضوع من حيث طبيعة التدقيق أو الجهة الخاضعة للتدقيق[25].

يجب على مدقق تكنولوجيا المعلومات صياغة الاستنتاجات بشأن ملاحظات التدقيق بناء على أهداف التدقيق، وينبغي أن تكون الاستنتاجات ذات صلة ومنطقية وغير متحيزة، كما ينبغي تجنب الاستنتاجات العامة بشأن غياب الضوابط ووجود المخاطر، وذلك عندما لا يتم دعمها بالفحص الأساسي.

يجب على مدققي تكنولوجيا المعلومات القيام بتحديد التوصيات عندما يتم التأكد من إمكانية حدوث تحسن واضح في العمليات والأداء من خلال الملاحظات التي تم الإبلاغ عنها، كما ينبغي على المدققين تحديد وضع الملاحظات والتوصيات الهامة من عمليات التدقيق السابقة والتي لم يتم اتخاذ إجراءات تصحيحية حولها ولها

---

24 ISSAI 100 paragraph 55

25 ISSAI 100 paragraph 54.

تأثير على أهداف التدقيق الحالية، ويمكن للتوصيات البناءة أن تشجع على التغير للأفضل، تكون التوصيات بناءة بشكل كبير عندما يتم توجيهها لإيجاد الحلول المناسبة لمشاكل محددة، وتكون عبارة عن إجراءات محددة وموجهة إلى الأطراف التي لديها صلاحية التصرف، وعملية، وفعالة من حيث التكلفة.

لعملية إعداد تقارير متوازنة، ينبغي أن يتم تسليط الضوء على الإنجازات الجديرة بالذكر، إذا كانت تقع ضمن التفويضات الممنوحة لجهاز الرقابة الأعلى والمتعلقة بإعداد التقارير.

VI.5 القيود المفروضة على تدقيق لتكنولوجيا المعلومات

أيضا ينبغي أن تتم الإشارة في التقرير إلى القيود المفروضة على تدقيق تكنولوجيا المعلومات، عادة ما تكون هذه القيود عبارة عن عدم القدرة على الدخول على البيانات والمعلومات، وعدم وجود التوثيق المناسب لعمليات الحوسبة، مما يقود مدقق تكنولوجيا المعلومات لابتكار أساليبه الخاصة للتحقيق والتحليل والتوصل إلى النتائج، ويجب أن تتم الإشارة في التقرير وبصورة مناسبة لأي من القيود التي واجهها مدقق تكنولوجيا المعلومات.

VI.6 استجابة الجهة

في حالة إعداد تقارير تدقيق تكنولوجيا المعلومات، فإن الحصول على ردود من الجهة على ملاحظات التدقيق يكون في غاية الأهمية، يجب أن يجتمع مدققي تكنولوجيا المعلومات مع إدارة الجهة على أعلى مستوى لتوثيق ردودها، في حال فشل هذه الجهود، يجب الاحتفاظ بأدلة كافية حول الجهود التي تم بذلها ويتم ذكرها في التقرير.

المراجـــع:

1. COBIT 4.1 Framework, 2007, IT Governance Institute
2. IDI AFROSAI/E-IT Audit Courseware
3. ISSAI 100 Fundamental Principles of Public Sector Auditing
4. ISSAI 200 Fundamental Principles of Financial Auditing
5. ISSAI 300 Fundamental Principles of Performance Auditing
6. ISSAI 400 Fundamental Principles of Compliance Auditing

نموذج مصفوفة التدقيق

استخدام مصفوفة التدقيق

من المفيد أن يتم وضع مصفوفة تدقيق تغطي كافة الموضوعات ذات الصلة بالتدقيق من حيث أهداف ومجال التدقيق وذلك خلال مرحلة التخطيط.

على الرغم من استخدام أجهزة الرقابة العليا لنماذج مختلفة من مصفوفات التدقيق للتخطيط لعملية التدقيق إلا أن المعلومات التي تحتويها مصفوفات التدقيق متشابهة.

والشكل المقترح لمصفوفة التدقيق[26] والتي تم استخدامها في هذا الدليل هي كما يلي:

مجال التدقيق	
هدف التدقيق:	
موضوع التدقيق:	
المعايير:	
المعلومات المطلوبة	وسائل التحليل
نتيجة التدقيق يتم تعبئتها من قبل المدقق:	

[26] تحدد مصفوفة التدقيق أهم مواضيع التدقيق ومجاله وأمور أخرى في مجالات مختلفة من تدقيق تكنولوجيا المعلومات، الأمر الذي يجب أن يدركه مدقق تكنولوجيا المعلومات بأنه يجب أن يتم إعداد هذه المصفوفة في مرحلة التخطيط، إلا أنه يمكن تحديث المحتويات أثناء عملية تدقيق تكنولوجيا المعلومات، إذا لزم الأمر. كما يمكن أن يجري جهاز الرقابة الأعلى التعديلات اللازمة على شكل مصفوفة التدقيق، إذا تم اعتبار ذلك ضروريا.

1. مجال التدقيق

يجب أن يكون مدققي تكنولوجيا المعلومات قادرين على تحديد مواضيع التدقيق التي سيتم تبنيها خلال مرحلة التقييم الأولية التي تتألف من تقييم أولي للجهة ولبيئتها، ولا سيما بيئة تكنولوجيا المعلومات.

كما أن مواضيع التدقيق ستتبين من خلال مجال تدقيق تكنولوجيا المعلومات، على سبيل المثال، في العديد من أجهزة الرقابة العليا يتم تنفيذ عملية تدقيق تكنولوجيا المعلومات جنباً إلى جنب مع التدقيق المالي وتدقيق الالتزام وتشمل تقييماً لضوابط تكنولوجيا المعلومات العامة وضوابط التطبيق، وفي حالات أخرى، يمكن أن يكون مجال تدقيق تكنولوجيا المعلومات عبارة عن تقييم لإجراءات الجهة المتبعة في شراء أو تطوير أنظمة إسناد أرضية جديدة (ITR Systems)، أصبح العديد والمزيد من أجهزة الرقابة العليا تقوم بإجراء تدقيق أداء شامل لأنظمة تكنولوجيا المعلومات الحساسة، بعض الأمثلة على ذلك نظام تقييم وجمع الإيرادات والضريبة، ونظام حجز السكك الحديدية، ونظام الخدمات المدنية مثل تسجيل الملكية، الإحصاءات السكانية، وأرقام الهوية الوطنية وغيرها.

إن مواضيع التدقيق يمكن أن تنشأ عن المواضيع المرتبطة بتكنولوجيا المعلومات أو عن مواضيع الحوكمة المؤثرة على نظم المعلومات في الجهة الخاضعة للرقابة.

2. أيضا ينبغي على مدققي تكنولوجيا المعلومات القيام بتحديد معايير التقييم، والتي يجب أن تكون قابلة للقياس وموثوق بها وتتوافق مع أهداف ومواضيع التدقيق الخاضعة للفحص في هذه المرحلة.

لاستيفاء شروط المعايير، يجب أن يتم تحديد وجمع معلومات أو أدلة كافية لدعم نتائج التدقيق وحفظها ليصبح ممكنا الرجوع إليها في المستقبل، قد تتطلب عملية جمع المعلومات أدوات وتقنيات معينة، يجب أن يتم تحديد تلك الأدوات والتقنيات المختلفة التي سيتم استخدامها، خاصة خلال مرحلة الاختبار الأساسي، وكذلك تعتبر طرق التحليل أساليب معتادة بالنسبة لبيئة نظم المعلومات وتحتاج إلى أن يتم استخدامها بشكل مناسب لاستخلاص النتائج ذات الصلة ولها دلائلها، سيتم مناقشة هذا لاحقا في الفحص الأساسي عند تنفيذ التدقيق.

تحديد مصادر المعلومات

تكون مصادر المعلومات عادة في الجهة ذات نظم تكنولوجيا المعلومات كما يلي:

أ. الرسوم البيانية التوضيحية، وهي تشمل الرسم البياني التوضيحي للنظام، والرسم البياني التوضيحي للبيانات، والرسم البياني التوضيحي للعمليات وغيرها.

ب. وثائق تطوير النظام مثل وثيقة مواصفات متطلبات المستخدم (URS)[27]، وثيقة مواصفات متطلبات النظام (SRS).

ت. البيانات الإلكترونية[28].

ث. المعلومات الأخرى المتاحة في الجهة وتتعلق بمهامها، ونظم الرقابة والتوجيه وغيرها، مثل النماذج والمعلومات المتعلقة بالميزانية، والتقارير المختلفة بما في ذلك التقارير حول عمليات التدقيق السابقة، وعمليات التدقيق الخارجية والداخلية وغيرها.

ج. السياسات والإجراءات والإرشادات الأخرى.

ح. مستخدمي النظام.

تحديد تقنيات وأدوات جمع المعلومات

لكل جهة خاضعة للتدقيق مجموعة خاصة بها من الأجهزة، ونظم التشغيل، ونظم إدارة قواعد البيانات، والتطبيقات، وبرامج الشبكة، ينبغي أن يكون مدققي تكنولوجيا المعلومات قادرين على جمع المعلومات من هذه

---

27 تحتوي وثيقة مواصفات متطلبات المستخدم (URS) على المتطلبات التي توضح مهام الجهة التي يفترض أن ينفذها نظام تكنولوجيا المعلومات وعمليات التشغيل التي يرغب بها المستخدم النهائي. وتعتبر هذه هي المرحلة التي يجب أن يحدد المستخدمين فيها متطلبات المستخدم تحديدا كاملاً وواضحاً. فقد يؤدي عجز في توثيق أحد متطلبات المستخدم إلى وضع نظام ناقص. هذه هي نقطة انطلاق جيدة لمدقق تكنولوجيا المعلومات.

28 تشمل البيانات الإلكترونية البيانات المركبة حيث تعتبر أنظمة إدارة قواعد البيانات (RDBMS) أكثرها شيوعاً وهي قادرة على التعامل مع حجم كبير من البيانات مثل Oracle, IBM DB2, Microsoft SQL Server, Sybase, and Teradata

المصادر للقيام بعمليات التحليل، من الواضح أن فهم نظام تكنولوجيا المعلومات وقواعد البيانات في الجهة يعتبر خطوة أساسية لاستخلاص البيانات.

يجب على مدققي تكنولوجيا المعلومات اتخاذ قرار بشأن مدى ملاءمة استخدام واحدة أو أكثر من تقنيات جمع المعلومات وأن هذه التقنيات تحوز على رضاهم من حيث نزاهتها وفائدتها، إن استخدام أي من هذه التقنيات ينبغي ألا يؤثر على سلامة التطبيق والبيانات الخاصة به في الجهة الخاضعة للتدقيق.

وينبغي أن يتم اختيار تقنيات جمع البيانات بناء على تقييم المخاطر الذي قام به فريق التدقيق، وكذلك بناء على الوقت والموارد المتاحة للتدقيق.

تم وضع مصفوفات التدقيق المقترحة لمجالات تدقيق مختلفة من تكنولوجيا المعلومات في الملاحق من الثاني إلى الثامن من هذا الدليل.

الفصل الثاني

حوكمة تكنولوجيا المعلومات

I. ماهي حوكمة تكنولوجيا المعلومات

يمكن اعتبار حوكمة تكنولوجيا المعلومات بأنها الإطار العام الذي يوجه عمليات تكنولوجيا المعلومات في الجهة لضمان تلبية احتياجات العمل في الوقت الحاضر، ويشتمل على خطط للنمو والاحتياجات المستقبلية. وهي تعتبر جزءا لا يتجزأ من مشروع الحوكمة الشامل، حيث تضم قيادات الجهة والهياكل التنظيمية والعمليات والآليات الأخرى (إعداد التقارير والتعقيب عليها، التنفيذ، الموارد وغيره) التي تضمن أن أنظمة تكنولوجيا المعلومات تحافظ على استراتيجية وأهداف الجهة مع تحقيق التوازن بين المخاطر وإدارة الموارد بفعالية.

تلعب حوكمة تقنية المعلومات دوراً رئيسياً في تحديد بيئة الرقابة ووضع الأساس لإنشاء ممارسات سليمة للرقابة الداخلية وإعداد التقارير ليتم الإشراف عليها ومراجعتها من قبل الإدارة.

هناك العديد من المعايير وأطر العمل التي تحدد مبادئ ومفاهيم حوكمة تقنية المعلومات وكيف يمكن للجهة ان تختار طريقة لتنفيذها.

الشكل 2.1 إطار العمل العام لحوكمة تقنية المعلومات

1.1 تحديد الاحتياجات، التوجيه، والمراقبة

تعتبر حوكمة تكنولوجيا المعلومات عنصرا رئيسيا في الحوكمة العامة للجهة. وينبغي النظر إلى حوكمة تكنولوجيا المعلومات على إنها الوسيلة التي يتم من خلالها خلق قيمة تتوافق مع الاستراتيجية العامة لحوكمة الجهات، ولا تعتبر أبداً نظام ضبط بحد ذاتها. وفي حال تبني هذه الطريقة، سيتم إلزام جميع أصحاب المصلحة بالمشاركة في عملية صنع القرار، ومن شأن ذلك خلق قبول مشترك وتحمل مسؤولية النظم الهامة، وكذلك ضمان أن القرارات المتعلقة بتكنولوجيا المعلومات تتم بناء على العمل وليس العكس[29].

29 What is IT Governance and Why is it Important for the IS Auditor: WGITA Into IT Issue 25/8/2007

كي تتمكن حوكمة تكنولوجيا المعلومات من ضمان أن الاستثمار في مجال تكنولوجيا المعلومات يؤدي إلى أعمال أفضل قيمة، وأنه قد تم تخفيف المخاطر التي ترتبط بتكنولوجيا المعلومات، فمن الضروري أن يتم وضع هيكل تنظيمي يتضمن أدوار محددة جيداً للمسؤوليات المتعلقة بالمعلومات، وطريقة سير العمل، والتطبيقات والبنية التحتية.

ومن الضروري أيضا أن تشارك حوكمة تكنولوجيا المعلومات في تحديد احتياجات العمل الجديدة أو المحدثة، ومن ثم توفير الحلول المناسبة لمستخدم تكنولوجيا المعلومات. وخلال عملية التطوير للحل المطلوب أو اقتنائه، تضمن حوكمة تكنولوجيا المعلومات أن الحلول التي تم اختيارها هي استجابة للأعمال المطلوبة وأنه تم توفير التدريب والموارد اللازمة (الأجهزة والأدوات وسعة الشبكة وغيرها) لتنفيذ هذا الحل. ويمكن تنفيذ أعمال المراقبة من خلال التدقيق الداخلي أو مجموعة ضمان الجودة، التي من شأنها أن تقدم تقارير دورية للإدارة حول النتائج التي توصلوا إليها.

فيما يلي وصف للعناصر الرئيسية التي تحدد حوكمة تكنولوجيا المعلومات في الجهة:

II.2 العناصر الرئيسية لحوكمة تكنولوجيا المعلومات[30]

أ- استراتيجية تكنولوجيا المعلومات والتخطيط

تمثل استراتيجية تكنولوجيا المعلومات التوافق المتبادل بين استراتيجية تكنولوجيا المعلومات والأهداف الاستراتيجية للعمل. ينبغي أن تأخذ الأهداف الاستراتيجية لتكنولوجيا المعلومات في الاعتبار الاحتياجات الحالية والمستقبلية للعمل، وقدرة تكنولوجيا المعلومات الحالية على تقديم الخدمات، والموارد المطلوبة[31]. يجب أن تراعي الاستراتيجية كلا من البنية التحتية الحالية لتكنولوجيا المعلومات والاستثمارات، ونموذج التسليم، وتوفير الموارد بما في ذلك الموظفين، ووضع استراتيجية تدمج هذه العناصر في نهج مشترك لدعم أهداف الأعمال.

---

[30] يتم دعم العناصر الرئيسية التي تم عرضها في هذا الفصل (حوكمة تكنولوجيا المعلومات) من قبل إطار عمل COBIT 5 ومعيار ISO 38.500 مع استخدام التعريفات والأمثلة على نطاق واسع.

[31] ISO 38.500

من المهم أن يراجع مدقق تكنولوجيا المعلومات استراتيجية تكنولوجيا المعلومات المطبقة في الجهة لتقييم إلى أي مدى تم إشراك حوكمة تكنولوجيا المعلومات في عملية صنع القرار الخاص بتحديد استراتيجية تكنولوجيا المعلومات.

ب. الهياكل التنظيمية والمعايير والسياسات والعمليات

الهياكل التنظيمية هي عنصر أساسي في حوكمة تكنولوجيا المعلومات لتوضيح أدوار جهات الحوكمة والجهات الإدارية في صنع القرار وفي الأعمال. ينبغي أن يتم تحديد أشخاص مفوضين لصنع القرار ومراقبة الأداء. كما يجب ان يتم دعم الهياكل التنظيمية بالمعايير والسياسات والإجراءات المناسبة، بحيث تعزز القدرة على صنع القرار.

تتأثر الهياكل التنظيمية في جهات القطاع العام من قبل أصحاب المصلحة –أي جميع المجموعات أو المنظمات أو الأعضاء أو الأنظمة الذين تؤثر أو يمكن أن تتأثر بإجراءات الجهة – من الأمثلة على أصحاب المصلحة الخارجيين المهمين البرلمان والكونغرس والجهات الحكومية الأخرى والمواطنين. وتتأثر الهياكل التنظيمية أيضاً بالمستخدمين – داخليين وخارجيين.

المستخدمين الداخليين هم رجال الأعمال، والإدارات العاملة في الجهة، والأفراد ضمن الجهة الذين يتعاملون مع عمليات الجهة. المستخدمين الخارجيين هم الوكالات، والأفراد، والجمهور الذين يستخدمون المنتجات أو الخدمات التي تقدمها الجهة (على سبيل المثال الإدارات الأخرى، والمواطنين، وما إلى ذلك). وتتأثر أيضا الهياكل التنظيمية من مقدمي الخدمات – من شركات، أو وحدات أو أشخاص –سواء من الداخل أو الخارج.

تأتي الحاجة إلى أعمال تكنولوجيا المعلومات من المستخدمين وأصحاب المصلحة. وفي جميع الحالات، يتطلب وجود هياكل تنظيمية وأدوار ومسؤوليات مناسبة للحصول على تفويض حولها من الهيئة الإدارية، ليتم بذلك توفير ملكية واضحة ومساءلة عن القرارات والمهام الهامة. ويجب أن يشمل ذلك العلاقات مع مقدمي خدمات تكنولوجيا المعلومات كطرف ثالث رئيسي[32].

[32] COBIT 5 – Appendix E Mapping of COBIT

ج- عادة ما يشمل الهيكل التنظيمي لتكنولوجيا المعلومات المهام التالية:

اللجنة التوجيهية لتكنولوجيا المعلومات – وتعد الجزء الأساسي من الهيكل التنظيمي. وتضم في عضويتها كبار الموظفين والإدارة العليا وتتحمل مسؤولية المراجعة، والمصادقة، وتوفير الأموال لاستثمارات تكنولوجيا المعلومات. يجب أن يكون للجنة دور توجيهي فعال في وضع القرارات المتعلقة بالأعمال والتي يتم بناء عليها توفير التكنولوجيا لدعم استثمارات العمل وكذلك الموافقة على كيفية الحصول على هذه التكنولوجيا. بشكل عام، قرارات الاستثمار التي تتضمن "بناء الحلول مقابل الشراء" هي من مسؤولية اللجنة التوجيهية لتكنولوجيا المعلومات بعد صدور التوصيات المناسبة من لجان أو مجموعات معينة.

أخيرا، تلعب اللجنة التوجيهية دوراً حاسماً في تعزيز الأمور الضرورية في الشراء وتوفير الدعم الإداري للبرامج التي تنطوي على تغييرات في الجهة.

في الكثير من جهات القطاع العام، تعتبر مهام اللجنة التوجيهية المعنية بتكنولوجيا المعلومات جزءا من وظيفة الإدارة.

المدير التنفيذي للمعلومات (CIO) – هو من كبار الموظفين ومسؤول عن تشغيل وإدارة إمكانيات تكنولوجيا المعلومات المتاحة في الجهة. وفي الكثير من جهات القطاع العام يمكن ان يتم القيام بالمهام التي يقوم بها كبير موظفي تكنولوجيا المعلومات من قبل مجموعة من الموظفين أو من قبل الإدارة التي تتمتع بالمسؤوليات والسلطة والموارد اللازمة.

د- المعايير والسياسات والعمليات

تقوم الجهة بتبني المعايير والسياسات ويتم اعتمادها من الإدارة العليا. حيث تضع هذه السياسات إطارا للعمليات اليومية من أجل تحقيق الأهداف التي وضعتها الإدارة. ويتم دعم السياسات بإجراءات وعمليات تحدد طريقة إنجاز العمل ومراقبته. توضع تلك الأهداف من قبل الإدارة العليا لإنجاز مهام الجهة، وفي الوقت نفسه لتحقيق التوافق مع المتطلبات التنظيمية والقانونية. ويجب أن يتم ابلاغ جميع المستخدمين المعنيين في الجهة بالسياسات والإجراءات المناسبة بصفة دورية.

تشتمل بعض السياسات الرئيسية التي توجه حوكمة تكنولوجيا المعلومات على ما يلي:

- **سياسة الموارد البشرية**

تتناول سياسة الموارد البشرية مهام التعيين والتدريب وإنهاء الخدمات ومهام أخرى تتعلق بتنظيم الموارد البشرية. فهي تتضمن أدوار ومسئوليات مختلف الموظفين في الجهة، بالإضافة إلى المهارات اللازمة أو التدريب المطلوب منهم لتنفيذ مهامهم. وكذلك تحدد سياسة الموارد البشرية الأدوار والمسؤوليات والفصل بين الواجبات.

- **سياسات التوثيق والاحتفاظ بالمستندات**

تعتبر عملية توثيق نظم المعلومات، والتطبيقات، وطبيعة الوظائف، ونظم التقارير، والتقارير الدورية نقطة مرجعية هامة للتوفيق فيما بين عمليات تكنولوجيا المعلومات وأهداف الأعمال. إن السياسات المناسبة للتوثيق والاحتفاظ بالمستندات تتيح إمكانية التتبع وإدارة التغييرات المتكررة في بنية المعلومات في الجهة.

- **سياسة الاستعانة بمصادر خارجية**

غالباً ما يكون الهدف من الاستعانة بالمصادر الخارجية هو منح إدارة الجهة فرصة لتركيز جهودها على أنشطة الأعمال الأساسية. ويمكن أن تكون الحاجة إلى الاستعانة بالمصادر الخارجية بسبب الحاجة إلى تخفيض تكاليف التشغيل. وتضمن سياسة الاستعانة بالمصادر الخارجية أنه قد تم وضع وتنفيذ المقترحات أو المهام أو قاعدة البيانات المتعلقة بالاستعانة بالمصادر الخارجية بطريقة تعود بالفائدة على الجهة.

- **سياسة أمن تكنولوجيا المعلومات**

هذه السياسة تحدد المتطلبات اللازمة لحماية أصول المعلومات، ويمكن الإشارة إلى إجراءات أو أدوات أخرى بشأن طريقة حماية هذه المعلومات. وينبغي أن تكون هذه السياسة متاحة لجميع الموظفين المسؤولين عن أمن المعلومات، بما في ذلك مستخدمي أنظمة الأعمال الذين لديهم دور في حماية المعلومات (مثل سجلات الموظفين والبيانات المالية وغيرها).

II.3 الضوابط الداخلية

الضوابط الداخلية هي عملية تطبيق نظام للضوابط والإجراءات الخاصة لتحديد مدى توافق أنشطة الجهة مع الخطط المعتمدة ومدى الالتزام بها. وفي حال لزم الأمر فانه يتم اتخاذ التدابير التصحيحية اللازمة بحيث يمكن

تحقيق أهداف السياسة العامة. وتحافظ الضوابط الداخلية على إبقاء نظام تكنولوجيا المعلومات في المسار الصحيح. حيث تشمل الضوابط الداخلية إدارة المخاطر، والالتزام بالإجراءات الداخلية والتعليمات والتشريعات والأنظمة الخارجية، والتقارير الدورية والتقارير الخاصة للإدارة، والتحقق من سير العمل ومراجعة الخطط وعمليات التدقيق والتقييم والمراقبة.[33]

أ- إدارة المخاطر[34]

يجب أن تشكل إدارة مخاطر تكنولوجيا المعلومات الجزء الأساسي من استراتيجيات وسياسات إدارة المخاطر للشركة. وتشمل إدارة المخاطر تحديد المخاطر المتعلقة بالتطبيقات الموجودة والبنية التحتية لتكنولوجيا المعلومات، والإدارة المستمرة، بما في ذلك المراجعة السنوية/الدورية والتحديث من قبل إدارة المخاطر ومراقبة استراتيجيات تقليل المخاطر.

ب-آلية الالتزام

تحتاج الجهات إلى وجود آلية للالتزام تضمن تطبيق جميع السياسات والإجراءات. إن ثقافة الجهة أساسا هي التي تثير حساسية جميع الموظفين حول جميع قضايا عدم الالتزام. ويمكن أن تشمل آلية دعم الالتزام أيضاً مجموعة ضمان الجودة، وموظفي الأمن، وأدوات الميكنة وغيرها. ينبغي ان تتم مراجعة تقرير عدم الالتزام من قبل الإدارة المناسبة، ويجب أن يتم التعامل مع قضايا عدم الالتزام الخطيرة أو المتكررة. قد تختار الإدارة التعامل مع عدم الالتزام من خلال التدريب لتجديد المعلومات، أو الإجراءات المعدلة، أو حتى عبر إجراءات تصعيد العقوبة تبعاً لطبيعة عدم الالتزام (مثل انتهاك الأمن، عدم حضور التدريب الإلزامي، وغيرها).

الضمان المستقل الذي يأتي بصورة عمليات تدقيق داخلية أو خارجية (أو مراجعات) يمكن أن يقدم التقييم والملاحظات في الوقت المناسب حول مدى التزام تكنولوجيا المعلومات بسياسات ومعايير وإجراءات الجهة وأهدافها العامة. ويجب أن يتم إجراء عمليات التدقيق هذه بطريقة موضوعية وغير متحيزة، بحيث يتم تزويد المدراء بتقييم عادل لمشروع تكنولوجيا المعلومات الذي خضع للتدقيق.

---

[33] IT Governance in Public Sector: A top priority- WGITA IntoIT Issue 25, August 2007

[34] انظر الفصل السابع حول أمن تكنولوجيا المعلومات لمزيد من التفاصيل

I.4 قرارات الاستثمار (تطوير واقتناء الحلول)

يجب أن توفر حوكمة تكنولوجيا المعلومات لمستخدمي الأعمال برامج تفي بمتطلباتهم الجديدة أو المعدلة. ويمكن أن يتحقق ذلك عن طريق إدارة تكنولوجيا المعلومات سواء كان من خلال تطوير (بناء) البرامج أو الأنظمة الجديدة، أو اقتنائها من الموردين بناء على التكلفة. من أجل تحقيق هذا الأمر بنجاح، عادة ما تتطلب أفضل الممارسات نهجاً نظامياً حيث يتم تحديد الاحتياجات وتحليلها، وتحديد أولوياتها واعتمادها، ويتم تحليل المنفعة مقابل التكلفة بين البرامج المنافسة واختيار البرنامج الأمثل (على سبيل المثال، البرنامج الذي يوازن بين التكلفة والمخاطر).

I.5 عمليات تكنولوجيا المعلومات

عمليات تكنولوجيا المعلومات هي عادة ما تكون مهام التشغيل اليومي للبنية التحتية لتكنولوجيا المعلومات لدعم احتياجات العمل. إن عمليات تكنولوجيا المعلومات التي يتم إدارتها بشكل صحيح تتيح تحديد العقبات، ووضع خطة للتغييرات المتوقعة (أجهزة إضافية أو مصادر شبكة العمل)، وقياس الأداء للتأكد من أنها تلبي احتياجات أصحاب الأعمال المتفق عليها، وتقديم الدعم لإدارة مكتب المساعدة والأحداث العرضية لمستخدمي مصادر تكنولوجيا المعلومات.

I.6 الأشخاص والمصادر

من المستحسن أن تحرص الإدارة على تخصيص مصادر كافية لتكنولوجيا المعلومات لتلبية احتياجات الجهة من خلال عمليات تقييم منتظمة وفقاً للأولويات المتفق عليها وقيود الميزانية. علاوة على ذلك، ينبغي احترام الجانب الإنساني في السياسات والممارسات وقرارات تكنولوجيا المعلومات، والتي يجب أن تراعي الاحتياجات الحالية والمستقبلية للمشاركين في تلك العمليات. كما ينبغي أن تقيم إدارة الحوكمة بانتظام كيف أن استخدام الموارد وتحديد أولوياتها يتم بالشكل الذي تتطلبه أهداف العمل.

II. المخاطر التي تواجه الجهة الخاضعة للتدقيق

يحتاج المدققين إلى فهم وتقييم مختلف مكونات هيكل حوكمة تكنولوجيا المعلومات لتحديد ما إذا كانت قرارات تكنولوجيا المعلومات، والاتجاهات، والمصادر، والإدارة والمراقبة تدعم استراتيجيات وأهداف الجهة. ويحتاج المدقق لتنفيذ التقييم إلى معرفة المكونات الأساسية لحوكمة تكنولوجيا المعلومات والإدارة، كما ينبغي على المدقق أن يكون على بينة بالمخاطر المرتبطة بعدم ملاءمة كل مكون من مكونات الجهة.

تواجه كل جهة تحديات مختلفة في أنواعها وذلك وفق الاختلاف في طبيعتها الفردية والبيئية والسياسية والجغرافية والاقتصادية والاجتماعية. العواقب المذكورة أدناه ليست شاملة لكل شيء إلا أنها تمثل المخاطر والعواقب الشائعة التي قد تنجم عن عدم وجود حوكمة تكنولوجيا معلومات ملائمة.

أ- نظم تكنولوجيا المعلومات غير فعالة أو غير ملائمة للمستخدم:

إن نظم الإدارة العامة التي تهدف إلى خدمة المجتمع والأعمال أو تعزيز الأداء الوظيفي للجهات الحكومية، غالباً ما تكون حلول (برامج) واسعة النطاق ومعقدة. بالتالي، يجب أن يتم تصميمها بشكل صحيح، ووفق الاحتياجات الحقيقية، ومنسقة بكفاءة، وتدار بجدارة. قد تكون حوكمة تكنولوجيا المعلومات الضعيفة على مستوى الحكومة وعلى مستوى الجهات الفردية العقبة الأولى التي تواجه وجود أنظمة تكنولوجيا المعلومات ذات جودة.

ب- مهام تكنولوجيا المعلومات تفتقر وجود التوجيهات ولا تخدم احتياجات قطاع الأعمال:

قد لا يكون هناك قيمة للأعمال كعائد من وراء استثمارات تكنولوجيا المعلومات الكبيرة أو قد تكون قيمة هذه الأعمال قليلة لأنها لا تتماشى استراتيجياً مع أهداف الجهة ومصادرها. إن افتقار وجود التوافق الاستراتيجي هذا يؤدي إلى أن حتى عند جودة تكنولوجيا المعلومات المقدمة فإنها قد لا تسهم في تحقيق الأهداف العامة للجهة بكفاءة وفعالية. وهناك طريقة لضمان وجود التوافق وهي إشراك المستخدمين وأصحاب المصلحة الآخرين الذين يفهمون الأعمال في صنع قرار تكنولوجيا المعلومات.

ج- ضوابط نمو الأعمال:

إن عدم ملاءمة أو عدم وجود تخطيط لتكنولوجيا المعلومات قد يؤدي إلى عرقلة نمو الأعمال بسبب عدم وجود موارد تكنولوجيا المعلومات أو عدم استخدام الموارد المتاحة بكفاءة. وهناك طريقة لتقليل أثر هذه المخاطر وهي أن يكون هناك تحديث دوري لاستراتيجية تكنولوجيا المعلومات، التي من شأنها تحديد الموارد والخطط لتلبية الاحتياجات المستقبلية للعمل.

د- إدارة غير فعالة للموارد:

يجب على الجهة إدارة موارد تكنولوجيا المعلومات على نحو فعال وبكفاءة لتحقيق أفضل النتائج وبأقل التكاليف. حيث يعتبر ضمان وجود ما يكفي من التقنيات، والمعدات، والبرمجيات، والأهم من ذلك وجود الموارد البشرية لتقديم خدمات تكنولوجيا المعلومات العامل الرئيسي في تحقيق القيمة من الاستثمارات في مجال تكنولوجيا المعلومات. كما أن تحديد موارد تكنولوجيا المعلومات ومراقبة استخدامها، يسمح للجهة أن تعرف بشكل موضوعي ما إذا كانت متطلبات الموارد كافية لتلبية احتياجات العمل (على سبيل المثال اتفاقية مستوى الخدمة).

هـ- اتخاذ القرارات غير المناسبة:

قد يؤدي ضعف مستوى هيكل رفع التقارير إلى اتخاذ قرارات غير ملائمة، وقد يؤثر هذا على قدرة العميل على تقديم خدماته، وربما يمنعهم من تحقيق مهامهم. وتساعد اللجان التوجيهية والمجموعات التنظيمية الأخرى، مع وجود التمثيل المناسب، في اتخاذ القرارات التي تؤثر على الجهة.

و – فشل المشروع:

تفشل العديد من الجهات في الانتباه لأهمية حوكمة تكنولوجيا المعلومات. حيث أنها تعمل بمشروعات تكنولوجيا المعلومات دون الفهم الكامل لمتطلبات الجهة بالنسبة للمشروع، وكيفية ربط هذا المشروع بتحقيق أهداف الجهة. وفي ظل عدم وجود هذا الفهم والإدراك ستصبح مشاريع تكنولوجيا المعلومات أكثر عرضة للفشل. من حالات الفشل العامة الأخرى هو اقتناء أو تطوير تطبيقات لا تفي بالحد الأدنى من المعايير الأمنية ومعايير التصميم. قد تتكبد هذه المشاريع تكاليف إضافية لصيانة وإدارة الأنظمة والتطبيقات غير القياسية. يعتبر استخدام دورة حياة تطوير البرمجيات(SDLC) في التطوير أو الاقتناء وسيلة للحد من مخاطر فشل المشروع.

ز – تبعية الطرف الثالث (المورد) :

بما أنه لا توجد عمليات مناسبة لتنظيم عمليتي الاقتناء والاستعانة بالمصادر الخارجية، فقد يؤدي ذلك إلى وضع الجهة في موقف الاعتماد الكلي على مورد واحد أو مقاول واحد. أولاً، تعتبر هذه بيئة عالية المخاطر، حيث في حال خروج المورد من السوق، أو فشله في تقديم الخدمات المتعاقد عليها، عندها ستكون الجهة في موقف صعب. هذا إلى جانب الحالات الأخرى، على سبيل المثال، النزاعات حول الملكية الفكرية، والنظم وقواعد البيانات. قد تحتاج الجهات التي تستعين بالمصادر الخارجية أو تتعاقد بانتظام مع موردين للحصول على خدماتهم إلى وضع سياسة للاستعانة بالمصادر الخارجية أو للاقتناء يتم عبرها تحديد الحالات التي يجوز أو لا يجوز الاستعانة بالمصادر الخارجية بشأنها.

ح – نقص الشفافية والمساءلة :

المساءلة والشفافية هما عنصرين من العناصر الهامة للحوكمة ذات الجودة. وتعتبر الشفافية قوة هائلة، ومتابعة تطبيقها يساعد في محاربة الفساد، وتحسين الحوكمة وتعزيز المساءلة[35]. لذلك، في حال غياب الهياكل التنظيمية والاستراتيجيات والإجراءات والضوابط الرقابية المناسبة، قد تفشل المؤسسة في أن تصبح مسؤولة مسؤولية كاملة وأن تتسم بالشفافية.

[35] ISSAI 20 مفاهيم المساءلة والشفافية، الصفحة 4.

ط- عدم الالتزام بالتشريعات القانونية والتنظيمية:

يطلب أصحاب المصلحة ضمانات كافية بأن الشركات ملتزمة بالقوانين واللوائح وأنها متوافقة مع أفضل الممارسات لحوكمة الشركات في بيئة التشغيل الخاصة بها. وبما أن تكنولوجيا المعلومات أتاحت وجود أعمال سلسة بين الشركات، فقد ظهرت هناك حاجة متزايدة للمساعدة في التأكيد على أن العقود تشمل متطلبات هامة تتعلق بتكنولوجيا المعلومات في مجالات مثل الخصوصية، والسرية، والملكية الفكرية، والأمن (إطار عمل (COBIT 5)، المبدأ 5، والتوافق). يجب أن تشتمل السياسات المختلفة للجهة مثل أمن تكنولوجيا المعلومات، والاستعانة بالمصادر الخارجية، والموارد البشرية، وغيرها على الأطر القانونية والتنظيمية ذات الصلة.

ي- التعرض لمخاطر أمن المعلومات:

قد تنشأ الكثير من المخاطر ذات الصلة بأمن المعلومات نتيجة غياب الهياكل والعمليات والسياسات المناسبة، مثل: اختلاس الأصول، والكشف غير المصرح به للمعلومات، والاطلاع غير المصرح به، والتعرض لهجمات منطقية ومادية، واضطراب المعلومات وعدم توافرها، وإساءة استخدام المعلومات، وعدم الالتزام بقوانين ولوائح البيانات الشخصية، والفشل في استرداد الأوضاع بعد الكوارث. وينبغي أن تحدد السياسة الأمنية لتكنولوجيا المعلومات أصول الجهة (كالبيانات والمعدات ومنهجية الأعمال) التي يجب حمايتها وربطها بالإجراءات، والأدوات، والضوابط على الوصول المادي التي تحمي هذه الأصول.

تستمر حوكمة تكنولوجيا المعلومات في كونها مصدر قلق بالنسبة لمعظم جهات القطاع العام. في الوقت نفسه، العديد من أجهزة الرقابة العليا تركز بشكل متزايد على حوكمة تكنولوجيا المعلومات كجزء من عمليات تدقيق تكنولوجيا المعلومات. يمكن أن يساعد مدققي تكنولوجيا المعلومات حوكمة تكنولوجيا المعلومات عبر ما يلي :

ضمان وجود حوكمة تكنولوجيا المعلومات في جدول أعمال الحوكمة المؤسسية الشاملة، وتعزيز وجود سياسات حوكمة تكنولوجيا المعلومات.

مصفوفة التدقيق

تعتبر مصفوفة التدقيق في الملحق الثاني نقطة انطلاق للمدققين لتقييم الضوابط التي وضعتها الجهة لإدارة المخاطر التي تواجهها في حوكمة تكنولوجيا المعلومات أو تقييم عدم وجودها. وهي تحتوي على المجالات التي تمت مناقشتها أعلاه.

من المهم أن نلاحظ أن موضوعات حوكمة تكنولوجيا المعلومات ستشكل جزءاً من التقييم الشامل الذي يقوم به المدقق لبيئة الرقابة العامة للجهة.

مراجع / للمزيد من الاطلاع:

1. What is IT Governance and why is it important for the IS auditor, WGITA, IntoIT. http://www.intosaiitaudit.org/intoit_articles/25_p30top35.pdf
2. COBIT 4.1 Framework, 2007, IT Governance Institute
3. COBIT 5 Framework, 2012, ISACA
4. ISO/IEC 38500 Corporate Governance of Information Technology
5. OECD Principles of Corporate Governance, OECD, 1999 and 2004
6. Michaels Paul; Anand, Navin; and Iyer, Sudha; What is IT Governance. Computer World UK. April, 2012 http://blogs.computerworlduk.com/management-briefing/2012/04/what-is-it-governance/index.htm
7. http://www.gao.gov/new.items/d04394g.pdf

الفصل الثالث

التطوير والاقتناء

I. ما المقصود بالتطوير والاقتناء

من أجل دعم استراتيجية العمل، تقدم جهات تكنولوجيا المعلومات الحلول (البرامج) للأعمال أو لمستخدمي الأعمال. يجب أن يتم التخطيط لعمليات التطوير، أو الاقتناء، أو التعاقد الخارجي للحصول على الحل (البرنامج) بحيث يمكن إدارة المخاطر وزيادة فرص النجاح. بالإضافة إلى ذلك، ينبغي أن يتم تحديد متطلبات هذه الحلول (البرامج)، وتحليلها، وتوثيقها، وترتيبها من حيث الأهمية. كما يجب على المنظمات أيضاً استخدام ضمان الجودة واختبار الوظائف لضمان جودة هذه الحلول (البرامج).

عادة ما يتم بناء الحلول (البرامج) أو اقتنائها من خلال تشكيل فريق للمشروع. على الرغم من أنه في بعض الأحيان قد لا تضفي الجهات الطابع الرسمي على المشروع، إلا أنه لا بد من إنجاز المهام المتعارف عليها.

ويمكن تقديم الحلول (البرامج) إما عن طريق تطويرها داخلياً أو الحصول عليها من مصدر خارجي من خلال الشراء أو التعاقد أو عملية الاستعانة بمصادر خارجية. في كثير من الأحيان، يتم استخدام وسيلة تجمع بين الوسائل السابقة بحيث يتم تحقيق أكبر قدر من الاستفادة.

وفقاً لتكامل نموذج نضوج المقدرة (CMMI) لجامعة " كارنيجي ميلون" الخاص باقتناء البرامج، الإصدار 1.3، أصبحت الجهات تسعى بصورة متزايدة للحصول على القدرات اللازمة لها حيث أن المنتجات والخدمات متوفرة وجاهزة وعادة ما تكون أرخص من عملية التطوير الداخلية التي تتم في الجهة. ومع ذلك، فإن مخاطر اقتناء المنتجات التي لا تلبي هدف العمل أو تفشل في إرضاء المستخدمين هي واقع فعلي. يجب إدارة هذه المخاطر بشكل جيد لكي تحقق عملية اقتناء او شراء المنتجات أهداف العمل بنجاح. عندما تتم هذه العملية بطريقة منضبطة، فيمكن أن تقوم عملية اقتناء المنتجات بتحسين الكفاءة التشغيلية للجهة من خلال الاستفادة من قدرات الموردين لتقديم حلول ذات جودة بشكل سريع، وبتكلفة أقل، واستخدام التكنولوجيا الأكثر ملاءمة.

بطبيعة الحال تتطلب عملية اقتناء المنتجات أو الحلول أن تكون الجهة على وعي وإدراك باحتياجاتها ومتطلباتها. وينبغي أن تشمل عملية تحديد المتطلبات جميع أصحاب المصلحة المعنيين الذين يشاركون في الأعمال، بما في ذلك المستخدمين النهائيين والموظفين الفنيين الذين سيقومون بصيانة ودعم النظام. عند طلب الخدمات (من مكتب المساعدة، ميكنة العمل، الخ،) يجب أن تشتمل عملية تحديد المتطلبات قسم تكنولوجيا المعلومات التي ستتواصل مع موفر الخدمة. يجب أن يتم ترتيب المتطلبات وفق الأولويات بحيث إذا كان هناك عجز في الميزانية أو قيود أخرى من حيث التكلفة، يمكن أن يتم تأجيل بعض هذه المتطلبات للمستقبل أو أن يتم الحصول عليها او اقتنائها بالشكل المناسب.

إن عملية تحديد المتطلبات ليست سوى الخطوة الأولى في عملية الاقتناء. حيث تتطلب عملية الاقتناء إدارة العديد من المجالات الإضافية، على سبيل المثال، المخاطر، وإدارة البرامج، والاختبار، والإشراف على الموردين سواء خلال عملية الاقتناء وما بعد ذلك في حال كونها تقوم بتشغيل النظام أو تدعمه، وتكامل التدريب الداخلي والأمور المتعلقة بالتنفيذ. توجد طرق معينة لأفضل الممارسات إذا تم استخدامها فإنها ترفع احتمالات النجاح في اقتناء المنتجات أو الخدمات.

I.1 العناصر الأساسية للتطوير والاقتناء:

أ- تحديد وإدارة المتطلبات

للقيام بأي مشروع تطوير او اقتناء، يجب على الجهة أن تقوم بتوثيق المتطلبات المتعلقة بالأمور التي تريدها والتي تحتاجها وأن تقوم بإدارة تلك المتطلبات. تشمل عملية إدارة المتطلبات ترتيبها وفق الأولويات، وذلك بما يتوافق بالشكل الأمثل مع المعايير المستخدمة للترتيب (على سبيل المثال الأهمية، التكلفة، التعقيد)، وتجزئة هذه المتطلبات على مراحل في حالة عدم القدرة على تنفيذها في مهمة واحدة. ينبغي أن تشمل عملية تحديد المتطلبات أصحاب الأعمال، والمستخدمين، وموظفي الدعم والخبراء في المجال، وجميع أصحاب المصلحة المعنيين حسب الحاجة. تشكل المتطلبات أساس طلب استدراج العروض من الموردين، وينبغي أن تكون واضحة ومحددة. من خلال تحليل الاحتياجات وترتيبها من حيث الأولوية، تستطيع الجهة اتخاذ القرارات الخاصة بالتكلفة والمفاضلة للحصول على الحل الأمثل.

ب – إدارة وضبط المشروع

تتضمن إدارة المشروع القيام بتحديد خطة المشروع وضوابطه. كما تتضمن تحديد التكلفة والجدول الزمني الأساسي، وتحديد جداول المشروع الزمنية، وإشراك أصحاب المصلحة في الأنشطة الرئيسية. ضوابط المشروع تتضمن عملية الإشراف وتقديم التقارير الدورية لاتخاذ الإجراءات التصحيحية في حال عدم توافق أداء المشروع مع الخطة. على سبيل المثال، إذا ارتفعت تكلفة المشروع بشكل كبير، قد تلجأ الجهة إلى الغاء بعض وظائف النظام المطلوبة بعد التشاور مع أصحاب المصلحة لاحتواء التكاليف. يجب ان يتم وصف هيكل إدارة المشروع في دورة حياة تطوير النظام (SDLC) أو في استراتيجية الاقتناء التي تم اعتمادها حسب الملائمة. وبشكل عام، يشتمل الهيكل على مدير المشروع، مسئول مخاطر، وضمان الجودة، وفريق دعم إدارة إعدادات النظام، وموظفين من مجموعة الاختبار إن لم يكن ذلك جزءاً من ضمان الجودة وغيرها. تشكل خطة المشروع أساس توجيه جميع الأنشطة. إن تقديم موجز دوري للإدارة العليا يبقيهم على علم بمستجدات المشروع والطريقة التي تدار بها المخاطر. بالإضافة إلى أنه يتيح لهم تقدير الخيارات التي تتعلق بالتكلفة، والجدول الزمني، والأداء حيث أنه من النادر أن يحقق المشروع جميع الأهداف المرجوة في هذه المجالات.

ج – اختبار وضمان الجودة

توفر عملية ضمان الجودة تصوراً لإدارة المشروع والموظفين حول جودة وكفاءة الأعمال المرحلية والنهائية. حيث يقوم الموظفين العاملين في مجال ضمان الجودة بتقييم دوري لمخرجات العمل للتأكد من أنها تتوافق مع معايير الجودة الموثقة لدى الجهة وأن الموظفين قد اتبعوا الإجراءات اللازمة لتطوير المنتجات. تحتاج الجهات إلى التحقق من أن المنتج الذي تم تطويره او اقتناءه يتوافق مع الاحتياجات ومعايير القبول (على سبيل المثال، الأخطاء الغير خطرة تقل عن العدد الذي تم تحديده، الخ) وخضعت لاختبارات بمشاركة المستخدمين وأصحاب المصلحة. كما يجب على موظفي ضمان الجودة التأكد من اتباع المنهج المعتمد والمتفق عليه للتطوير وأنه تم تطبيق الرقابة اللازمة. على سبيل المثال، يجب عليهم التأكيد أنه تم القيام بالمراجعات (الرسمية والغير رسمية) وأنه تم إرسال تقارير الحالة اللازمة لأصحاب المصلحة والإدارة المعنيين. بالإضافة إلى أنه من خلال إشراك موظفي ضمان الجودة، تفرض الإدارة العليا أو تحصل على معلومات حول مدى تطبيق فريق المشروع للسياسات والإجراءات الداخلية المتعلقة بالتطوير أو الاقتناء.

د. استدراج العروض

استدراج العروض هو عملية توثيق متطلبات الأعمال وجمع المواد المرجعية الأخرى التي من شأنها مساعدة المورد في توفير حلول تكنولوجيا المعلومات. ويشمل على إعداد حزمة استدراج العروض وعرضها كمناقصة، وتلقي العروض من ثم الاختيار من بين مختلف الموردين. ينبغي أن تكون عملية الاختيار شفافة وموضوعية وعلى أساس المعايير التي تتناسب مع النظام أو الخدمات التي يتم شراءها. من الضروري قيام فريق المشروع باشراك الإدارة القانونية في هذه العملية. يدرك الفريق القانوني جيداً القوانين واللوائح، ويمكنه المساعدة في ضمان عدالة معايير اختيار الموردين وسيتم تأييدها في المحكمة القانونية في حال طعن الموردين في إرساء العطاء.

هـ – إدارة الاعداد (CM)

يتم استخدام إدارة الاعداد (CM) لضمان المحافظة على سلامة الوثائق، والبرمجيات وغيرها من المواد الوصفية أو مواد الدعم التي هي جزء من النظام. يتم إدارة التغييرات على هذه المواد (وتسمى أيضاً منتجات العمل) ووضع نقاط القياس (أو الاصدارات) بحيث يمكن للجهة الرجوع إلى النسخ المعروفة التي خضعت للاختبارات عند الحاجة. كما يشارك العاملون في إدارة الاعداد في الموافقة أو إعطاء الإذن لتركيب البرمجيات في بيئة الإنتاج. وعادة ما يتم ذلك بعد اختبار المستخدم وأي اختبارات إضافية لازمة لضمان استمرار عمل النظم الأخرى كما في السابق قبل أن يتم تثبيت النظام أو البرنامج الجديد (اختبار التراجع أو اختبار التكامل).

II. المخاطر التي تواجهه الجهة الخاضعة للتدقيق

عندما تقوم الجهة بتطوير البرامج داخلياً هناك عدد من المخاطر أو التحديات التي تواجهها لضمان نجاح المشروع، منها المخاطر المتصلة بالمهارات في مجال البرمجيات، والخبرة في مجال الاختبار وإدارة المشاريع، ووجود تقدير معقول للتكلفة والفوائد العائدة من المشروع، والقدرة على مراقبة وتتبع حالة المشروع.

بالإضافة إلى ذلك، يجب أن تشمل عملية جمع المتطلبات والموافقة عليها للبرنامج أو النظام الأشخاص الذين سيقومون باستخدامها، وسيأخذ المدققين في الاعتبار عما إذا تم تقييم جودة النظام خلال التطوير بشكل

موضوعي من خلال استشارة المستخدمين في تحديد المتطلبات واشراكهم في مجال ضمان الجودة. كذلك في حالة اقتناء البرامج، تحتاج الإدارة بأن يتم اخطارها بشكل دوري على حالة المشروع وان تقوم باتخاذ الإجراءات التصحيحية الملائمة.

في حال التدقيق على جهة قامت باقتناء نظام (أو منتج) يركز المدققين بشكل أساسي على تحديد ما إذا كانت الوكالة تقوم بمتابعة المورد وتحصل على تقارير دورية حول الوضع القائم واتخاذ إجراءات تصحيحية. من أجل القيام بذلك، يجب أن يتضمن العقد تحديد مراحل المشروع الرئيسية أثناء تطوير النظام حيث يكون هناك مراجعات وإعداد تقارير رسمية تزود الجهة بمعلومات حول التكلفة، والجدول الزمني، والأداء. يجب على المدقق التأكيد على أن إدارة الجهة أو الموظفين المعينين قد تلقوا تقارير عن حالة المشروع وأنشطة العقد وأنهم يقومون بالمراجعة واتخاذ الإجراءات التصحيحية اللازمة.

مصفوفة التدقيق

يمكن الاطلاع على مصفوفة التدقيق المتعلقة بهذا القسم في الملحق الثالث.

مراجع / لمزيد من الاطلاع:

1. http://www.dodig.mil/Audit/pmeguide.html
2. DCAA Contract Audit Manual. USA, 2013
3. http://www.dcaa.mil/cam.htm
4. CMMI for Development, Version 1.3
5. http://www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm
6. CMMI for Acquisition, Version 1.3
7. http://www.sei.cmu.edu/library/abstracts/reports/10tr032.cfm
8. ISACA – System Development & Project Management Audit/Assurance Framework
9. COBIT 4.1 Framework, 2007, IT Governance Institute. Acquire and Implement

الفصل الرابع

عمليات تكنولوجيا المعلومات

I. ماهي عمليات تكنولوجيا المعلومات

في حين أن هناك العديد من التفسيرات والتعريفات لعمليات تكنولوجيا المعلومات، إلا إنها ينظر إليها بأنها المهام اليومية التي تتعلق بتشغيل ودعم نظم المعلومات للأعمال مثل (تشغيل الخوادم، والصيانة، وتوفير وسائل التخزين اللازمة، وتشغيل مكتب الدعم وغيرها). يتم قياس العمليات وإدارتها باستخدام مؤشرات الأداء الرئيسية لعمليات تكنولوجيا المعلومات (KPIs) والتي تضع المقاييس التي على أساسها يمكن قياس الفعالية التشغيلية، وعادة ما يتم توثيق ومراجعة هذه المقاييس أو ما يعادلها بصورة دورية. توثق معظم الجهات هذه المقاييس باتفاق بين مستخدمي الأعمال وإدارة تكنولوجيا المعلومات. اتفاقية مستوى الخدمة الداخلية (SLA) هي احدى هذه الاتفاقيات الرسمية، حيث يتم توثيق هذه المقاييس وغيرها من الترتيبات.

II. العناصر الرئيسية لعمليات تكنولوجيا المعلومات

بعض المجالات أو العناصر الخاصة بعمليات تكنولوجيا المعلومات التي يحتاج المدقق أن يأخذها بالاعتبار لتحديد ما إذا كانت الجهة تدير عمليات تكنولوجيا المعلومات بشكل فعال تشتمل العمليات، تصميم الخدمة وتقديمها، وإدارة القدرات والخدمات، وإجراءات التعامل مع الحوادث الطارئة لضمان استمرارية العمليات، والممارسات التي تتعلق بإدارة التغيير.

الشكل 4.1 مجالات عمليات تكنولوجيا المعلومات

يتم تعريف هذه المجالات وغيرها في مكتبة دعم خدمات تكنولوجيا المعلومات (ITIL)[36] والتي تعتبر واحدة من أكثر أطر العمل المعتمدة وعلى نطاق واسع لتحديد وتخطيط وتقديم ودعم خدمات تكنولوجيا المعلومات للأعمال.

لتحديد ما إذا كانت الجهة الخاضعة للرقابة تقدم الخدمات الموثقة بفعالية يجب أن يطلع المدقق على اتفاقية مستوى الخدمة (SLA) التي ينبغي أن تتضمن معايير محددة للخدمات المختلفة. في بعض الأحيان في الجهات الصغيرة يتم اشتمال متطلبات مستوى الخدمة في مخطط العمل أو في وثائق أخرى بدلاً من وجود اتفاقية مستوى الخدمة بين أصحاب الأعمال ومجموعة تكنولوجيا المعلومات. بغض النظر عن اسم الوثيقة، لا بد من توثيقها والمصادقة عليها من قبل أصحاب الأعمال أو المستخدمين وإدارة تكنولوجيا المعلومات.

أ- إدارة استمرارية خدمات تكنولوجيا المعلومات

الغرض من إدارة الاستمرارية هو الحفاظ على المتطلبات المناسبة لاستمرارية الأعمال الجارية. وتحقق إدارة تكنولوجيا المعلومات هذا عن طريق تحديد أهداف زمنية لاسترداد مختلف مكونات تكنولوجيا المعلومات التي تدعم العمليات بناء على الاحتياجات والمتطلبات المتفق عليها. بالإضافة إلى ذلك، إدارة الاستمرارية تشمل المراجعة والتحديث بشكل دوري لأوقات الاسترداد وذلك لضمان توافقها مع خطط استمرارية الأعمال وأولويات العمل. وسوف يتم تناول هذا المجال في مزيد من التفاصيل لاحقاً في الفصل السادس.

ب- إدارة أمن المعلومات

تتعلق إدارة أمن المعلومات بإدارة المخاطر المتعلقة بالأمن، واتخاذ الإجراءات المناسبة، مع ضمان توفر المعلومات عند الحاجة وقابليتها للاستخدام، وكمالها، وأنها غير منقوصة. كما إنها تتعلق أيضاً بضمان إطلاع المستخدمين المخولين فقط على المعلومات، وأن المعلومات محمية عندما يتم نقلها بين المواقع، وموثوق بها عند استلامها. ويتم تناول هذا المجال بمزيد من التفصيل لاحقاً في الفصل السابع.

---

[36] ITIL, http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx

ج – إدارة القدرات

تشتمل إدارة القدرات على إدارة الخدمات المختلفة التي تدعم الأعمال بطريقة تواكب متطلبات العمل أو المستخدمين. زيادة القدرة الإنتاجية لشبكة العمل، وتوافر الموارد، وتحسين وتعزيز التخزين هي أجزاء من إدارة القدرات. من أجل إدارة القدرات تحتاج إدارة تكنولوجيا المعلومات لقياس الظروف الراهنة وتحتاج إلى اتخاذ إجراءات لتسهيل تزويد المستخدمين بقدرات إضافية، على سبيل المثال الحصول على طاقة معالجة إضافية عندما يتم تجاوز معايير معينة (أي عندما يكون الانتفاع من قدرات الكمبيوتر بنسبة 75 ٪ أو أكثر بنسبة 60٪ من يوم العمل). بالإضافة إلى ذلك، بالنسبة لإدارة تكنولوجيا المعلومات التي تقدم الخدمات للأعمال، تكون إدارة القدرات فعالة عندما يتم توزيع موظفي إدارة تكنولوجيا المعلومات المؤهلين والمدربين بصورة مناسبة، واستخدام الموارد الكافية والأدوات المناسبة لمراقبة شبكة العمل ومتابعة وظائف مكتب المساعدة، وأن يشارك الموظفين وبشكل استباقي في معالجة العقبات مع الحفاظ على استجابتهم لاحتياجات العمل.

د – إدارة الحوادث الطارئة والمشاكل

إدارة الحوادث الطارئة هي النظم والممارسات المستخدمة لتحديد ما إذا كان يتم تسجيل الحوادث الطارئة أو الأخطاء وتحليلها وإيجاد الحلول لها في الوقت المناسب. وتهدف إدارة المشاكل إلى حل القضايا من خلال التحقيق والتحليل المتعمق للحوادث الأساسية أو المتكررة من أجل تحديد السبب الجذري لحدوثها. عندما يتم التعرف على المشكلة وإجراء التحليل للوقوف على الأسباب الجذرية لحدوثها، تصبح هذه المشكلة خطأ أو عدم كفاءة معروف، ومن ثم يمكن وضع حل للتصدي لها والحيلولة دون تكرارها في المستقبل. ينبغي أن يتم وضع آلية للكشف عن الظروف التي يمكن أن تؤدي إلى تحديد هذه الحوادث وتوثيقها. يجب أن يحتفظ قسم عمليات تكنولوجيا المعلومات بإجراءات موثقة للكشف عن الظروف غير الطبيعية وتسجيلها. يمكن استخدام سجل يدوي أو سجل آلي لبرامج تكنولوجيا المعلومات المخصصة لتسجيل هذه الحالات. ويمكن أن تشمل الأمثلة على كل من الوصول غير المصرح به للمستخدم أو التسلل (الأمن)، وفشل شبكة العمل (تشغيلي)، وظائف متدنية للبرامج (تقديم الخدمات) أو نقص مهارات المستخدم (التدريب).

هـ- إدارة التغيير

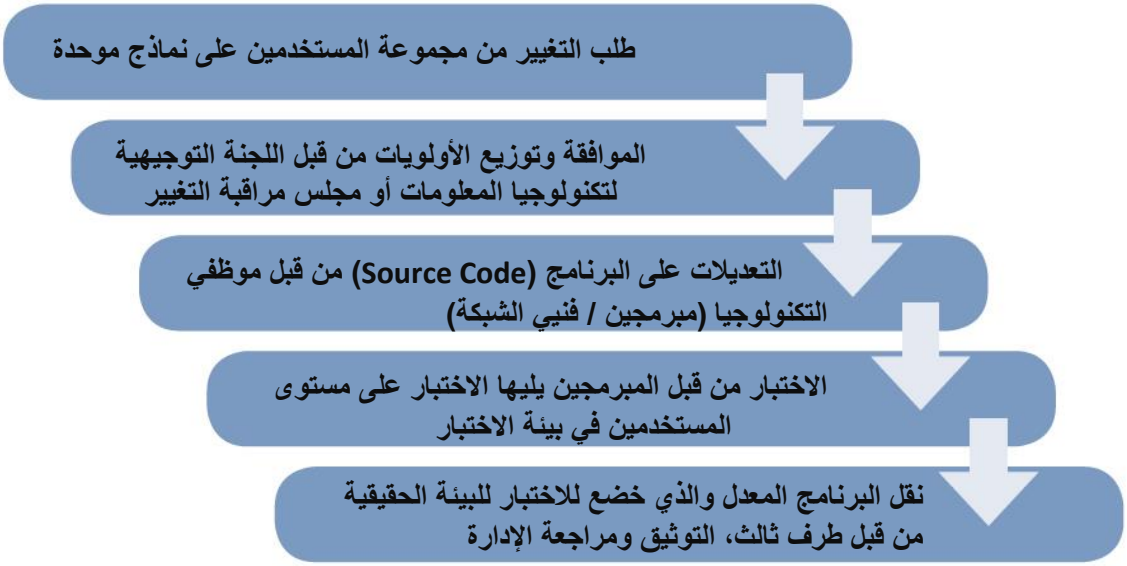
في إدارات تكنولوجيا المعلومات، عادة ما يتم استخدام عملية إدارة التغيير في إدارة وتوجيه التغيرات في الأصول، مثل البرامج والأجهزة، والوثائق ذات الصلة. تنبع الحاجة إلى ضوابط التغيير لضمان وجود التخويل لجميع التغييرات على تكوين النظام، وأن هذه التغييرات تم اختبارها وتوثيقها ومراقبتها بحيث تستمر النظم في دعم الأعمال بالطريقة المخطط لها، وأن هناك سجلات وافية للتغييرات.

يمكن أن يسفر التغيير الغير معتمد أو الغير مقصود عن مخاطر شديدة وعواقب مالية للجهة. يجب على الجهات اتباع إجراءات محددة لإدارة التغيير تتطلب الحصول على موافقة المجلس قبل تطبيقها في البيئة التشغيلية. ينبغي أن تكفل عملية إدارة التغيير تسجيل التغييرات وتقييمها، وأنها مخولة، وتم تحديد أولوياتها، والتخطيط لها، واختبارها، وتنفيذها، وتوثيقها، ومراجعتها وفقاً لإجراءات إدارة التغيير المعتمدة والموثقة.

يمكن أن تبدأ التغييرات على سبيل المثال بسبب تغير بيئة الأعمال، أو تعديل طريقة سير العمل، أو الاحتياجات المتداخلة بين العمليات التشغيلية، أو بسبب نتائج تحليل الحدث الطارئ أو المشكلة. وينبغي أن تشمل إجراءات مراقبة التغيير إجراءات تخويل الإدارة (بناء على معيار الأولية أو عملية التوثيق لتسجيل طلب التغيير (RFC) ؛ من خلال الاختبار والحصول على التخويل من إدارة العمليات قبل استخدامها في البيئة الحقيقية، مراجعة الإدارة لتأثير أي تغييرات، وحفظ السجلات الكافية، وإعداد خطط الاسترجاع (في حالة حدوث أي خطأ)، ووضع إجراءات لإجراء تغييرات في حالات الطوارئ.

تعتبر كل من تكلفة التغيير، والتأثير على نظام تكنولوجيا المعلومات، وأهداف العمل، وتأثير عدم التنفيذ، والاحتياجات المستقبلية من الموارد، عناصر هامة في التخويل بالتغيير وتحديد أولوياته.

التغييرات الطارئة لا يمكن أن تنتظر لتمر بالإجراءات الاعتيادية لمراقبة التغيير، ويجب أن يتم تنفيذها دون أدنى تأخير. هناك وقت قليل متاح للقيام بمثل هذا التغيير واختباره. وقد يؤدي ذلك إلى التعرض لمخاطر أكبر تتمثل في وجود الزلات وأخطاء البرمجة.



الشكل 4.2 خطوات إدارة التغيير

عند وجود إجراءات التغيير في حالات الطوارئ، يجب على المدقق التحقق من ملاءمتها وأنها تحتوي نوعا من أنواع الرقابة. ويشمل هذه على الموافقة على التغيير الطارئ من قبل أحد الموظفين الذي يتمتع بالصلاحيات المناسبة، ولديه اسم الإصدار المناسب إلى جانب سجل التدقيق (استخدام تطبيقات مراقبة التغيير الآلية)، والموافقة بأثر رجعي من المجلس / مالك النظام، والاختبار بأثر رجعي وتحديث الوثائق.

و – اتفاقية مستوى الخدمة (SLA)

توثق اتفاقية مستوى الخدمة مختلف المعايير التي تستخدمها إدارة تكنولوجيا المعلومات لتقديم خدمة للأعمال. عادة ما تتم الموافقة على معايير اتفاقية مستوى الخدمة من قبل أصحاب المصلحة وإدارة تكنولوجيا المعلومات. سوف يستخدم المدقق المعايير المشمولة في اتفاقية مستوى الخدمة لمعرفة ما إذا كانت إدارة تكنولوجيا المعلومات تلبي مستويات الخدمة وعما إذا كان أصحاب المصلحة راضون عن ذلك ويتخذون الإجراءات المناسبة في حالة وجود انحرافات عن معايير مستوى الخدمة المتفق عليها. بشكل عام، هناك أيضا اتفاقية لمستوى الخدمة

أو اتفاقية رسمية أخرى تعقد بين إدارة تكنولوجيا المعلومات والمقاول. على سبيل المثال، قد يكون لإدارة تكنولوجيا المعلومات عدة اتفاقيات لمستوى الخدمة تعقد بينها وبين مختلف المقاولين الذين يقدمون لهم خدمة الاستعانة بمصادر خارجية أو خدمات الحوسبة السحابية. وسنتناول هنا اتفاقية مستوى الخدمة بين إدارة تكنولوجيا المعلومات وعملائها ضمن الجهة.

تتضمن اتفاقية مستوى الخدمة بنود عديدة منها مؤشرات الأداء الرئيسية (KPI) لخدمات تكنولوجيا المعلومات. إن مراجعة مؤشرات الأداء الرئيسية ستساعد المدقق في طرح التساؤلات المتعلقة بما يلي:

- إذا كانت الأنظمة تعمل وفقاً للاتفاقيات الموثقة.
- ما إذا قد تم وضع آليات لتحديد الثغرات في الأداء، ومعالجة الثغرات التي تم تحديدها ومتابعة تنفيذ الإجراءات التصحيحية التي تم اتخاذها نتيجة لتقييم أداء الجهة.
- تحديد قضايا الرقابة في الجهة الخاضعة للتدقيق مما يساعد على تحديد طبيعة وتوقيت ومدى الاختبارات.

على سبيل المثال، مقاييس مؤشرات الأداء الرئيسية والتعاريف والأهداف المقابلة لإدارة التغيير المذكورة أدناه:

العملية	الهدف (عنصر النجاح الهام)	مؤشر الأداء الرئيسي	طريقة القياس
إدارة التغيير	**تقليل الحوادث الناجمة عن التغييرات الغير المصرح بها**	**تخفيض نسبة الحوادث الناجمة عن الدخول غير المصرح به**	**يتم التتبع من خلال إدارة الحوادث، وإدارة التغيير والأعداد المبلغ عنها شهرياً.**

قد تكون هناك حالات حيث تستعين إدارة تكنولوجيا المعلومات بمصادر خارجية وتوكل الجزء الأكبر من مهامها إلى المقاول. في مثل هذه الحالة، تعتبر إدارة تكنولوجيا المعلومات همزة الوصل بين المقاول والمستخدمين وتكون مسؤولة عن التعامل مع المقاول لضمان تلبية احتياجات العمل. وتتوفر إرشادات مفصلة حول تدقيق تكنولوجيا المعلومات الخاص بالاستعانة بمصادر خارجية في الفصل الخامس من الكتيب.

III. المخاطر التي تواجه الجهة الخاضعة للتدقيق

كما لاحظنا من قبل، تعتبر اتفاقية مستوى الخدمة هي الأداة الرئيسية للمدقق. ويتم بذلك تحديد المعايير ومؤشرات الأداء والمتطلبات التي يتم قياس إدارة تكنولوجيا المعلومات وفقها. في حال عدم وجود هذه الوثيقة او عدم مراجعتها رسمياً واعتمادها من قبل أصحاب المصلحة، هناك خطر يتمثل في عدم استخدام مصادر تكنولوجيا المعلومات في الجهة بفعالية وكفاءة. عند تدقيق عمليات تكنولوجيا المعلومات، يحتاج المدقق للحصول على المستند الذي يتضمن تعريف الهدف العام والمعايير الفنية لعمليات تكنولوجيا المعلومات، وعادة ما يكون ذلك في اتفاقية مستوى الخدمة.[37]

في مجال إدارة التغيير، يجب على المدقق التحقق والتأكد من وجود إجراءات لمراقبة التغيير في موضع يضمن سلامة النظام، والتأكيد على استخدام التطبيقات التي تم اختبارها واعتمادها فقط للعمل في البيئة التشغيلية .

وينبغي أيضاً على المدقق الاهتمام بطريقة إدارة الوكالة للقدرات حول كيفية إدارة الوكالة للقدرات (التخزين، وحدة المعالجة المركزية، وموارد الشبكة، الخ) بفعالية لتكون متجاوبة مع المستخدمين، وإدارة الحوادث والقضايا الأمنية الأخرى بحيث لا يتم المساس بوظائف العمل.

---

[37] بعد الحصول على اتفاقية مستوى الخدمة، يحتاج المدقق إلى الحصول على التقارير الدورية من إدارة تكنولوجيا المعلومات التي تقيس المؤشرات وتقدم تقرير عن وضع هذه المؤشرات وكذلك القيام بالمراجعة الإدارية لنفس الإجراءات وأية بنود أو توجيهات لإدارة تكنولوجيا المعلومات عندما تكون هناك انحرافات كبيرة عن المعايير المتفق عليها.

مصفوفة التدقيق

توجد مصفوفة التدقيق لهذا الجزء في الملحق الرابع.

مراجع / للمزيد من الاطلاع:

1. *CISA* Review manual. ISACA. 2011
2. *CISA Item Development Guide.* ISACA.
3. http://www.isaca.org/Certification/Write-an-Exam-Question/ Documents/CISA-Item- Development-Guide.pdf
4. *COBIT 5*, 2012.
5. www.uservices.umn.edu/.../sla/BEST_PRACTICE_Service_Level_Agreement
6. *NIST – Computer Security Incident Handling Guide*
7. http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/ white_paper_c11-458050.pdf
8. ISACA Change Management Audit Assurance Programme
9. ISACA – Security Incident Audit Assurance Programme
10. What is ITIL http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx

الفصل الخامس

الاستعانة بالمصادر الخارجية

I. ما المقصود بالاستعانة بالمصادر الخارجية

الاستعانة بمصادر خارجية هي عملية التعاقد مع جهة خارجية للقيام بأعمال حالية قد قامت بها الجهة داخلياً مسبقاً أو للقيام بوظيفة جديدة. تتحمل الجهة المتعاقد معها مسئولية توفير الخدمات المطلوبة وفق العقد مقابل رسوم متفق عليها. وقد تختار الجهة الاستعانة بمصادر خارجية للقيام بأجزاء مختارة (أو لكافة الاجزاء) من البنية التحتية لتكنولوجيا المعلومات أو الخدمات أو العمليات. وينبغي أن يكون للجهة سياسة أو رؤية حول الجوانب أو وظائف العمل (عادة ما تكون تكنولوجيا المعلومات أو يمكن أن تكون غيرها) التي ستستعين بجهات خارجية للقيام بها والتي سيتم القيام بها داخلياً. وفق أهمية الخدمة التي سيتم تقديمها بالاستعانة بمصادر خارجية، ستقرر الجهة حجم الضوابط الرسمية (أكبر أو أقل) على هذه الخدمة. قد تقرر إدارات تكنولوجيا المعلومات الاستعانة بمصادر خارجية للقيام بكل أو بعض عملياتها وذلك لأن الاستعانة بمصادر خارجية قد يوفر بعض المزايا والتي تشمل ما يلي:

- **مرونة التوظيف**

إن عملية الاستعانة بمصادر خارجية للقيام بالعمليات التي لها مطالب موسمية أو دورية، تتيح جلب موارد إضافية عندما تحتاج الجهة لذلك، وتسريح هذه العمالة عند الانتهاء من العمليات الموسمية.

- **تنمية قدرات الموظفين**

في حال تطلب المشروع لمهارات لا تمتلكها الجهة حالياً، قد تقرر الجهة وقتها الاستعانة بمصادر خارجية للقيام بالمشروع بدلاً من تدريب موظفيها –لتوفير الوقت وتكلفة التدريب. وبهذه الطريقة وعبر الاعتماد على تواجد موظفي المقاول وخبراته الفنية، يمكن لموظفي الجهة الداخليين العمل جنباً إلى جنب مع موظفي المقاول لفترة من الزمن، وبالتالي توفير التدريب العملي لهم.

- **خفض التكاليف**

عادة ما تؤدي الاستعانة بمصادر خارجية إلى خفض التكاليف عن طريق تحويل العمالة والتكاليف الأخرى للمقاول الذي تكون لديه تكلفة العمالة منخفضة. إن إدارات تكنولوجيا المعلومات تستعين بمصادر خارجية لأداء المهام التي من شأنها أن تكون أكثر تكلفة في حال إنجازها داخلياً. على سبيل المثال، عندما تتعلق المهمة ببرامج تتطلب تدريباً خاصاً. إن الجهات التي لا يتوفر لديها الموظفين المؤهلين لإكمال هذه المهمة يمكنها أن تستفيد مالياً من خلال الاستعانة بمصادر خارجية لأداء هذه المهمة. كما أن الاستعانة بمصادر خارجية للقيام بالعمليات غير الأساسية يساعد الإدارة أيضاً على التركيز على أداء أعمالها الأساسية وتحقيق النتائج بكفاءة.

- **الخبراء عند الطلب**

الاستعانة بمصادر خارجية تمكن الجهة من التمتع بخدمة خبراء مستعدون عند الحاجة لتقديم المساعدة على وجه السرعة في المسائل الحالية أو المستجدة. حيث تكون الجهة قادرة على الاستجابة بسرعة للاحتياجات المتغيرة للأعمال (مهمة جديدة أو وظائف إضافية) بمساعدة الخبراء.

- **أمثلة على الاستعانة بمصادر خارجية**

وفقا لورقة بحث جمعية رقابة وتدقيق نظم المعلومات (ISACA) حول الاستعانة بالمصادر الخارجية[38]، يمكن ان تستعين الجهات بمصادر خارجية لمختلف مجالات الأعمال والبنية التحتية لتكنولوجيا المعلومات. منها ما يلي :

- تشغيل البنية التحتية التي قد تشمل مراكز البيانات والعمليات ذات الصلة.
- تشغيل تطبيقات داخلية بواسطة مزود الخدمة.
- تطوير نظم أو صيانة التطبيقات.
- تركيب وصيانة وإدارة أجهزة الحاسب الشخصية وشبكات العمل المرتبطة بها.

---

[38] الاستعانة بمصادر خارجية لتدقيق بيئات تكنولوجيا المعلومات/ برنامج الضمان، 2009

ومن التطورات الحديثة في الاستعانة بالمصادر خارجية هي **الحوسبة السحابية**[39]. في هذه الحالة تستعين الجهة بأجهزة الكمبيوتر المملوكة للمقاول لمعالجة بياناتها. المبدأ هو استضافة المقاول للأجهزة، أي انها تكون في حوزته، في حين أن الجهة الخاضعة للرقابة لا تزال تتمتع بالسيطرة على التطبيقات والبيانات. كما يمكن أن تشمل عملية الاستعانة على استفادة الجهة من أجهزة كمبيوتر المقاول في التخزين والدعم الاحتياطي، والدخول المباشر على البيانات عبر الإنترنت. وتحتاج الجهة إلى أن يكون الدخول إلى الإنترنت فعالا في حال رغبتها بأن يكون لدى موظفيها أو مستخدميها دخول جاهز وسريع على البيانات أو حتى الدخول على التطبيق الذي يعالج البيانات. في البيئة الحالية، تتوفر البيانات أو التطبيقات على معدات نقالة (أجهزة الكمبيوتر المحمولة مع وجود شبكة لاسلكية أو بطاقات الخلوي/ النقال، والهواتف الذكية، والكمبيوتر اللوحي).

تشمل الأمثلة على الحوسبة السحابية تطبيقات البريد الإلكتروني على شبكة الانترنت وتطبيقات الأعمال الشائعة التي يتم الوصول إليها عبر الإنترنت من خلال المتصفح، بدلاً من الكمبيوتر المحلي.

I.1 العناصر الرئيسية للاستعانة بالمصادر الخارجية

أ- سياسة الاستعانة بالمصادر خارجية

تحتاج الجهات إلى سياسات تحدد المهام التي يمكن القيام بها بالاستعانة بمصادر خارجية والمهام التي يجب أن يتم القيام بها داخلياً. عادة ما تستعين الجهات بالمصادر الخارجية للقيام بعمليات تكنولوجيا المعلومات الروتينية والصيانة وأجهزة الكمبيوتر الشخصية. وبشكل عام يتم الاحتفاظ بأعمال الموارد البشرية وسجلات الموظفين كمهام داخلية حيث إنها تتطلب مراقبة دقيقة وتخضع لكثير من متطلبات الخصوصية والأمن، الأمر الذي يجعل الاستعانة بالمصادر الخارجية غير فعالة من حيث التكلفة.

ينبغي أن يبدأ المدقق بالنظر في السياسات والإجراءات المعمول بها عند الاستعانة بالمصادر الخارجية في الجهة الخاضعة للتدقيق. في الجهات الكبرى، والتي غالباً ما يتم القيام بالنصيب الأكبر من عملياتها عبر الاستعانة بمصادر خارجية، يجب أن يكون لديها سياسة معتمدة للاستعانة بمصادر خارجية متضمنة عمليات استدراج عروض تم وضعها بوضوح. وقد لا يكون لدى الجهات الأصغر حجماً سياسة رسمية، ولكنها يجب أن تتبع إجراءات استدراج ذات كفاءة وتتسم بالشفافية.

---

[39] انظر دليل وكتيب مجموعة العمل المعنية بتدقيق تكنولوجيا المعلومات حول تدقيق الحوسبة السحابية.

ب. استدراج العروض

الاستدراج هو عملية توثيق متطلبات النظام وجمع المواد المرجعية الأخرى التي من شأنها مساعدة المقاول في بناء النظام. ويشمل ذلك إعداد المستندات التي سيتم من خلالها استدراج العروض وطرحها للحصول على عطاءات من مقاولين مختلفين ليتم المفاضلة والاختيار فيما بينهم. وينبغي أن تكون عملية الاختيار شفافة وموضوعية وتتم على أساس المعايير التي تتناسب مع النظام أو الخدمات المطلوبة.

ج. إدارة المقاول / العقود

تعد إدارة المقاول عنصراً أساسياً من الاستعانة بمصادر خارجية لضمان تقديم الخدمات وفقاً لتوقعات العميل. وينبغي أن تقوم الجهة الخاضعة للتدقيق بعمليات تضمن بها المتابعة الدورية لحالة المشروع وجودة الخدمة، وتشهد اختبار المنتجات التي تم إعدادها قبل إدخالها في البيئة التشغيلية. بالإضافة إلى ذلك، وكجزء من عملية مراقبة المقاول، يمكن للجهة الخاضعة للتدقيق مراجعة عملية ضمان الجودة الداخلية للمقاول لضمان اتباع موظفي المقاول للسياسات والخطط التي تم اعتمادها تعاقدياً لجميع الأعمال التي يقومون بها.

يجب على المدقق النظر فيما إذا كانت الجهة قد حددت متطلباتها للمهمة التي سيتم القيام بها عبر الاستعانة بمصادر خارجية قبل اختيار المقاول (متطلبات محددة ومقاييس تشغيلية مذكورة في العقد واتفاقية مستوى الخدمة)، وهل تقوم الجهة بمراقبة مدى توافق المقاول مع المتطلبات المنصوص عليها في اتفاقية مستوى الخدمة (عبر تقارير دورية)، وهل اتخذت الجهة الإجراءات اللازمة عند عدم التزام المقاول بالمقاييس الموضحة في اتفاقية مستوى الخدمة (التدابير التصحيحية أو عقوبات الدفع).

د. اتفاقية مستوى الخدمة (SLA)

اتفاقية مستوى الخدمة (SLA) هي اتفاق موثق بين الجهة والمقاول الذي يتم الاستعانة به كمصدر خارجي للقيام بالخدمات وهي أداة رئيسية لإدارة المقاول.

يجب ان تحدد اتفاقية مستوى الخدمة الخدمات التي من المتوقع أن يتم تقديمها إلى جانب المعايير الفنية لهذه الخدمات حيث إنها اتفاق ملزم قانوناً بين المقاول والجهة.

المجالات التي تغطيها اتفاقية مستوى الخدمة تشمل ما يلي :

- أنواع الخدمات التي سوف يتم تنفيذها من قبل المقاول.
- توزيع المسؤوليات بين الجهة والمقاول.
- الخدمات التي سيتم قياسها، فترة القياس، والمدة، والموقع، والجداول الزمنية لإعداد التقارير (معدلات الخلل، وزمن الاستجابة، ساعات موظفي مكتب المساعدة، الخ).
- الوقت لتنفيذ الوظائف الجديدة، مستويات التجديد.
- نوع الوثائق المطلوبة للتطبيقات التي يطورها المقاول.
- موقع تقديم الخدمات.
- معدل تكرار عملية النسخ الاحتياطي ومقاييس استعادة البيانات.
- الإنهاء وأساليب وأشكال تقديم البيانات.
- صيغة بنود الحوافز والعقوبات.

باختصار، يجب أن يتم وضع معظم البنود التي تعتبر هامة للجهة في اتفاقية مستوى الخدمة. ينبغي على مدقق تكنولوجيا المعلومات طلب اتفاقية مستوى الخدمة أو أي وثيقة أخرى (عقد أو اتفاق رسمي) التي تم بها توثيق هذه المعايير، والتأكيد على توافق تقارير المقاول حول المعايير المختلفة مع المتطلبات أو أن الجهة قد اتخذت الإجراءات التصحيحية اللازمة لمعالجة أوجه القصور.

هـ. تحقيق المنفعة

عادة ما تستعين الجهات الخاضعة للتدقيق بمصادر خارجية لتحقيق وفورات في التكاليف. حيث يتم تحقيق هذه الوفورات عندما تكون تكلفة تقديم هذه الخدمات من قبل المقاول أقل من تكلفة تقديمها من خلال استخدام الأيدي العاملة والبنية التحتية في الجهة. وهناك فوائد أخرى لا يمكن قياسها مباشرة، مثل الاستفادة من البنية التحتية للمقاول في التوسع السريع في نطاق مستوى الخدمة أو استخدام خبراتهم للحالات الخاصة. وكلما أمكن ذلك، يجب على الجهة أن تحاول وتحدد ما إذا كانت الوفورات المتوقعة يتم تحقيقها على أساس دوري. ويعد هذا الأمر أحد عناصر البيانات التي يتم استخدامها لاتخاذ القرار بخصوص استمرار أو وقف الاستعانة بالمصادر خارجية.

و. الأمن

عندما يتم الاستعانة بمصادر خارجية لقواعد البيانات وإدارتها، يجب على إدارة تكنولوجيا المعلومات تقييم ما إذا كان للمقاولين ممارسات أمنية قوية كافية، وعما إذا كان المقاولين قادرين على تلبية المتطلبات الأمنية الداخلية. بينما تجد معظم إدارات تكنولوجيا المعلومات الممارسات الأمنية للمقاول ممتازة (فهي غالباً ما تتجاوز الممارسات الداخلية)، إلا أن خطر الخروقات الأمنية أو حماية الملكية الفكرية يتزايد كون أنه قد تم الاستعانة بمصادر خارجية للتعامل مع البيانات. من جانب آخر، يجب أيضا معالجة الأمور المتعلقة بالخصوصية وذلك لوجود مسائل أمنية اخرى مثل سوء الإدارة أو الكشف عن البيانات الحساسة، أو الوصول غير المصرح به إلى البيانات والتطبيقات وخطة استرداد الأوضاع بعد الكوارث. وعلى الرغم من أنه من النادر أن تشكل هذه القضايا العقبات الرئيسية للاستعانة بالمصادر الخارجية، إلا أنه يجب أن يتم توثيق المتطلبات.

II. المخاطر التي تتعرض لها الجهة الخاضعة للتدقيق

أ. الاحتفاظ بالمعرفة المتعلقة بالأعمال وملكية منهجية الأعمال

هناك خطر ملازم وهو خسارة المعرفة المتعلقة بالأعمال، الذي يتواجد ضمن مطوري التطبيقات. إذا كان المقاول، ولأي سبب، غير قادر على توفير هذه الخدمة، يجب أن تكون الإدارات الحكومية لتكنولوجيا المعلومات على استعداد لتولي هذه المهمة مرة أخرى. وبما أنه سيتم تطوير التطبيق خارج الجهة، فإن الجهة تتعرض أيضاً لخطر التخلي عن أو فقدان ملكية منهجية الأعمال، والتي قد يطالب بها مقدم الخدمة على انها من ملكية فكرية خاصة به. يجب على الجهات معالجة هذه المسألة وقت الدخول في العقد، والتأكيد على امتلاكها الوثائق الكاملة الخاصة بعملية تطوير النظام وكذلك تصميمه. ومن شأن هذا مساعدة الجهة في تبديل مقدم الخدمة، إذا لزم الأمر.

ب. فشل المقاول في التسليم

في بعض الأحيان قد يفشل المقاول في تسليم المنتج وقد يعود سبب ذلك إما لعدم التسليم في الوقت المحدد أو أن المنتج غير صالح ويجب التخلي عنه لعدم اشتماله على الوظائف الصحيحة. إذا لم يتم تنفيذ عملية استدراج

العروض بشكل صحيح هناك احتمال كبير بعدم توافق النظام أو الخدمات التي يتم تحصيلها مع احتياجات المستخدمين، أو سوف تكون دون المستوى، أو ستكون التكلفة مرتفعة، أو ستحتاج موارد كبيرة للصيانة والتشغيل أو قد تكون ذات جودة منخفضة وتحتاج إلى الاستبدال في المستقبل القريب. إن العقد الضعيف، والنظام المعيب وعدم جودة عملية اختيار المقاولين، وعدم وضوح المراحل وظروف السوق الغير المواتية هي بعض الأسباب الشائعة لفشل المقاول.

تحتاج إدارات تكنولوجيا المعلومات لوجود خطط للطوارئ لمثل هذا الحدث. عند النظر في الاستعانة بمصادر خارجية، ينبغي على إدارات تكنولوجيا المعلومات تقييم الآثار المترتبة على فشل المقاول (على سبيل المثال، هل للفشل انعكاسات بليغة على أداء الأعمال؟). إن توافر وثائق تفصيلية حول تصميم النظام، وتطوير النظام يساعد الجهة في ضمان استمرارية الأعمال من خلال مقدم خدمة آخر أو أن يقوموا بالعمل بأنفسهم.

ج. التغيير في نطاق العمل

تتضمن جميع عقود الاستعانة بمصادر خارجية الخطوط الأساسية والافتراضات. في حال اختلاف العمل الفعلي عن التقديرات، يتحمل العميل دفع الفرق. هذه الحقيقة البسيطة أصبحت عقبة رئيسية بالنسبة لإدارات تكنولوجيا المعلومات التي تفاجأت بعدم ثبات السعر أو أن المقاول يتوقع أن يتم الدفع له عن إجراءات التغييرات الإضافية. معظم المشاريع تتغير بنسبة 10–15٪ من حيث المواصفات خلال دورة التطوير.

د. معدل دوران الموظفين الرئيسيين

النمو السريع فيما بين مقدمي خدمة الاستعانة بمصادر خارجية أدى إلى خلق سوق عمل ديناميكي. عادة ما يكون هناك طلب على الموظفين الرئيسيين في المشاريع البارزة الجديدة، أو أحياناً يكون هناك خطر تعيينهم من قبل شركات أخرى من الخارج. في حين أن الشركات الخارجية غالبا ما تستعرض احصائيات لمعدل دوران قد يظهر منخفض نسبيا إلا أن الإحصائية الأهم هي تلك التي توضح إدارة الشركة لمعدل دوران الموظفين الرئيسيين. عادة ما تكون معدلات الدوران المقبولة في حدود 15–20٪، وإعداد الشروط التعاقدية حول تلك المستويات هو طلب معقول.

هـ. المخاطر الخارجية (خارج الدولة)

توظيف مقدمي الخدمة من خارج الدولة هو شكل شائع من أشكال الاستعانة بالمصادر خارجية، وخصوصاً في بيئة الحوسبة السحابية. في هذا السيناريو، فإن مخاطر الاستعانة بالمصادر الخارجية تتعلق بالقوانين الأجنبية حول تخزين ونقل المعلومات والذي قد يحد مما يمكن تخزينه وطريقة معالجته، كما أنه يمكن أن يتم استخدام البيانات من قبل الجهات القانونية في البلد الأجنبي دون علم الجهة، وقد لا تكون معايير الخصوصية والمعايير الأمنية متناسبة، ولا يمكن تجنب النزاعات بسبب النظم القانونية المختلفة بالكامل.

مصفوفة التدقيق

يمكن الاطلاع على مصفوفة التدقيق لهذا القسم في الملحق الخامس.

المراجع / للمزيد من الاطلاع:

1. Davison, Dean. Top 10 Risks of Offshore Outsourcing. 2003. http://www.zdnet.com/news/top-10-risks-of-offshore-outsourcing/299274
2. Outsourced IT Environments Audit /Assurance Program, 2009. ISACA. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ Outsourced-IT-Environments-Audit-Assurance-Program.aspx
3. Governance of Outsourcing. ISACA, 2005. http://www.isaca.org/Knowledge-Center/Research/Documents/Outsourcing.pdf
4. Guideline on Service Agreements: Essential Elements Treasury Board of Canada Secretariat www.tbs-sct.gc.ca
5. NIST SP 500-292, Cloud Computing Reference Architecture
6. NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing.

الفصل السادس

خطة استمرارية الأعمال (BCP)

وخطة استعادة الأوضاع بعد الكوارث (DRP)

I. ماهي خطة استمرارية الأعمال وخطة استعادة الأوضاع بعد الكوارث

أصبحت الجهات الحكومية تعتمد بشكل متزايد على مدى توافر أنظمة الكمبيوتر والعمليات الصحيحة الخاصة بها من أجل الوفاء بالتزاماتها القانونية. تلعب أنظمة الكمبيوتر دوراً هاماً في مثل هذه الأنشطة المتنوعة مثل التقييم وجمع الضرائب والعائدات الجمركية؛ ودفع المعاشات التقاعدية للدولة واستحقاقات الضمان الاجتماعي؛ وفي معالجة الإحصاءات الوطنية (المواليد والوفيات، والجريمة، والأمراض، وغيرها). في الواقع، هناك العديد من الأنشطة التي لا يمكن القيام بها على نحو فعال دون دعم من أجهزة الكمبيوتر.

فقدان الطاقة، والإجراءات الصناعية، والحرائق، والتلف والضرر يمكن أن تكون جميعها لها آثار كارثية على أنظمة الكمبيوتر. قد يستغرق الأمر عدة أسابيع لتستأنف الجهة أعمالها بفعالية في حال عدم وجود خطة استمرارية الأعمال قابلة للتطبيق.

إن مصطلح خطة استمرارية العمل وخطة استعادة الأوضاع بعد الكوارث تستخدم في بعض الأحيان بشكل مترادف، ولكنهما في الواقع مصطلحين مختلفين ولكن متكاملين. كلاهما مهم لمدقق تكنولوجيا المعلومات، وذلك لأنها معاً يضمنان قدرة الجهة على العمل بمستوى محدد من القدرات عند حدوث عطل بأسباب من الطبيعة أو من صنع الإنسان. فيما يلي توضيح للمصطلحين:

- **التخطيط لاستمرارية الأعمال (BCP)** هو عملية تستخدمها الجهة لتخطيط واختبار استعادة أعمالها واختبارها بعد التعطل. كما أن المصطلح يصف طريقة استمرار الجهة بالعمل تحت الظروف المعاكسة التي قد تنشأ (على سبيل المثال، الكوارث الطبيعية أو غيرها).
- **التخطيط لاستعادة الأوضاع بعد الكوارث (DRP)** هي عملية التخطيط لاسترداد البنية التحتية لتكنولوجيا المعلومات واختبارها بعد وقوع كارثة طبيعية أو غيرها. وهي جزء من عملية تخطيط استمرارية الأعمال (BCP). يتم تطبيق تخطيط استمرارية الأعمال على وظائف الأعمال التنظيمية بينما يتم تطبيق التخطيط لاستعادة الأوضاع بعد الكوارث على موارد تكنولوجيا المعلومات التي تدعم وظائف العمل.

يعالج التخطيط لاستمرارية الأعمال قدرة الجهة على مواصلة العمل عندما تتعطل العمليات الاعتيادية. تتضمن هذه الخطة السياسات والإجراءات والممارسات التي تسمح للجهة لاستعادة واستئناف العمليات ذات المهام الحرجة اليدوية والآلية بعد وقوع الكارثة أو الأزمة. إلى جانب تبيان الممارسات التي يجب اتباعها في حالة التوقف، تشمل بعض عمليات تخطيط استمرارية الأعمال (BCP) مكونات أخرى مثل استعادة الأوضاع بعد الكوارث، والاستجابة في حالات الطوارئ، واسترداد بيانات المستخدم، وأنشطة الطوارئ وإدارة الأزمات. وعلى هذا النحو، في هذه الجهات، تعتبر استمرارية الأعمال مصطلح شامل يغطي كل من استعادة الأوضاع بعد الكوارث واستئناف الاعمال.

مع ذلك، سواء كان ذلك جزءاً من تخطيط استمرارية الأعمال BCP أو عملية منفصلة، ينبغي أن تحدد عمليات التخطيط لاستعادة الأوضاع بعد الكوارث DRPs الموارد، والإجراءات، والمهام والبيانات اللازمة لإدارة عملية استعادة الأوضاع للجهة في حال توقف الأعمال. يجب أن تساعد هذه الخطة الشركة على استرداد عمليات الأعمال المتضررة، من خلال تحديد خطوات معينة للشركة يجب أن تعمل بها عند لاستعادة الأوضاع. وعلى وجه التحديد، يتم استخدام التخطيط لاستعادة الأوضاع بعد الكوارث لعمليات الإعداد والتخطيط المتقدمة اللازمة لتقليل الأضرار الناجمة عن الكوارث وضمان توافر نظم المعلومات الهامة للجهة. فمن حيث تكنولوجيا

المعلومات، تعالج عمليات التخطيط لاستعادة الأوضاع بعد الكوارث عملية استرداد الأصول التكنولوجية الهامة، بما في ذلك النظم، والتطبيقات، وقواعد البيانات، وأجهزة التخزين، والمصادر الأخرى للشبكة.[40]

I.1 العناصر الرئيسية لعمليات التخطيط لاستمرارية الأعمال واستعادة الأوضاع بعد الكوارث

إن مدقق تكنولوجيا المعلومات مطالب بتقييم برامج إدارة استمرارية الأعمال للجهة، والذي يشتمل على تقييم خطط استعادة الأوضاع بعد الكوارث واستمرارية الأعمال، ونظم إدارة الأزمات. ويحتاج المدقق للقيام بذلك إلى فهم الأمور المتعلقة في تطوير استراتيجية إدارة استمرارية الأعمال، والخطوات التي ينبغي اتخاذها لتقييم فعالية البرامج الحالية التي تتضمن العمليات اللازمة من استمرارية الأعمال واستعادة الأوضاع بعد الكوارث، وجهود إدارة الأزمات.

إن التخطيط الفعال للاستمرارية يتألف من عدة مراحل مشتركة بين جميع نظم المعلومات. الخطوات العامة لذلك كما يلي[41]:

1. خطة وسياسة استمرارية العمل.
2. تنظيم وظيفة استمرارية الأعمال.
3. تقييم تأثير الأعمال (BIA) وإدارة المخاطر.
4. الضوابط الوقائية بما في ذلك الضوابط البيئية.
5. خطة استعادة الأوضاع بعد الكوارث.
6. توثيق خطة استمرارية الاعمال.
7. اختبار الخطة والتدريب.

---

[40] The IT Auditor's Role in Business Continuity Management, IIA Publication http://www.theiia.org/intAuditor/itaudit/archives/2008/january/the-it-auditors-role-in-business-continuity-management

[41] NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems, provide guidance on the contingency planning processes

8. تطبيق الأمن خلال تنفيذ خطة استمرارية الأعمال (BCP) وخطة استعادة الأوضاع بعد الكوارث (DRP).
9. النسخ الاحتياطي واستعادة الأوضاع بعد الكوارث لخدمات الاستعانة بمصادر خارجية.

وتمثل هذه الخطوات العناصر الرئيسية في القدرة الشاملة للتخطيط لاستمرارية الأعمال. فيما يلي شرح العناصر:

أ. سياسة استمرارية الأعمال، والخطة، والتنظيم

يبدأ التخطيط الفعال للاستمرارية بوضع سياسة لاستمرارية العمل في الجهة. يقدم فريق إدارة استمرارية الأعمال[42] جميع الوظائف الملائمة للأعمال كما يلعب دوراً مهماً في نجاح خطة استمرارية العمل للجهة. ينبغي أن تحدد سياسة التخطيط لاستمرار الأعمال الأهداف الشاملة للاستمرارية في الجهة، ووضع المسؤوليات وإطار العمل التنظيمي لتخطيط الاستمرارية.

ب. إنشاء وظيفة استمرارية الأعمال

يجب أن يتم تنظيم فريق إدارة استمرارية الأعمال من حيث تقديم جميع وظائف العمل المناسبة لتحقيق النجاح. كما يجب على الإدارة العليا والمسؤولين الأخرين دعم برنامج الاستمرارية وربطه بعملية وضع السياسة. ينبغي تحديد الأدوار والمسؤوليات بشكل واضح في الفريق.

ج. تقييم التأثير على الأعمال وإدارة المخاطر

i. تقييم أهمية وحساسية العمليات المحوسبة وتحديد الموارد الداعمة

في أي جهة، تعتبر استمرارية عمليات معينة أكثر أهمية من استمرار غيرها من العمليات، ولا يعتبر توفير نفس المستوى من الاستمرارية لجميع العمليات أمر مقبول من حيث التكلفة. لهذا السبب، من المهم أن تحدد

---

[42] سيتم شرحها في القسم التالي.

الجهة العمليات الهامة والمصادر التي تحتاج للاسترداد والدعم. ويتم ذلك عبر إجراء تقييم للمخاطر، وتحديد التهديدات المحتملة وتأثيراتها على معلومات الجهة والموارد ذات الصلة بما في ذلك البيانات، وبرامج التطبيقات، والعمليات. وينبغي أن يشمل تقييم المخاطر والتأثيرات جميع المجالات الوظيفية. بالتالي ينبغي أن يتم اتخاذ قرار بشأن المخاطر المتبقية حيث أن تأثير التهديد المحتمل قليل أو أن أنظمة التحكم كافية لتسليط الضوء على مثل هذه الحالات في الوقت المناسب.

ii. تحديد وترتيب أولويات البيانات والعمليات الهامة

ينبغي تحديد أهمية وحساسية البيانات والعمليات المختلفة وتحديد أولوياتها على أساس التصنيف الأمني والتقييم الشامل للمخاطر التي قد تواجه عمليات الجهة. يجب أن يكون مثل هذا التقييم للمخاطر بمثابة الأساس للخطة الأمنية للجهة. وتشمل العوامل التي ينبغي أخذها في الاعتبار أهمية وحساسية البيانات والأصول التنظيمية الأخرى، وتكلفة عدم استعادة البيانات أو العمليات بالسرعة المناسبة. على سبيل المثال، انقطاع ليوم واحد في النظم الرئيسية لجمع الرسوم والضريبة، أو فقدان البيانات ذات الصلة قد يؤدي إلى بطء أو وقف استلام الإيرادات، وتقليل الرقابة على ملايين الدولارات في الإيصالات، والحد من ثقة الجمهور. على نحو معاكس، قد يتعطل نظام مراقبة تدريب الموظفين ربما لعدة أشهر دون التسبب في عواقب وخيمة.

عموماً، ينبغي تحديد وتصنيف البيانات والعمليات الهامة من قبل الموظفين المشاركين في عمليات البرامج أو أعمال في الجهة. ومن المهم أيضاً الحصول على موافقة الإدارة العليا على هذه القرارات، وكذلك موافقة الأشخاص المتضررين.

ينبغي أن تتم مراجعة قائمة الأولويات لمصادر المعلومات الهامة والعمليات بصورة دورية لتحديد ما إذا كانت تعكس الظروف الحالية. يجب ان تتم مثل هذه المراجعات عندما يكون هناك تغيير كبير في عمليات ومهمة الجهة أو في موقع أو تصميم الأنظمة التي تدعم هذه العمليات.

iii. تحديد المصادر التي تدعم العمليات الهامة

عندما يتم تحديد البيانات والعمليات الهامة، ينبغي أن يتم تحديد الحد الأدنى من المصادر اللازمة لتقديم الدعم وتحليل أدوارها. وتشمل المصادر التي يتعين النظر فيها موارد الكمبيوتر، مثل الأجهزة والبرمجيات، وملفات البيانات، وشبكات العمل، بما في ذلك أجهزة التوجيه (router)، وحوائط الحماية (firewalls)، والإمدادات، بما في ذلك مخزون الورق والنماذج المطبوعة مسبقاً، وخدمات الاتصالات، وأية موارد أخرى تعتبر ضرورية للعملية، مثل الأفراد، والمرافق واللوازم المكتبية، والسجلات الغير محوسبة.

لأنه من المحتمل أن يتم إدارة أو حفظ الموارد الأساسية من قبل مجموعات متنوعة في الجهة، فمن المهم أن يدعم كل من البرنامج وأمن المعلومات عمل الموظفين بشكل جماعي لتحديد الموارد اللازمة للعمليات الهامة.

iv. تحديد أولويات معالجة حالات الطوارئ

بالتزامن مع تحديد وترتيب الوظائف الهامة، ينبغي على الجهة أن تضع خطة لاسترداد العمليات الهامة. يجب أن تحدد الخطة بوضوح الترتيب الذي بناء عليه يتم استعادة جوانب المعالجة، من هو المسؤول، وماهي المعدات الداعمة والموارد الأخرى اللازمة. أن وجود خطة تم وضعها بعناية لإعادة المعالجة يمكن أن تساعد الموظفين على الشروع في عملية الاستعادة على الفور، وتحقيق الاستخدام الأمثل لموارد الكمبيوتر المحدودة في حالات الطوارئ. وينبغي أن يشارك كل من مستخدمي النظام وموظفي دعم أمن المعلومات في تحديد أولويات معالجة حالات الطوارئ.

v. منع وتقليل التوقف والأضرار المحتملة

هناك عدد من الخطوات التي يجب أن تأخذها الجهة في الاعتبار لمنع أو تقليل الأضرار التي قد تلحق بالعمليات الآلية والتي يمكن أن تقع نتيجة لحوادث غير متوقعة. ويمكن تصنيفها على النحو التالي :

- التكرار الروتيني أو النسخ الاحتياطي لملفات البيانات، وبرامج الكمبيوتر، والوثائق الهامة أثناء التخزين خارج الموقع؛ وأيضا تكرار التنظيم لمرافق النسخ الاحتياطي البعيدة والتي يمكن استخدامها في حالة تلف المرافق المعتادة للجهة ولا يمكن استخدامها.

- بناء القدرات لاسترداد نظام المعلومات وإعادة تكوينه حيث يمكن استرداد نظام المعلومات وإعادته إلى حالته الأصلية بعد التوقف أو الفشل.
- تركيب الضوابط البيئية، مثل نظم إخماد الحرائق أو إمدادات الطاقة الاحتياطية.
- التأكيد على فهم الموظفين ومستخدمي النظم الأخرى لمسؤولياتهم أثناء حالات الطوارئ.
- الصيانة الفعالة للأجهزة، وإدارة المشاكل، وإدارة التغيير.

vi. تنفيذ إجراءات النسخ الاحتياطي للبيانات والبرنامج

النسخ الروتيني لملفات البيانات والبرمجيات وتخزينها في مكان بعيد آمن، عادةً ما يكون أكثر الإجراءات فعالية من حيث التكلفة ويمكن أن تتخذها الجهة للتخفيف من اضرار انقطاع الخدمة. على الرغم من أن الاستعداد لاستبدال المعدات في كثير من الأحيان يتم بسهولة، إلا أن التكاليف يمكن أن تكون كبيرة، وإعادة تكوين ملفات البيانات التي تم معالجتها، واستبدال البرمجيات قد تكون عملية مكلفة وتستغرق وقتاً طويلاً. في الواقع، لا يمكن دائماً إعادة تكوين ملفات البيانات. بالإضافة إلى التكاليف المباشرة لإعادة تكوين الملفات والحصول على البرمجيات، يمكن أن يؤدي انقطاع الخدمات المعنية إلى خسائر مالية كبيرة.

vii. التدريب

ينبغي أن يتم تدريب الموظفين وأن يكونوا على علم بمسؤولياتهم لمنع وتخفيف الضرر والاستجابة في حالات الطوارئ. على سبيل المثال، يجب على موظفي دعم أمن المعلومات تلقي تدريب دوري على التعامل مع حالات الحرائق، والمياه، وأجهزة الانذار، وكذلك التعرف على مسؤولياتهم الخاصة في بدء تشغيل الموقع البديل لمعالجة البيانات. في حال كون المستخدمين الخارجيين طرف هام في عمليات الجهة، فإنه يجب أن يتم إبلاغهم بالخطوات التي يتم اتخاذها في حالة الطوارئ.

viii. خطط لصيانة الأجهزة، وإدارة المشاكل، وإدارة التغيير

يمكن أن يحدث الانقطاع الغير متوقع للخدمة نتيجة أعطال في المعدات أو نتيجة لتغيير المعدات دون إخطار مسبق يتم توجيهه لمستخدمي النظام بفترة كافية. لمنع حدوث مثل هذه الحوادث يتطلب الأمر وجود برنامج فعال للصيانة، وإدارة المشاكل، وإدارة التغيير لمعدات الأجهزة.

د. الضوابط الوقائية والبيئية

تمنع الضوابط البيئية وتحد من الأضرار المحتملة في المرافق وانقطاع في الخدمة. فيما يلي أمثلة على الضوابط البيئية:

- طفايات الحريق ونظم مكافحة الحريق.
- أجهزة إنذار الحريق.
- كاشفات الدخان.
- كاشفات المياه.
- الإضاءة في حالات الطوارئ.
- تجهيز نظم تبريد هواء احتياطية.
- المولدات الاحتياطية للطاقة.
- وجود وإجراءات وصمامات إيقاف لأي من خطوط السباكة التي قد تعرض مرافق المعالجة للخطر.
- بناء مرافق المعالجة بمواد مقاومة للحريق ومصممة للحد من انتشار الحريق.
- سياسات تحظر الأكل والشرب والتدخين داخل مرافق الكمبيوتر.

يمكن أن تقلل الضوابط البيئية من الخسائر الناجمة عن بعض الانقطاعات مثل الحرائق، أو منع الحوادث عن طريق الكشف عن المشاكل المحتملة في وقت مبكر، مثل تسرب الماء أو الدخان، بحيث يمكن معالجتها. يمكن أيضاً أن تتحمل إمدادات الطاقة غير المنقطعة (UPS) أو المولدات الاحتياطية للطاقة عملية تزويد الجهة بالطاقة عند انقطاع التيار الكهربائي لفترة قصيرة أو توفير الوقت لعمل نسخة احتياطية من البيانات وإجراء عمليات إغلاق منظمة خلال انقطاع التيار الكهربائي لفترة طويلة.

هـ. خطة استعادة الأوضاع بعد الكوارث

ينبغي وضع خطة لاستعادة الأوضاع بعد الكوارث لاستعادة التطبيقات الهامة؛ وهذا يشمل الترتيبات اللازمة لمرافق المعالجة البديلة في حالة تضرر المرافق المعتادة بشكل كبير أو في حال عدم التمكن من الوصول إليها. تحدد السياسات والإجراءات على مستوى الجهة عملية التخطيط لاستعادة الأوضاع ومتطلبات التوثيق. علاوة على ذلك، يجب أن توضح الخطة التي تم وضعها على نطاق الجهة النظم الهامة، والتطبيقات، وأية خطط تابعة أو ذات الصلة. من المهم أن يتم توثيق هذه الخطط بشكل واضح، وتوصيلها إلى الموظفين المتأثرين، وتحديثها لتعكس العمليات الحالية.

i. توثيق خطة حديثة لاستعادة الأوضاع

يجب توثيق خطط استعادة الأوضاع بعد الكوارث، واعتمادها من إدارتي أمن الأعمال وأمن المعلومات، وإبلاغ الموظفين المتأثرين بذلك. وينبغي أن تعكس الخطة المخاطر والأولويات التشغيلية التي حددتها الجهة. كما يجب أن يتم تصميم الخطة بحيث لا تتجاوز تكاليف التخطيط لاستعادة الأوضاع التكاليف المرتبطة بالمخاطر التي تهدف الخطة إلى تقليلها. وينبغي أيضاً أن تكون الخطة تفصيلية وموثقة بصورة مناسبة بحيث لا يعتمد نجاحها على معرفة أو خبرة شخص أو شخصين .

يجب أن يتم توفير نسخ متعددة من خطة الاستمرارية، وتخزين بعضها خارج الموقع لضمان عدم تدميرها من قبل نفس الأحداث التي دمرت مرافق معالجة البيانات الأولية.

ii. ترتيبات الموقع البديل

اعتماداً على درجة استمرارية الخدمة المطلوبة، ستتراوح الخيارات للمواقع أو المرافق البديلة من موقع مجهز على استعداد لتقديم خدمة الدعم الاحتياطي الفوري، ويشار إليه "hot site"، إلى موقع غير مجهز سيأخذ بعض الوقت للتحضير للعمليات، ويشار إليه "cold site". وبالإضافة إلى ذلك، يمكن أن يتم الترتيب المسبق مع الموردين بخصوص أنواع مختلفة من الخدمات. ويشمل ذلك على إجراء الترتيبات مع موردي أجهزة الكمبيوتر وخدمات الاتصالات وكذلك مع موردي مختلف الخدمات وغيرها مثل اللوازم المكتبية.

و. الاختبار

i. الاختبار الدوري لخطة الاستمرارية

يعتبر اختبار خطط الاستمرارية أمرا ضروريا لتحديد ما إذا كانت هذه الخطط ستعمل على النحو المنشود في حالة الطوارئ. يجب أن يكشف الاختبار عن نقاط الضعف الهامة في الخطط، مثل مرافق الدعم الاحتياطي التي لا يمكنها إجراء العمليات الهامة بنفس كفاءة العمليات الأصلية كما كان متوقعاً. تحتاج هذه الخطط إلى إجراء التحسينات عليها من خلال عمليات الاختبار.

تختلف فترات تكرار إجراء الاختبار لخطة الاستمرارية تبعاً لمدى أهمية عمليات الجهة. بصورة عامة، ينبغي اختبار خطط الاستمرارية للوظائف المهمة بشكل كامل مرة واحدة كل سنة أو سنتين، وكلما تم إجراء تغييرات هامة على الخطة، أو عند حدوث تدوير للأشخاص الرئيسيين فيها. فمن المهم للإدارة العليا أن يتم تقييم مخاطر مشكلات خطة الاستمرارية، ووضع وتوثيق سياسة حول فترات تكرار هذه الاختبارات ومداها.

ii. تحديث خطة الاستمرارية بناء على نتائج الاختبار

توفر نتائج اختبار الاستمرارية مقاييس هامة لدراسة جدوى خطة الاستمرارية. وإبلاغ الإدارة العليا بذلك بحيث يتم تحديد الحاجة للتعديل وإجراء الاختبارات الإضافية، وأن تكون الإدارة العليا على بينة من مخاطر الاستمرار في العمل دون خطة استمرارية ملائمة.

ز. الأمن

ينبغي أن يتم تضمين أمن الموارد والعمليات في خطة استمرارية الأعمال حيث تتعرض البيانات الهامة، وبرامج التطبيق، والعمليات والموارد للضياع بسهولة عند الكوارث أو إجراء نشاط إدارة استمرارية الأعمال. على سبيل المثال، خلال النسخ الاحتياطي للبيانات، فإن انعدام الأمن يمكن أن يؤدي إلى وجود نسخ مكررة وتسرب البيانات الهامة. في الوقت نفسه، فإنه من الممكن أن يتم ضياع البيانات التي تم نسخها احتياطياً أثناء عملية النسخ (البيانات التي يتم نسخها من خادم المعاملات إلى خادم النسخ الاحتياطية).

ح. النسخ الاحتياطي واستعادة البيانات لخدمات الاستعانة بالمصادر الخارجية

تستعين العديد من الجهات بمصادر خارجية لأداء أنشطتها أو جزء منها ويسمى بمزود الخدمة. بما أن مزود الخدمة سينفذ العمليات اليومية والضوابط، فمن الضروري أن تؤكد الجهة على تضمين خطة استمرارية الأعمال واستعادة الأوضاع بعد الكوارث في العقد. وأن تقوم الجهة بمراقبة مزود الخدمة والتأكيد على جهوزيته لاستمرارية الأعمال واستعادة الأوضاع بعد الكوارث، ويشمل هذا جهوزيته من الناحية الأمنية أيضا. قد تحتاج الجهة إلى التأكيد على محافظة مزود الخدمة على سرية البيانات وبرامج التطبيقات التي يحتفظ بها. وينبغي على الجهة الاحتفاظ بملكية منهجية الأعمال. يجب أن يكون للجهة خطة للاستمرارية لضمان استمرارية أعمال مزود الخدمة إذا انتهت أعماله أو إذا تم الاستحواذ عليه من قبل شركة أخرى.

II. المخاطر التي تتعرض لها الجهة الخاضعة للتدقيق

الخدمات أو المنتجات الأساسية هي تلك التي يجب أن يتم تقديمها لضمان البقاء وتجنب التسبب في الخسارة، والالتزام بالضوابط القانونية وغيرها في الجهة. تعتبر كل من العناصر الرئيسية لتخطيط استمرارية الأعمال (BCP) وعمليات التخطيط لاستعادة الأوضاع بعد الكوارث (DRPs) عملية تخطيط مسبق تؤكد على قدرة منهجية الأعمال والبنية التحتية لتكنولوجيا المعلومات في الجهة على دعم احتياجات المهام التي تخلف وقوع الكارثة أو أي خلل آخر. تخدم الجهات الحكومية العديد من الاحتياجات الهامة (كالمدفوعات للمواطنين، وتوفير الرعاية الصحية، والتعليم، والدفاع، والخدمات الأخرى التي يعتمد عليها المواطنين). في حال توقف هذه الخدمات لفترات طويلة من الزمن، سوف يؤدي ذلك إلى خسائر مالية وغيرها. يجب على المدققين التأكد من وجود خطط لاستمرارية الأعمال (BCP) ولاستعادة الأوضاع بعد الكوارث (DRPs) في جميع الجهات الحكومية، وضمان قدرة الجهة على الاستمرار في خدمة المواطنين.

عند تقييم قدرة عمليات التخطيط استمرارية الأعمال (BCP) وعمليات التخطيط لاستعادة الأوضاع بعد الكوارث (DRPs) على ضمان وحماية موثوقية واستمرارية البنية التحتية لتكنولوجيا المعلومات وعمليات الأعمال، هناك بعض المخاطر المتعلقة بالتدقيق والتي يمكن للمدقق أن يركز عليها. ويشمل ذلك أن تقوم خطط استعادة الأوضاع بعد الكوارث واستمرارية العمل بتغطية جميع المجالات الوظيفية الهامة. وفي حال عدم تغطية خطة استعادة الأوضاع بعد الكوارث لمجال وظيفي مهم، ستكون استمرارية العمل في خطر. وقد

تصبح خطة الاستمرارية غير فعالة وإن كانت جيدة عند عدم وضوح الأدوار والمسؤوليات وعدم فهم الموظفين المعنيين لها.

تعتبر إجراءات تقييم آثار الأعمال، والضوابط الوقائية والبيئية، والتوثيق، واختبار خطة الاستمرارية، وتدريب الموظفين المعنيين، كلها دعم للتنفيذ الفعال لخطة استمرارية العمل في الجهة. وإن القصور في الجوانب الأمنية في تنفيذ خطة استمرارية العمل وخطة استعادة الأوضاع بعد الكوارث قد يؤدي إلى خطر فقدان البيانات، وفقدان الوقت الثمين وغيرها من التكاليف بسبب العملية غير الفعالة لاستعادة الوضع بعد وقوع كارثة.

عند الاستعانة بمصادر خارجية لتقديم الخدمات تنشأ منطقة خطر جلية لا تكون فيها خطة استمرارية الأعمال (BCP) وخطة استعادة الأوضاع بعد الكوارث (DRPs) تحت سيطرة الجهة بالكامل. فهناك مخاطر يجب ان تتم معالجتها مثل أمن البيانات، وفقدان البيانات، والتعامل مع البيانات من قبل غير المرخص لهم بذلك، وتسرب البيانات. كما إن استمرارية الخدمة ذاتها من خلال مزود الخدمة تشكل خطراً في حد ذاته سواءً كان ذلك من خلال فقدان المعرفة بالأعمال أو ملكية العمليات وبالتالي عدم القدرة على تغيير مزود الخدمة في حالة القصور في الأداء، وفي حالات أخرى إنهاء الخدمة أو استحواذ جهات أخرى على مزود الخدمة.

مصفوفة التدقيق

يمكن الاطلاع على مصفوفة التدقيق لهذا القسم في الملحق السادس.

المراجع:

1. GAO Federal Information Systems Audit Manual (FISCAM)
2. COBIT 4.1 Framework, 2007, IT Governance Institute
3. NIST Contingency Planning Guide for Federal Information Systems, Special Publication 800-34
4. The IT Auditor’s Role in Business Continuity Management, Internal Auditor, January 2008 edition.

الفصل السابع

أمن المعلومات

I. ما المقصود بأمن نظم المعلومات؟

يمكن تعريف أمن المعلومات بأنه قدرة النظام على حماية المعلومات وموارد النظام فيما يتعلق بالسرية والسلامة. كما أنها تشمل حماية المعلومات ونظم المعلومات من الوصول غير المصرح به أو تعديل المعلومات، سواء في التخزين، أو المعالجة، أو النقل، وتشمل كذلك ضمان عدم انقطاع الخدمة عن المستخدمين المعتمدين. ويشمل أمن المعلومات تلك التدابير اللازمة للكشف عن مثل هذه التهديدات وتوثيقها ومواجهتها. يتيح أمن المعلومات للجهة حماية البنية التحتية لنظم المعلومات من المستخدمين غير المصرح بهم. ويضم أمن المعلومات كل من أمن الكمبيوتر وأمن الاتصالات.

ومن الجوانب الأساسية لحوكمة تكنولوجيا المعلومات هو أمن المعلومات لضمان **التوافر والسرية والتكامل** – والتي يعتمد عليها كل شيء. يعتبر أمن المعلومات بمثابة حارس البوابة الذي يحمي الأصول المعلوماتية في الجهة. ويدعو ذلك إلى وجود برنامج أمن المعلومات لحماية البيانات وفي ذات الوقت يمكن الجهة من تحقيق أهدافها وأعمالها مع تحمل مستوى مقبول من المخاطر عند القيام بذلك. إن توفير المعلومات لأولئك الأشخاص الذين ينبغي أن تصلهم أمر مهم كأهمية حمايتها من أولئك الذين لا ينبغي أن تصلهم هذه المعلومات. يجب ان يمكن الأمن عملية أداء الأعمال ودعم أهدافها بدلاً من أن يصبح خدمة لمصالح ذاتية.

I.1 أهمية أمن المعلومات

تتزايد أهمية أمن المعلومات بالنسبة للمؤسسات الحكومية حيث أن الترابط بين شبكات العمل العامة والخاصة وتبادل مصادر المعلومات زاد من تعقيد التحكم في الوصول لهذه المعلومات والحفاظ على السرية والسلامة وتوافر البيانات.

نظم المعلومات هي تجمعات معقدة تجمع التكنولوجيا، والعمليات، والاشخاص الذين يعملون بتعاون لتأدية أعمال المعالجة، والتخزين، ونقل المعلومات حتى يتم دعم مهمة الجهة ووظائف أعمالها. لذلك، من الضروري أن تضع كل جهة برنامج أمن المعلومات.

إن الهدف من برنامج أمن نظم المعلومات هو حماية معلومات الجهة عن طريق الحد من خطر فقدان السرية والسلامة وتوافر تلك المعلومات إلى المستوى المقبول. إذا لم يكن لدى الجهة ضماناً لأمن المعلومات فإنها سوف تتعرض للمخاطر والتهديدات المحتملة لعمليات الجهة، وتحقيق أهدافها العامة، مما يؤثر في نهاية المطاف على مصداقية الجهة.

بتزايد إمكانيات تكنولوجيا المعلومات وتعقيدها ودورها، أصبح أمن المعلومات موضوعاً متزايد الأهمية بالنسبة لعمليات تدقيق تكنولوجيا المعلومات. بل هو عامل حاسم من أنشطة الجهات، حيث أن نقاط الضعف في أمن المعلومات قد يؤدي إلى أضرار جسيمة في النواحي التالية:

- **القانون** – انتهاكات قانونية وتنظيمية.
- **السمعة** –أضرار تلحق بمكانة الجهة، مما يتسبب في خرق الثقة مع الجهات الأخرى أو تشويه صورة الحكومة أو الدولة.
- **التمويل** –على سبيل المثال الغرامات والتعويضات وانخفاض المبيعات، وتكاليف الإصلاح والإستعادة.
- **الإنتاجية** –الحد من الفعالية أو الكفاءة في مشروع أو برنامج أو خدمة كاملة تقدمها الجهة.
- **وجود ثغرات (عدم حصانة)** – الوصول إلى النظم والبيانات بطريقة غير مصرح بها الأمر الذي يجعلها عرضة للبرامج الضارة وإتاحة المجال لمزيد من الاختراقات.

فيما يلي ما قد يكون السبب لهذا الضرر:

- انتهاكات الأمن، سواء التي تم كشفها والتي لم يتم كشفها.
- الاتصالات الخارجية غير المصرح بها بمواقع بعيدة.
- كشف المعلومات –الكشف عن أصول الشركات والمعلومات الحساسة إلى أطراف غير المصرح لهم بالاطلاع.

I.2 تشكيل ثقافة أمن المعلومات

أحد مقومات نجاح برامج أمن المعلومات في الجهة هو خلق الثقافات التنظيمية التي تعالج القضايا الأمنية. للتصدي بشكل موحد لهذه القضايا وغيرها في جهة كبيرة، ينبغي اتباع نموذج عمل لأمن المعلومات[43]. وتتضمن العناصر ما يلي:

- **خلق الوعي الأمني:** يتكون هذا من أنشطة عامة لزيادة الوعي حول المعلومات الأمنية ودورات تعليمية موجهة للموظفين. تعتبر هذه الدورات فرصة جيدة للبدء في تعريفهم بمسئولياتهم فيما يتعلق بأمن المعلومات. وقد تكون مهمة الموارد البشرية أن تتحمل مسؤولية التدريب وتعزيز الوعي الأولي لدى الموظفين الجدد. يجب استمرار التدريب خلال فترة عمل الموظفين حتى النهاية حيث ينبغي تعزيز الوعي الأمني دائماً.

- **المطالبة بالتزام الإدارة:** يعتبر التزام الإدارة ميزة داعمة في تشكيل ثقافة أمن المعلومات. لا يكون التزام الإدارة من خلال إعداد الوثائق الرسمية حول السياسات الأمنية فقط، ولكن من خلال المشاركة بفعالية أيضا. في حالة عدم وجود دعم فعلي لبرنامج أمن المعلومات من قبل الإدارة، فإن ذلك قد يتسبب في ضعف إحساس أي موظف آخر بالالتزام أو المسؤولية اتجاه البرنامج. لذلك من المهم أن تقبل الإدارة ملكية أمن المعلومات وتقديم الدعم الكامل للبرنامج.

- **بناء قاعدة تنسيق صلبة من خلال تشكيل فرق متعددة الوظائف:** بما أن أمن المعلومات يتضمن العديد من جوانب الجهة التي تتطلب التنسيق، فإنه ينبغي النظر إلى تشكيل فرق متعددة الوظائف مما يشجع على التواصل والتعاون ويقلل من عزلة الإدارات وتكرار الجهود.

---

[43] ISACA Business Model for Information Security, 2010.

تعتبر عملية انشاء ثقافة أمن المعلومات جزءا لا يتجزأ من تنفيذ الحوكمة في نظم معلومات الجهة، وتتميز بما يلي:

- **التوفيق فيما بين أمن المعلومات وأهداف الأعمال:** من الضروري أن يتم التوافق فيما بين أمن المعلومات وأهداف الأعمال حيث أنها تمكن وتدعم أهداف الأعمال. يتوافق برنامج أمن المعلومات مع الجهة، ويتطلب أن تكون ضوابط أمن المعلومات ضوابط عملية وتقلل من المخاطر بصورة فعلية وقابلة للقياس.

- **تقييم المخاطر:** يجب استكمال تطبيق أمن المعلومات من خلال تقييم المخاطر، لتحديد شكل الضوابط المطلوبة. غالباً ما يتم تجاهل تقييم المخاطر، مما يؤدي إلى انخفاض مستوى حماية البنية التحتية والمعلومات الحساسة، أو في بعض الحالات التسبب في المبالغة في الحماية. سوف يساعد تطبيق تقييم المخاطر الإدارة على تحديد الضوابط المناسبة لتخفيف المخاطر بشكل فعال.

وتشمل عملية تقييم المخاطر تحديد وتحليل ما يلي :

- ❖ جميع الأصول والعمليات المرتبطة بالنظام.
- ❖ التهديدات المحتملة التي يمكن أن تؤثر على السرية أو السلامة أو توافر النظام.
- ❖ نقاط ضعف النظام والتهديدات المرتبطة.
- ❖ التأثيرات المحتملة والمخاطر الناجمة عن أنشطة التهديد.
- ❖ متطلبات الحماية للتخفيف من المخاطر.
- ❖ اختيار التدابير الأمنية المناسبة وتحليل علاقات المخاطر.

- **تحقيق التوازن بين الجهة، والأفراد، والعمليات، والتكنولوجيا:** يتطلب أمن المعلومات الفعال الدعم التنظيمي والموظفين المؤهلين، والعمليات الفعالة، واختيار التكنولوجيا المناسبة. يتفاعل كل عنصر مع آخر ينتمي لمجال مختلف، ويؤثر ويدعم العناصر الأخرى، وغالباً ما يكون ذلك بطرق معقدة، لذلك لا بد من تحقيق التوازن فيما بين هذه العناصر. وفي حال نقص أحد العناصر فإن ذلك يضعف من أمن المعلومات.

I.3 العناصر الرئيسية لأمن المعلومات

أ. بيئة أمن المعلومات

هناك بعض العناصر الحاسمة التي يجب أن تتحقق لدعم التنفيذ الناجح لأمن المعلومات على نحو فعال. وهي كالتالي:

- **الحفاظ على السرية** وهي المحافظة على الضوابط المرخصة للوصول إلى المعلومات والكشف عنها، بما في ذلك وسائل لحماية الخصوصية الشخصية والمعلومات السرية. يعتبر جانب الحفاظ على السرية جانب مهم جداً لأنه يتعلق بمسائل الخصوصية التي يجب أن تكون مشروطة. لاستمرار المحافظة على ذلك، يجب أن يضمن النظام احتفاظ كل فرد بحق السيطرة على المعلومات التي يتم جمعها، وكيف يتم استخدامها، ومن الذي يستخدمها، وما هو الغرض الذي تستخدم من اجله.

- **السلامة** وهي المحافظة على المعلومات من التغيير بشكل خاطئ أو التدمير، وذلك يشمل التأكد من عدم الإنكار والأصالة[44]. للتصديق على سلامة المعلومات، فإن استخدام آلية للمصادقة يعتبر ضروريا للتحقق من صحة هوية المستخدمين. كما أنه ينبغي أن تكون عملية التأكد من أن المعلومات التي تم إنشاؤها أو إرسالها متوافقة مع متطلبات عدم الإنكار[45].

- **التوافر** هو التأكيد على توافر جميع نظم المعلومات بما في ذلك الأجهزة وشبكات الاتصالات، وتطبيقات البرمجيات والبيانات التي في حوزتها للمستخدمين وذلك في الأوقات اللازمة لتنفيذ أنشطة العمل. كما ينبغي أن تكفل الوصول إلى المعلومات واستخدامها في الوقت المناسب وبطريقة يمكن الاعتماد عليها. إلا أن الالتزام بمبدأ الأمن لاستخدام الأجهزة، وشبكات الاتصالات، وتطبيقات البرمجيات، واستخدام حق الوصول إلى البيانات سيتطلب سياسة رقابة للوصول إلى المعلومات. إن الهدف من رقابة الوصول إلى البيانات هو لضمان وصول المستخدمين إلى تلك المصادر والخدمات التي يحق لهم الوصول إليها فقط، وعدم رفض المستخدمين المؤهلين من الوصول إلى الخدمات التي يحق لهم استلامها شرعياً.

---

[44] الأصالة هي امتلاك صفة الحقيقة والقدرة على التحقق من صحتها والوثوق بها؛ الثقة من صحة النقل، أو الرسالة، أو رسالة المنشئ. قد لا تعد الأصالة ضرورية لتقييم السلامة لتحقيق هدف التدقيق.

[45] عدم الإنكار هو ضمان استلام المرسل للمعلومات إثبات بالتسليم واستلام المتلقي إثبات بهوية المرسل، بحيث لا يستطيع أي طرف منهما إنكار ذلك لاحقاً بعد معالجة المعلومات. لا يعتبر عدم الإنكار ضروريا لتقييم سلامة تحقيق هدف التدقيق.

أمن المعلومات هو تقليل التعرض للمخاطر بناء على إدارة المخاطر في جميع مجالات حوكمة تقنية المعلومات. قد يتسبب الفشل في تنفيذ ورصد عمليات التخفيف من المخاطر في منطقة واحدة أضرارا في الجهة بأكملها. حتى لو كان من المعروف، وعلى نطاق واسع، أن الإدارة الفعالة لمخاطر أمن المعلومات أمر ضروري لسلامة الجهة، إلا أنه غالباً ما يتم التغاضي عن هذه المخاطر أو عدم تحديث احتياطات السلامة للاستجابة للظروف المتغيرة.

تغطي مناقشة أمن المعلومات في الجهات المجالات التالية:

ب. تقييم المخاطر

تقييم المخاطر هي عملية تحديد وتحليل وتقييم المخاطر في البنية التحتية الأمنية لتكنولوجيا المعلومات وتقييم المخاطر ذات الصلة بالأمن من التهديدات الداخلية والخارجية للجهة، وأصولها، وموظفيها.

ج. سياسة الأمن

السياسة الأمنية للجهة هي مجموعة من القوانين والقواعد والممارسات التي تنظم طريقة الجهة في إدارة وحماية، وتوزيع الموارد لتحقيق الأهداف الأمنية المحددة. يجب أن تحدد هذه القوانين والقواعد والممارسات المعايير لسلطات الأفراد المعنيين، وقد تحدد الشروط التي يتم بموجبها السماح للأفراد بممارسة سلطاتهم. ولتكون ذات معنى، فإنه يجب أن تمنح هذه القوانين والقواعد والممارسات الأفراد المقدرة على تحديد ما إذا كانت إجراءاتهم تنتهك السياسة أو تمتثل لها.

فيما يلي الشكل الموصى به لسياسة أمن تقنية المعلومات:

عناصر سياسة أمن تكنولوجيا المعلومات	تعريف أمن المعلومات – الأهداف والنطاق (بما في ذلك سرية البيانات).
	متطلبات الالتزام ومعايير ومبادئ الأمن بالتفصيل. • ينبغي ألا يملك موظفي إدارة تكنولوجيا المعلومات المسؤوليات التنفيذية أو المحاسبة.
	تعريف المسؤوليات العامة والخاصة لجميع جوانب أمن المعلومات.
	استخدام أصول المعلومات والوصول إلى البريد الإلكتروني، وشبكة الانترنت.
	صيغة وطريقة الوصول.
	إجراءات النسخ الاحتياطي.
	إجراءات للتعامل مع البرامج الخبيثة.
	عناصر التعليم والتدريب الأمني.
	عملية الإبلاغ عن الحوادث الأمنية المشتبه بها.
	خطط استمرارية العمل.
	أساليب إبلاغ الموظفين بالسياسة والإجراءات المعتمدة لأمن نظم المعلومات.

د. تنظيم أمن تكنولوجيا المعلومات

يعنى تنظيم أمن تكنولوجيا المعلومات بتنفيذ السياسة الأمنية في الجهة. ويمكن أن يوكل هذا العمل لوحدة أو أشخاص يستعينون بإدارة تكنولوجيا المعلومات للحصول على الأدوات المناسبة، وإجراء العمليات الملائمة لتنفيذ السياسة الأمنية بفعالية. كما تقع على عاتقهم مسئولية تنظيم الدورات التدريبية المبدئية والدورية للموظفين ومعالجة الحوادث الأمنية. وهناك أيضا حاجة للتأكد من أن البيانات الخاصة بالجهة التي يتم نقلها أو الدخول إليها من قبل الجهات الخارجية آمنة قدر الإمكان. ويجب على المدقق التأكد أن الجهة الخارجية قادرة على تنفيذ شروط أمن المعلومات كما هو موثق.

هـ. إدارة الاتصالات والعمليات

يتعين على الجهة متابعة العمليات والاجراءات المستخدمة في الأعمال. وتضم عملية المتابعة مجموعة من الإجراءات والعمليات التنظيمية التي تضمن المعالجة السليمة للبيانات في الجهات. وهذا يشمل توثيق الإجراءات للتعامل مع وسائل التخزين ومعالجة البيانات، وإجراءات الطوارئ، وأمن التسجيل في الشبكة، والإجراءات الاحتياطية.

و. إدارة الأصول

إدارة الأصول بمعناها العام، تشير إلى أي نظام يقوم بمتابعة الممتلكات ذات القيمة لجهة أو مجموعة ويحافظ عليها. فإدارة الأصول هي عملية منهجية لتشغيل، والحفاظ على، وتطوير، والتخلص من الأصول بفعالية من حيث التكلفة.

بالنسبة لتكنولوجيا المعلومات، تشمل إدارة الأصول الحفاظ على جرد دقيق لمعدات تكنولوجيا المعلومات، ومعرفة تراخيص المعدات ذات الصلة، وصيانة وحماية المعدات (مخزن آمن، وغرفة تحكم، الخ). كما تشمل إدارة أصول تكنولوجيا المعلومات إدارة البرامج ووثائق العمليات القيمة بالنسبة للجهة.

بالنسبة للجهات الحكومية، تعد إدارة الأصول هامة جدا في ظل البيئة المالية الحالية بسبب القيود المالية التي قد لا تسمح باستبدال الأصول المفقودة أو المسروقة بطريقة معقولة. وإضافة إلى ذلك، فإن الجهة قد تكون في خطر إذا لم يتوفر لديها جرد كامل بأصولها عندما تحتاج إلى تطوير البرامج لتلبية متطلبات الأعمال المستقبلية.

ز. أمن الموارد البشرية

يحتاج الموظفون المسئولين عن التعامل مع البيانات الشخصية في الجهة إلى تلقي تدريب توعوي مناسب وتحديثات منتظمة بشأن الحفاظ على البيانات التي بحوزتهم. ويجب تحديد وتوثيق الأدوار والمسؤوليات الموكلة في كل وصف وظيفي تطبيقا للسياسة الأمنية في المنظمة. ويجب حماية البيانات المؤسسية من الوصول غير المصرح به، أو كشف البيانات، أو تعديلها، أو تدميرها أو التدخل بها. إن إدارة أمن الموارد البشرية ومخاطر الخصوصية تعد ضرورية خلال جميع مراحل العمل مع المنظمة.

الجوانب الثلاثة لأمن الموارد البشرية:

- قبل التوظيف: يتضمن هذا الموضوع تحديد أدوار ومسؤوليات الوظيفة وتحديد حق الوصول المناسب إلى المعلومات الحساسة للوظيفة، وتحديد دقة مستوى الاختيار بالنسبة للمرشح لشغل الوظيفة –وفقا لسياسة أمن تكنولوجيا المعلومات في الشركة. وخلال هذه المرحلة، يجب وضع شروط العقد.
- خلال التوظيف: يجب أن يتلقى الموظفين ممن لديهم إمكانية الوصول إلى المعلومات الحساسة في المؤسسة تنبيهات دورية حول مسئولياتهم بالإضافة إلى تلقي تدريب أمني توعوي مستمر، لضمان فهمهم للتهديدات الحالية والإجراءات الأمنية التي يجب اتخاذها لمواجهة مثل هذه التهديدات.
- إنهاء أو تغيير العمل: لمنع الوصول غير المصرح به إلى المعلومات الحساسة، يجب إلغاء الصلاحيات فور إنهاء خدمة الموظف. ويشمل هذا أيضا إرجاع أي أصول تابعة للجهة تكون بحوزة الموظف.

يجب أن يكون هناك برنامجا للتوعية الأمنية، ينبه جميع الموظفين من المخاطر المحتملة، وإمكانية التعرض لها ومسؤولياتهم كأوصياء على معلومات الجهة.

ح. الأمن المادي والبيئي

يعنى بالأمن المادي، التدابير التي تم تصميمها لمنع وصول الموظفين غير المصرح لهم (بما في ذلك المهاجمين أو المتسللين من غير قصد) إلى مبنى أو مرفق أو مورد أو معلومات مخزنة؛ والتوجيه بشأن كيفية تصميم مباني لمنع أعمال يحتمل أن تكون عدائية. ويمكن أن يكون الأمن المادي ببساطة باب مغلق أو طبقات متعددة من الحواجز وحراس أمن مسلحين ومرافق حراسة.

يرتبط الأمن المادي بالدرجة الاولى مع تقييد الوصول المادي لغير المصرح لهم (عادة ما يفسر أنه المتطفلين) للمرافق الخاضعة للرقابة على الرغم من وجود اعتبارات أو حالات أخرى تكون فيها تدابير الأمن المادي هامة جدا (على سبيل المثال، تقييد الوصول داخل المرفق و/أو أصول معينة، والضوابط البيئية للحد من الحوادث المادية مثل الحرائق والفيضانات).

من المؤكد أن توفير الأمن ينطوي على تكاليف كبيرة، وفي الواقع، لن يكون أبدا مثاليا أو كاملا – وبعبارة أخرى، الأمن يمكن أن يقلل من المخاطر لكن لا يقضي عليها. ونظراً لأن عناصر الرقابة غير متكاملة، فإن الأمن المادي القوى يطبق مبدأ الدفاع باستخدام تركيبات مناسبة من عناصر رقابية متداخلة ومتكاملة. فعلى سبيل المثال، عناصر الرقابة على الوصول المادي للمرافق المحمية تهدف بشكل عام إلى:

- ردع المتسللين المحتملين (مثل علامات التحذير والخطوط الخارجية).
- التمييز بين الأشخاص المصرح لهم والأشخاص غير المصرح لهم (مثل استخدام بطاقات/ شارات الدخول والمفاتيح).
- تأخير وإحباط ومنع محاولات التسلل (مثل الجدران المتينة، إقفال الأبواب والخزائن) .
- الكشف عن الاختراقات ومراقبة / تسجيل المتسللين (مثل صافرات الإنذار والكاميرات) .
- الاستجابة المناسبة للحوادث (مثلاً عن طريق حراس الأمن والشرطة).

ط. ضوابط الدخول

تشير ضوابط الدخول إلى التحكم بعملية التفاعل مع الموارد. في كثير من الأحيان ولكن ليس دائما، تمنح هذه السلطة لأحد المسئولين. المورد يمكن أن يكون مبنى، أو مجموعة معينة من المباني، أو نظام تكنولوجيا المعلومات الذي يعتمد على الكمبيوتر. ومسألة ضوابط الدخول –سواء المادي أو المنطقي – في واقع الأمر هي ظاهرة يومية. إن قفل باب السيارة هو أساسا شكل بسيط من أشكال ضوابط الدخول. والرقم السري على جهاز الصرف الآلي في البنوك هو أحد أشكال ضوابط الدخول وكذلك أجهزة القياس الحيوي. وحيازة التحكم في الوصول لها أهمية قصوى عند الأشخاص الذين يسعون لتأمين المعلومات والمعدات المهمة أو السرية أو الحساسة.

في البيئة الحكومية، التحكم بالوصول أمر هام جدا نظراً لأن العديد من الجهات الحكومية تتعامل مع البيانات الحساسة، ومخاوف الخصوصية تحد من عدد الأشخاص الذين يمكنهم الاطلاع على المعلومات. ويضمن التحكم في الوصول أن يكون بإمكان المستخدمين المصرح لهم فقط الوصول إلى البيانات الحساسة.

ي. اقتناء وتطوير وصيانة نظم تكنولوجيا المعلومات

إن دورة حياة تطوير النظم، أو عملية تطوير البرامج في هندسة النظم، أو أنظمة تكنولوجيا المعلومات وهندسة البرامج هي عملية إنشاء أو تغيير نظم تكنولوجيا المعلومات، والنماذج والمنهجيات التي يستخدمها الأشخاص لتطوير هذه النظم. في هندسة البرامج، يدعم مفهوم دورة حياة تطوير النظم العديد من منهجيات تطوير البرامج. وتشكل هذه المنهجيات إطار للتخطيط ومراقبة إنشاء نظم تكنولوجيا المعلومات او عملية تطوير البرامج.

تشتمل صيانة نظام تكنولوجيا المعلومات خلال دورة الحياة التغييرات والتحديثات على النظام نتيجة للمتطلبات الجديدة، وإصلاح أخطاء النظام، والتحسينات التي تجرى نتيجة لظهور واجهات جديدة.

ك. إدارة حوادث أمن تكنولوجيا المعلومات

في مجالات أمن الكمبيوتر وتكنولوجيا المعلومات، تشمل إدارة الحوادث في أمن تكنولوجيا المعلومات مراقبة والكشف عن الحوادث الأمنية على أجهزة الكمبيوتر أو شبكة الكمبيوتر، والإجراء المناسب للتعامل مع تلك الحوادث. إن إدارة حوادث أمن تكنولوجيا المعلومات هو شكل متخصص من إدارة الحوادث الطارئة.

ل. إدارة استمرارية الأعمال

التخطيط لاستمرارية الأعمال هو عملية تستخدمها الجهة في التخطيط وفحص استعادة نشاطها بعد توقف العمليات. كما يصف كيفية استمرار العمل في ظل الظروف السيئة التي قد تنشأ (على سبيل المثال، الكوارث الطبيعية).

م. الالتزام

يجب على مدقق تكنولوجيا المعلومات مراجعة وتقييم مدى الالتزام بجميع المتطلبات الداخلية والخارجية (المتطلبات القانونية والبيئية وجودة المعلومات، والائتمانية والأمن).

II. المخاطر على الجهة الخاضعة للتدقيق

السياسات والإجراءات الأمنية على تكنولوجيا المعلومات وتنفيذها تمكن الجهة من حماية البنية التحتية لتكنولوجيا المعلومات من المستخدمين غير المصرح بهم. فسياسة أمن المعلومات في الجهة تضع المتطلبات العامة للمنظمة وموظفيها لحماية الأصول الحيوية. كما تنص على تدريب الموظفين على القضايا الأمنية وتضمن أنهم يتبعون الإجراءات المطلوبة في الوصول إلى البيانات. بالإضافة إلى ذلك، تشير سياسة تكنولوجيا المعلومات إلى القوانين واللوائح الأخرى التي يجب على الجهة اتباعها. وهناك العديد من العقبات التي تواجه الجهات فيما يتعلق بتنفيذ نظام فعال لأمن المعلومات. ودون الحوكمة الفعالة في التعامل مع هذه العقبات، سيتعرض أمن تكنولوجيا المعلومات لخطر الفشل في تحقيق أهداف الجهة .

كل جهة تواجه تحديات خاصة بها نظرا لاختلاف الأمور البيئية والسياسية والجغرافية والاقتصادية والاجتماعية بشكل خاص. وأي أمر من هذه الأمور يمكن أن يشكل عقبات في طريق توفير حوكمة فعالة لتكنولوجيا المعلومات، وأنها من مسؤولية مدقق تكنولوجيا المعلومات أن يشير إلى المخاطر في أمن المعلومات للإدارة.

وفيما يلي جميع المخاطر الهامة المحددة في معظم الجهات:

- الكشف غير المصرح به للمعلومات.
- التعديل أو التدمير غير المصرح به للمعلومات.
- ضعف الاستجابة لهجمات أمن المعلومات.
- تدمير البنية التحتية لأمن المعلومات.
- تعطيل الوصول إلى المعلومات أو نظام المعلومات.
- تعطيل معالجة نظام المعلومات.
- سرقة المعلومات أو البيانات.

عند البحث عن تعرض الجهات الخاضعة للتدقيق للمخاطر، يجب الاهتمام بالمجالات التالية:

- استراتيجيات أمن المعلومات لا تتسق مع تكنولوجيا المعلومات أو متطلبات الأعمال.
- عدم تطبيق السياسات بشكل موحد.
- عدم الالتزام بالمتطلبات الداخلية والخارجية.
- أمن المعلومات غير مدرج في ملف صيانة وتطوير المشاريع.
- ينتج عن التصميم حلول أمن معلومات غير فعالة أو مضللة.
- عدم ملاءمة تدابير الأمن المادي وإدارة الأصول.
- عدم ملاءمة إعدادات برمجيات نظام الأجهزة.
- عدم كفاءة تنظيم عمليات أمن المعلومات وعدم وجود هيكل لمسئوليات أمن المعلومات أو يكون مبهم.
- حلول غير مناسبة للموارد البشرية.
- الاستخدام غير الفعال للموارد المالية المخصصة لأمن المعلومات، وأن هيكل قيمة أمن المعلومات (التكلفة والعائد) لا يتماشى مع احتياجات العمل.
- عدم وجود مراقبة لأمن المعلومات أو تكون هذه المراقبة غير فعالة.

يجب أن يبدأ المدقق بتقييم مدى ملاءمة أساليب تقييم المخاطر، وأن يأخذ في الاعتبار المسائل المتعلقة بالتدقيق وذات الصلة بتنفيذ أمن المعلومات. وسوف تساعد مصفوفة التدقيق المدقق على طرح الأسئلة وإمكانية استخدام معايير تقييم وتحديد الوثائق المطلوبة والتحليل الفني. في النهاية، يكون بإمكان المدقق وضع برنامج تفصيلي للتدقيق وفقا للاحتياجات والتطوير خلال عمل التدقيق.

عند القيام بتدقيق أمن معلومات، يجب على المدقق معالجة القضايا المتصلة بالمجالات الاثني عشر (على النحو الوارد أعلاه) في أمن المعلومات[46].

مصفوفة التدقيق

يمكن الاطلاع على مصفوفة التدقيق لهذا القسم في الملحق السابع.

المراجع / للمزيد من الاطلاع:

1. ISSAI 5310 Information System Security Review Methodology
2. ISO 27000 series Information Security Management System
3. ISO 27005 information security risk management
4. ISACA RiskIT Framework
5. COBIT 4.1 Framework, 2007, IT Governance Institute
6. COBIT 5 Framework, 2012, Isaca
7. ISACA ITAF – A Professional Practices Framework for IT Assurance. USA. 2008
8. ISACA Information Security Audit/Assurance Program, 2010
9. ISACA IT Risk Management Audit/Assurance Program, 2012
10. COSO Enterprise Risk Management Framework.

[46] ISO 27000 series Information Security Management System

الفصل الثامن

ضوابط التطبيق

I. ما هي ضوابط التطبيق

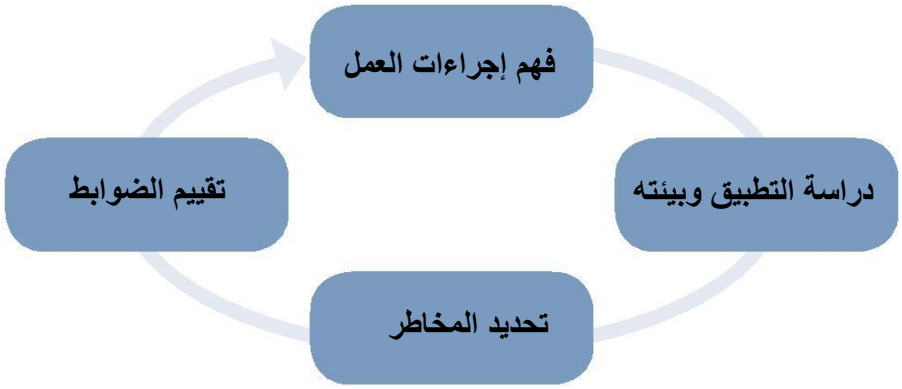
التطبيق هو برنامج محدد يستخدم لتنفيذ ودعم عملية محددة. ويمكن أن يشمل الإجراءات اليدوية والآلية معا للمعاملات، ومعالجة البيانات، وحفظ السجلات، وإعداد التقارير. ويمكن أن يكون لكل جهة عدد من التطبيقات التي يتم استخدامها لأداء اعمالها – وتتراوح في حجمها من نظام على مستوى الجهة يستخدمه جميع الموظفين في الجهة، إلى تطبيق صغير خاص بالمستخدم لا يمتلك إلا موظف واحد أحقية استخدامه. ويمكن أن يكون التطبيق عبارة عن نظام الرواتب، أو نظام الفواتير، أو نظام الجرد، أو ربما نظام التخطيط لموارد الجهة (ERP) وهو اختصار للاستخدام الأمثل للموارد.

من خلال مراجعة ضوابط التطبيق يتمكن المدقق من تزويد الإدارة بتقييم مستقل حول كفاءة وفعالية تصميم وأداء الضوابط الداخلية والإجراءات المتعلقة بميكنة أعمال الجهة، وتحديد الأمور المتعلقة بالتطبيقات التي تستوجب الاهتمام.

بما أن ضوابط التطبيق ترتبط ارتباطا وثيقا بالمعاملات الفردية، فمن السهل رؤية كيف أن عملية فحص الضوابط ستزود المدقق بضمان دقة عملية معينة. على سبيل المثال، فحص الضوابط في تطبيق الرواتب سيضمن صحة الأرقام المثبتة في حساب العميل. ولا يمكن القول أن فحص الضوابط العامة لتكنولوجيا المعلومات الخاصة بالعميل (مثل إجراءات ضوابط التغيير) سيوفر مستوى مشابه من الضمان لرصيد الحساب نفسه.

استناداً للأهداف المحددة للتدقيق، يمكن مراجعة التطبيق بطرق مختلفة. أي أن طريقة فحص الضوابط قد تختلف من عملية تدقيق لأخرى. على سبيل المثال، قد تركز عملية مراجعة التطبيق على الالتزام بالقوانين والمعايير، وبالتالي تكون النقطة الأساسية هي التحقق من مدى تطبيق الضوابط بصورة تساعد في معالجة تلك القضايا. ومن منظور آخر، قد تكون عملية مراجعة التطبيق جزء من عملية تدقيق الأداء، لذا من المهم أن نرى كيف يتم تنفيذ قواعد العمل في التطبيق. اما إذا كان الهدف من التدقيق هو التحقق من أمن المعلومات، يجب أن يتم التركيز على الضوابط المسئولة عن ضمان سرية وسلامة وتوافر البيانات.

قد تنطوي الخطوات الواجب اتباعها في مراجعة ضوابط التطبيق على سلسلة من الأنشطة. وعلى الرغم من أنه قد يكون من الأفضل البدء من منظور الأعمال، إلا أن من المهم أن نلاحظ عدم وجود تسلسل هرمي صارم من ضمن هذه الخطوات. وبعضها قد ورد بإيجاز في الفقرات التالية.



شكل 8.1 دورة مراجعة التطبيق

فهم إجراءات العمل: قبل استكشاف الأمور الفنية المتعلقة بالتطبيق فإنه من المفيد التعرف على إجراءات العمل التي تم ميكنتها في التطبيق – القواعد والتدفقات والمستخدمين والأدوار ومتطلبات الالتزام ذات الصلة. حيث تعتبر عملية فهم إجراءات العمل الضمنية خطوة هامة تساعد على التحقق من توافق ضوابط التطبيق مع العمليات الآلية. ويعتمد مدى التعمق بهذه الخطوة على هدف التدقيق. ويتم ذلك عادة من خلال دراسة خطوات وإجراءات العمل والتشغيل، ومخطط سير العمل في الجهة، أو غيرها من المواد المرجعية. وقد يتعين على فريق التدقيق إجراء المقابلات مع مدراء الأعمال والمدراء التنفيذيين في مجال تكنولوجيا المعلومات والمستخدمين الرئيسيين للتطبيق.

دراسة التطبيق وبيئته: دراسة تصميم وفعالية التطبيق إما عن طريق مراجعة الوثائق (المخططات التنظيمية، والرسومات التخطيطية لتدفق البيانات، وأدلة المستخدم) أو عن طريق مقابلة كبار الموظفين. ودراسة الوظائف الرئيسية للبرنامج في العمل من خلال التفاعل ومراقبة الموظفين المستخدمين للتطبيق أثناء العمل. ومن خلال المناقشات، على المدقق ان يتعرف على اجراءات العمل والتطبيق من بداية إدخال البيانات إلى المخرجات والتسويات لملاحظة كيف تتدفق العمليات ومراقبة أي أنشطة يدوية مرتبطة بالتطبيق وتعمل كضوابط إضافية. بالإضافة إلى ذلك على المدقق مناقشة المدراء، والمشغلين، والمطورين والحصول على الوثائق المتعلقة بالبنية التحتية الخاصة بتكنولوجيا المعلومات: نظام

التشغيل، وبيئة شبكة العمل، ونظام إدارة قواعد البيانات، والعوامل المشتركة مع التطبيقات الأخرى، وهل تم برمجة التطبيق داخل الجهة أم تم الاستعانة بمصادر خارجية، كيفية معالجة البيانات من نواحي إدخال مجموعة من البيانات/الوقت الحقيقي/استخدام الانترنت. وهذا يعطي مؤشرا حول مدى تأثير البنية التحتية التكنولوجية على التطبيق.

تحديد المخاطر: المهمة الأساسية هي تحديد المخاطر المرتبطة بالأعمال التي يخدمها التطبيق (ما الخطأ الممكن حدوثه؟) وملاحظة كيف يتعامل البرنامج مع هذه المخاطر (كيف يتم ضبطها). في بعض الأحيان تكون عملية تقييم مخاطر الأعمال متوفرة (عملية تدقيق سابقة، التدقيق الداخلي أو الإدارة) ويمكن أن يستفيد المدقق من استخدام هذه المواد بعد التحقق من دقة تقييم المخاطر المتوفر.

تقييم الضوابط: بعد التعرف على البيئة (الاجرائية والفنية) المحيطة بالتطبيق يصبح المدقق قادرا على تقييم الضوابط المستخدمة في معالجة المخاطر الحالية. ويجب على المدقق أن يكون رأيا عند تقييم الضوابط وأن يكون حذرا عند وضع التوجيهات والتوصيات من أجل التطوير. على سبيل المثال، التفاصيل المسهبة في المعاملات قد تزيد من تكاليف النفقات العامة في الجهة، وقد لا توضح تقفي الأثر المطلوب. ويجب أن يشتمل التدقيق على تقييم أنواع مختلفة من الضوابط الموضحة في الجزء التالي.

I.1 العناصر الرئيسية لضوابط التطبيق

تعتبر ضوابط التطبيق عناصر تحكم فريدة من نوعها في كل تطبيق آلي. فعندما يتم ميكنة إجراءات العمل في تطبيق تكنولوجيا المعلومات، يتم كذلك وضع القواعد الإجرائية للعمل على شكل ضوابط في التطبيق. فتنطبق على أجزاء التطبيق وترتبط بالمعاملات والبيانات الدائمة.

في حين أن الضوابط العامة لتكنولوجيا المعلومات في الجهة تحدد أسلوب البيئة الرقابية بأكملها لنظم المعلومات، إلا أن ضوابط التطبيق يتم وضعها في صلب التطبيقات لضمان وحماية دقة وسلامة وموثوقية وسرية المعلومات. فهي تضمن ان المعاملات منذ بدايتها يتم التعامل معها من قبل مستخدم مصرح له وأنه تم إدخالها ومعالجتها بشكل صحيح وأن المعاملات قد سجلت وحفظت بدقة.

توضيح

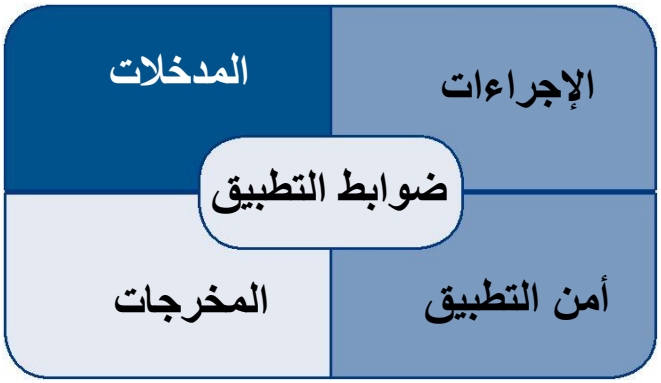
في تطبيق الدفع الإلكتروني عبر الانترنت (انظر إلى صورة بوابة الدفع عبر الانترنت أدناه)، أحد شروط إجراء هذه المعاملة الإلكترونية هو أن تاريخ انتهاء صلاحية بطاقة الائتمان يجب أن يكون بعد تاريخ إتمام العملية. والشرط الآخر هو ان يكون رقم البطاقة صحيح ويوافق اسم حامل البطاقة ورقم التحقق من البطاقة (cvv–number) وفقاً للجهة المصدرة لبطاقة الائتمان. وهناك شرط آخر هو أن بيانات المعاملة يجب ان تكون مشفرة حين تحويلها. ويجب أن تضمن الضوابط المضمنة في التطبيق أن هذه الشروط لا يمكن اختراقها، مما يضمن صحة المعاملات.

الشكل 8.2 مثال عن ضوابط التطبيق

كما تشمل ضوابط التطبيق الإجراءات اليدوية التي تعمل مع التطبيق. هذه الضوابط ليست مضمنة في التطبيقات فقط ولكن في إجراءات الأعمال المحيطة بها أيضا. على سبيل المثال، الموظف المسئول عن إدخال البيانات قد يشترط وجود نموذج معتمد بالتوقيع لإدخال البيانات قبل إدخالها على النظام.

إن دمج التطبيق اليدوي والآلي معا غالبا ما يكون ناتجا عن اعتبارات تتعلق بالتكلفة والضبط توضع في عين الاعتبار في مرحلة تصميم التطبيق.

يمكن تقسيم التطبيق إلى الشرائح التالية: **المدخلات** من البيانات (أصل البيانات وإدخال البيانات)، معالجة المعاملات، **المخرجات** من البيانات (توزيع النتائج) و**الأمن** (تسجيل الدخول، الاتصالات، التخزين). وتدمج الضوابط في كل شريحة من التطبيق مع الضوابط التي تحد من صلاحيات الدخول على التطبيق والملفات الرئيسية.



شكل 8.3 العناصر الرئيسية لضوابط التطبيق

على الرغم من أنه من غير المعقول أن توضع خطوات وقوائم مرجعية مفصلة لكل تدقيق يجرى على التطبيق، إلا أنه يجب أن يكون مدقق تكنولوجيا المعلومات على دراية بمفاهيم الرقابة الشائعة في تقريبا جميع التطبيقات. ويمكن استخدام ذلك لتوليد الأفكار والإبداعات فيما يخص إعداد خطوات مخصصة لفحص التطبيق الذي يتم التدقيق عليه.

الجدول التالي يلقي الضوء على بعض عناصر الرقابة الأكثر شيوعا:

ضوابط الادخال	• فحص إدخال البيانات/الحقول (مثل التحقق من صحة أرقام بطاقة الائتمان المدخلة) • إدارة الوثائق الأصلية (مثل إجراءات الاعداد والحفظ) • آليات معالجة الأخطاء (رسائل بالأخطاء، الملفات المعلقة) • قواعد صلاحيات إدخال البيانات (مثل الفصل بين المهام)

الشكل 8.4 بعض الأمثلة عن ضوابط التطبيق

أ. ضوابط الإدخال

تهدف ضوابط الإدخال إلى التحقق من صحة ومصداقية البيانات المدخلة قبل قبولها بالتطبيق وان تتم هذه العملية في الوقت المناسب.

يتم تصميم جزء كبير من هذه الإجراءات خلال مختلف مراحل تطوير الأنظمة، وذلك بعد دمج قواعد العمل المنصوص عليها عند تحديد الاحتياجات. وعلى الرغم من أن عملية ادخال البيانات إما يدوية أو من خلال ربط الأنظمة، إلا أنه يمكن تقنين الأخطاء والإلغاءات من خلال تحري الدقة في إدخال البيانات

وفق التصميم، وفصل المهام بخصوص إنشاء واعتماد البيانات المدخلة، وتحديد اختبارات الرقابة ذات العلاقة للتحقق من التخويلات والدقة والكمال (باستخدام خيارات القائمة أو الرسائل التفاعلية).

عناصر ضوابط الإدخال	الوصف
التدقيق على ادخال البيانات (الصحة، الاكتمال، فحص التكرار)	التحقق الآلي من صحة البيانات المدخلة (مثلا، تاريخ الرحلة خارج نطاق فترة الحجز المفتوحة)، فحص الاكتمال للتأكد من إدخال جميع البيانات الرئيسية المطلوبة (مثلا، أن يتم إدخال تاريخ الرحلة، وأسماء الركاب، وأرقام الهويات وهي جميع الحقول الرئيسية المطلوبة)، فحص التكرار (الازدواجية) ويتم بمقارنة المعاملات الجديدة مع المعاملات التي تم إجراؤها في وقت سابق (مثلا، التحقق من عدم تكرار الفواتير).
إدارة الوثائق الأصلية	الوثائق المتعلقة بإجراءات اعداد الوثائق الأصلية، تسجيل الوثائق الأصلية، ترقيم الوثائق الأصلية، وإجراءات حفظ الوثائق.
إجراءات معالجة الأخطاء	إجراءات التعامل مع المدخلات المرفوضة. (مثل، رسائل الأخطاء، تدابير التصحيح اللاحقة، تمكين إعادة الإدخال، البيانات المعلقة).
التصريح بالإدخال	الإجراءات اليدوية/التصريح الإشرافي للدخول على البيانات في نموذج إدخال البيانات. مثل التصريح للمشرف بالدخول على تفاصيل الفواتير قبل إدخالها من قبل الموظف المسئول عن إدخال البيانات لتجهيزها في التطبيقات الجمركية.

ب. ضوابط معالجة البيانات

إن هدف وضع ضوابط على معالجة البيانات هو لحماية كمال وصحة وموثوقية البيانات والحذر من أن تقع أخطاء خلال دورة المعاملات – من وقت استلام البيانات من النظام الفرعي إلى وقت إرسالها لقاعدة البيانات أو الاتصالات أو النظام الفرعي للمخرجات. كما تكفل ان البيانات المدخلة الصحيحة يتم معالجتها مرة واحدة فقط، وأن الكشف عن المعاملات الخاطئة لا يعطل المعاملات الصحيحة. وعلاوة على ذلك، تسعى إلى تعزيز موثوقية التطبيقات التي تنفذ أوامر البرامج لتلبية احتياجات المستخدم.

تشمل الإجراءات الرقابية إنشاء وتطبيق آليات للسماح بالبدء بمعالجة المعاملات، وتنفيذ التطبيقات والأدوات المصرح بها فقط. ويتم التحقق بشكل روتيني من استكمال ودقة المعالجة بنظم الرقابة الآلية، حيثما كان ذلك مناسباً.

قد تتضمن أنواع الضوابط هذه التحقق من أخطاء التسلسل والازدواجية، وتسجيل عدد المعاملات، والتحقق من سلامة البيانات، وعمل اختبارات مجموع الضوابط والتجزئة (Control & Hash Totals)، واختبارات النطاق وتجاوز سعة التخزين.

من الإجراءات الرقابية التعويضية التي تتم في أنظمة الوقت الحقيقي هي مراجعة العمليات بشكل فردي، ومجاميع البيانات السابقة، تسجيل الاستثناءات والحسابات المعلقة.

ج. الضوابط على المخرجات

إن أهداف الضوابط على المخرجات هو ان تكون التدابير المضمنة في التطبيق تحقق استكمال ودقة وصحة توزيع مخرجات المعاملة. كما تسعى أيضا لحماية البيانات التي تتم معالجتها بواسطة التطبيق من التعديل والتوزيع الغير المصرح بهما.

تشمل هذه الضوابط وجود تعريف واضح للمخرجات والتقارير المطلوبة في مرحلة تصميم وتطوير النظام والتوثيق الملائم لطريقة استخراج التقارير، والضوابط التي تحد من الدخول على البيانات التي يتم معالجتها، ومراجعة المخرجات والتسوية والمراجعة.

د. الضوابط على أمن التطبيق

أهمية أمن التطبيق تكمن بالحفاظ على السرية والنزاهة وتوافر المعلومات في جزئية التطبيق. وبغرض التدقيق، من المهم أن نفهم هذه الواجهات والمصادر المختلفة للبيانات المدخلة إلى التطبيق والبيانات المستخرجة منه بالإضافة إلى طرق تخزين البيانات.

يتم الوصول لمعظم التطبيقات عن طريق استخدام الهوية الشخصية للمستخدم وكلمة المرور. ومع ذلك، هناك طرق أخرى لتسجيل الدخول، مثل آلية الدخول المفرد (Single Sign-On)، والتي أصبحت شائعة الاستخدام في الآونة الأخيرة، بالنظر إلى حجم التطبيقات المستخدمة في بيئة الجهة. لذلك يجب فهم تصميم التطبيق الخاص لإدارة حسابات المستخدمين مسبقا. وقد يحتاج المدقق إلى مراجعة سياسات وإجراءات الجهة التي يتم

اتخاذها للحصول على وإلغاء صلاحية دخول المستخدم من أجل فهم مدى تضمين قواعد الدخول في كل مستويات التطبيق وضمان أن للتطبيق ضوابط حول توفير وإلغاء الدخول على البيانات.

وللتمكن من فهم إجراءات الضوابط الأمنية للتطبيق، على المدقق أن يفهم الأطراف الفاعلة والأدوار والمسئوليات المتضمنة في التطبيق، مثل مدراء التشغيل (Administrators) وكبار المستخدمين (Power Users) والمستخدمين العاديين وغيرهم. وقد يتنوع تصميم ضوابط الدخول المنطقي إلى عدة أنواع. ومعظم البرامج تتحقق من صحة هوية المستخدم وكلمة المرور قبل السماح له بالدخول. ويمكن التحكم بصلاحيات الدخول لكل جزئية من البرنامج أو خيارات القائمة والشاشات من خلال الأدوات والأدوار. ويجب على مدقق تكنولوجيا المعلومات أن يراجع تصميم ضوابط الدخول، مع الأخذ بالاعتبار مدى أهمية الوظائف والإجراءات المتاحة. في الواقع، من الضروري القدرة على التعرف على الآليات المستخدمة في التطبيق لضمان صحة تخويل المعاملات وإمكانية تتبعها إلى جانب حماية البيانات المخزنة فيه.

فيما يلي قائمة بأمثلة عن الموضوعات القابلة للتدقيق بخصوص الرقابة على أمن التطبيقات:

تتبع المعاملات: تسجيل المعاملات، والتحقق من هوية المستخدم، ومراقبة السجلات الإلكترونية، إذ يجب أن يدون في سجل التدقيق الحقول التي طرأ عليها تعديلات، ومتى تم ذلك، والقيم الأصلية والجديدة لتلك الحقول، ومن قام بالتعديل.

إدارة حسابات المستخدم، الصلاحيات وإدارة كلمات المرور: الرقابة على استخدام حسابات المستخدم والحسابات المؤقتة والحسابات العامة، واستخدام الحسابات ذات الصلاحيات المميزة وحسابات مدراء التشغيل والضوابط التعويضية، وإجراءات إنهاء العمل وإلغاء الصلاحيات، واعتماد مبدأ أقل الامتيازات، ودخول فريق تطوير البرامج على قاعدة بيانات الإنتاج، والإجراءات الرسمية لاعتماد ومنح الصلاحيات بالدخول، واستخدام كلمات مرور متينة، وإجبار إجراء التغييرات الدورية عليها، وتشفير كلمات المرور، إلخ.

حماية بيانات الملفات الرئيسية الدائمة (وشبه الدائمة): وضع الضوابط لضمان صحة التخويل بالتعديلات على البيانات الدائمة، وتحميل المستخدمين مسئولية أي تغييرات يتم إجراؤها، والتأكد من صحة وحداثة البيانات الدائمة، والحفاظ على سلامة الملفات الرئيسية. ومن الأمثلة على البيانات الدائمة: تفاصيل المورد والعميل (الاسم، العنوان، الهاتف، رقم الحساب)، ومعدلات التضخم، وبيانات إدارة النظام، مثل ملفات كلمات الدخول والتحكم بصلاحيات الدخول، إلخ.

اعتماد مبدأ المهام المتضاربة وفصل المهام: تحديد أدوار مختلفة للمستخدمين، وتوافر حقوق الدخول لكل مستخدم، ووضع قواعد للفصل بين الواجبات.

II. مخاطر على الجهة الخاضعة للتدقيق

غالبا ما تتوقف عواقب فشل ضوابط التطبيق على طبيعة التطبيق. ويمكن أن تتراوح المخاطر من عدم رضا المستخدم إلى حدوث كوارث حقيقية وخسائر في الأرواح. على سبيل المثال، قد تخسر الجهة من قيمتها في السوق في حال أصبحت أحد خدماتها غير متاحة، وقد تخسر الجهة الأموال بسبب فقدان طلبيات الشراء على الانترنت، كما تفقد ثقة المواطنين في الخدمات الحكومية، ويمكن أن يؤدي عدم الالتزام بالمعايير القانونية إلى إقامة دعاوى قضائية على الجهة، وقد لا تصل الكهرباء إلى المنازل، وقد تتعرض الحسابات المصرفية إلى الاحتيال وغيرها.

على وجه التحديد، ربما وقعت المخاطر الهامة في ظل غياب الضوابط الملائمة للمدخلات والمتمثلة في مخاطر المعالجة الخاطئة والاحتيالية عندها سيفشل التطبيق في تحقيق أهداف العمل. وقد تكون البيانات المعالجة بواسطة التطبيق غير متناسقة، مما يؤدي بالبرامج إلى تقديم مخرجات غير ملائمة. وما هو أكثر من ذلك، فحتى بوجود هذه النظم الرقابية إلا أن من المحتمل تجاوزهم في حالات معينة. وفي هذه الحالة، يجب وضع ضوابط تعويضية مثل السجلات الإلكترونية (Logs) وقواعد منح الصلاحيات، وإلا سيتم إساءة استخدام ميزات التجاوز وتؤدي إلى عدم تناسق البيانات المدخلة في التطبيق.

أيضا تعتبر الإجراءات الخاصة بإدارة الوثائق الأصلية والتصريح بإدخال البيانات أنواعا هامة من ضوابط الإدخال. وفي غياب الإدارة السليمة للوثائق الأصلية يصبح من الصعب تتبع مصدر المعلومات المدخلة على النظام، وقد لا يتحقق الالتزام القانوني، وتنتهك سياسات حفظ البيانات والوثائق، وقد تدرج بيانات غير موثوقة في التطبيق. ومن ناحية أخرى، عند غياب ضوابط التصريح، قد تؤدي البيانات الغير المصرح بها إلى وقوع الأخطاء أو الاحتيال.

بشكل عام، قد يؤدي فشل الضوابط على المعالجة إلى حدوث الأخطاء والفشل في تحقيق أهداف عمل التطبيق. وقد تظهر بسبب وضع قواعد عمل غير صحيحة، وبسبب عدم ملاءمة اختبار رموز البرنامج، أو عدم وجود ضوابط كافية على الإصدارات المختلفة للبرنامج لاستعادة سلامة المعالجة بعد حدوث مشكلة أو انقطاع غير

متوقع. وفي غياب الممارسات الضرورية لمراقبة المعالجة، من الممكن أن تتكرر الأخطاء في المعاملات والتي بدورها تؤثر على أهداف العمل.

باستخدام نظم المعالجة في الوقت الحقيقي، فإن بعض التدابير الرقابية مثل تسوية إجمالي بيانات المدخلات والمخرجات للتأكد من اكتمال المدخلات وحفظ الوثائق الأصلية للتدقيق غير متاحة. ومع ذلك، تتضمن أنظمة الوقت الحقيقي ضوابط بديلة داخل التطبيق، بما في ذلك، اكتمال البيانات التفاعلية، والتحقق من صحة المطالبات، وتسجيل محاولات الدخول على النظام، الخ.

يؤدي عدم وجود ضوابط كافية على المخرجات إلى مخاطر تعديل/حذف البيانات الغير المصرح به، وإنشاء تقارير إدارية مخصصة بشكل خاطئ وخرق سرية البيانات. وأيضا، تعتمد نتائج المخرجات الخاطئة على طريقة استخدام المعلومات من قبل الجهة.

وفي سياق أمن التطبيق، فإن عدم كفاية آليات التسجيل قد تجعل من المستحيل تتبع التصرفات الخاطئة لبعض المستخدمين. كما أن وعي المستخدم بإجراءات مراجعة التسجيل وآليات التقرير بذلك من شأنه وبحد ذاته أن يخفف من مخاطر سوء استخدام نظم المعلومات. والأخطاء الدائمة في البيانات لها تأثيرات بعيدة المدى على التطبيق، بما أن هذه البيانات يمكن استخدامها في معاملات كثيرة في التطبيق.

بطبيعة الحال، إن مخاطر التعامل غير الصحيح مع أمن المعلومات يؤدي إلى حدوث مخاطر أكبر من ذلك. حيث أنها تؤدي إلى عواقب تختلف درجات الخطورة فيها، من ضمنها، فقدان الدخل، وانقطاع الخدمة، وفقدان المصداقية، وتوقف الأعمال، وإساءة استخدام المعلومات، والعواقب القانونية، والدعاوى القضائية، وسوء استغلال الملكية الفكرية. وسنتحدث بالتفصيل عن هذه المخاطر والضوابط التخفيفية في فصل أمن المعلومات.

مصفوفة التدقيق

يمكن الاطلاع على مصفوفة التدقيق لهذا الجزء في الملحق الثامن.

المراجع:

1. ISACA IT Audit and Assurance Guideline G38, Access Controls
2. *IT Audit Manual* Volume I, SAI India
3. *IT Auditing: Using Controls to Protect Information Assets*, Second Edition by Chris Davis, Mike Schiller and Kevin Wheeler McGraw-Hill/Osborne
4. *Singleton, Tommie W. Auditing applications* – Part 2. ISACA Journal, Vol IV. 2012.

الفصل التاسع

موضوعات أخرى هامة

يقدم هذا الجزء نظرة عامة لبعض الموضوعات الأخرى ذات الصلة بتدقيق تكنولوجيا المعلومات التي ممكن أن يتعرض لها المدقق خلال قيامه بعملية التدقيق. وهناك العديد من المجالات التي قد تطرأ خلال عملية التدقيق على تكنولوجيا المعلومات والتي يمكن أن تتطور إلى مواضيع قابلة للتدقيق. لذلك يجب على المدقق أن يكون على دراية تامة بوجود هذه المجالات وأن يكون قادراً على النجاح في التعامل مع هذا النوع من المواضيع.

على الرغم من أن هذه المجالات قد تحتمل وجود اختلافات تقنية أو غيرها، إلا أنه يمكن إجراء التدقيق باستخدام نفس المنهجيات والتقنيات التي تم التطرق لها في هذا الدليل. ومن المحتمل أن يتطلب التدقيق طرح بعض الاستفسارات الإضافية التي يمكن أن يضيفها المدقق عندما يتعامل مع مثل هذه الموضوعات بحيث تخدم أهداف التدقيق.

1. المواقع/البوابات الإلكترونية

المواقع الإلكترونية هي نظم معلومات موجودة على شبكة الانترنت أو الشبكات الداخلية التي تقدم الخدمات والمحتويات مثل النصوص والصور والمرئيات والصوتيات إلخ. أما البوابة الإلكترونية فهي تنظم المعلومات من مصادر مختلفة بطريقة موحدة، بحيث تقدمها بصورة متناسقة ومريحة للنظر. وعادة تقدم البوابات الإلكترونية الخدمات مثل محركات البحث والأخبار والمعلومات والدخول إلى الأنظمة وقواعد البيانات والمواد الترفيهية. وبعض الأمثلة عن بوابات الانترنت العامة هي AOL، iGoogle، Yahoo، India.com.

مجالات التدقيق

خبرات المستخدم.

الأمن، الخصوصية.

الزمن المستغرق للحصول على الإجابة.

الاستعانة بمصادر خارجية للمواضيع ذات الصلة.

المراجع / للمزيد من الاطلاع:

- 1. http://en.wikipedia.org/wiki/Web_site
- 2. http://en.wikipedia.org/wiki/Web_portal
- 3. Kenyon, Geoff. *Technical Site Audit Checklist*. 2011,
- http://www.seomoz.org/blog/how-to-do-a-site-audit
- 4. Jones, Harrison. *How-to: Guide -to Performing Website Audits*. 2011
- http://www.techipedia.com/2011/website-audit-guide/

2. الحوسبة المتنقلة

هناك جهد متزايد لتقديم الخدمات للعامة من خلال جميع أنواع قنوات تكنولوجيا المعلومات. ويرتبط ذلك باستخدام تكنولوجيات الاتصالات اللاسلكية لتوفير التطبيقات والمعلومات. في الوقت الحاضر، العديد من التطبيقات يتم تقديمها في بيئة متنقلة، مثل الهواتف النقالة، وأجهزة tablets، والشبكات اللاسلكية وأجهزة التلفاز، ومجموعة متكاملة من الأجهزة الإلكترونية الحديثة التي تقوم بإيصال المعلومات. يمكن اعتبار الحوسبة المتنقلة على أنها نقطة دخول لتكنولوجيا المعلومات (أجهزة الكمبيوتر، أجهزة الكمبيوتر النقال، إلخ) إنما لها مجالات تدقيق خاصة قد تكون ذات أهمية.

مجالات التدقيق

الأمن اللاسلكي والخصوصية والتشفير.

خبرات المستخدم.

سياسات محددة بخصوص الحوسبة المتنقلة في الجهة.

مخاطر استخدام الأجهزة الشخصية للدخول على بيانات وخدمات الجهة.

مخاطر الدخول غير المصرح به على البيانات الموجودة داخل الجهاز.

المخاطر المتزايدة لتلف أو سرقة أجهزة الجهة.

المراجع / للمزيد من الاطلاع:

1. ISACA IT Audit and Assurance Guideline G 27 – Mobile Computing
   http://www.isaca.org/Knowledge-Center/Standards
2. ISACA Mobile Computing Security Audit/Assurance Program
   http://www.isaca.org/auditprograms

3. التدقيق الجنائي (أو التحقيقات الجنائية على أجهزة الكمبيوتر)

التدقيق الجنائي هو نوع من أنواع التدقيق الذي يجرى لفحص الوسائط الرقمية للأدلة المتعلقة بالتحقيقات أو النزاعات. ويجب التشديد على الاحتفاظ بالأدلة خلال إجراء التحليل الجنائي على أجهزة الكمبيوتر. ويشمل ذلك نهج وأدوات وتقنيات دراسة المعلومات الرقمية لتحديد وحفظ واسترداد وتحليل وتقديم الحقائق والآراء حول المعلومات المخزنة.

إنها في الغالب مرتبطة بالتحقيقات الجنائية بهدف مساعدة جهات تنفيذ القوانين وتقديم أدلة قوية في المحكمة. وقد تم تطبيق التحقيقات الجنائية على أجهزة الكمبيوتر في عدد من الجوانب مثل قضايا الاحتيال والتجسس والقتل والابتزاز وسوء استعمال الكمبيوتر وسوء استعمال التكنولوجيا والفضائح والرسائل غير اللائقة، وتسريب المعلومات وسرقة الملكية الفكرية والمواد الإباحية ورسائل الكمبيوتر غير المرغوب بها، والقرصنة والتحويل غير المشروع للأموال[47].

مجالات التدقيق

يشمل الانضباط تقنيات وقواعد مشابهة لاسترداد البيانات ولكن بإرشادات وممارسات إضافية مصممة لإنشاء سجل قانوني لأثر التدقيق.

حفظ الإثباتات (البيانات، الدخول، التسجيل) للتحليل.
حجز وحفظ البيانات بالقرب من الانتهاك القانوني على قدر الإمكان.
معايير جمع البيانات لاحتمال استخدامها في إنفاذ القانون.
حجز البيانات دون التسبب بانقطاع الأعمال.
تحديد المهاجمين ان أمكن.

[47] ISACA's IT Audit and Assurance Guideline G38 Computer Forensics

المراجع / للمزيد من الاطلاع:

1. ISACA IT Audit and Assurance Guideline G 27 – Mobile Computing
   http://www.isaca.org/Knowledge-Center/Standards
2. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*
3. http://www.ncjrs.gov/pdffiles1/nij/199408.pdf
4. *Electronic Crime Scene Investigation: A Good Practice Guide for Computer-Based Electronic Evidence*
5. http://www.met.police.uk/pceu/documents/ACPOguidelinescomputerevidence.pdf
6. Computer Forensics. Wikipedia
7. http://en.wikipedia.org/wiki/Computer_forensics

4. الحكومة الإلكترونية، والحوكمة الإلكترونية والحوكمة المتنقلة (eGov, e-Gov & m-Gov)

أدى التطور التكنولوجي إلى تغيير جذري في طريقة تقديم الحكومة لخدماتها للمواطنين. وفي الوقت الذي تنتشر فيه التكنولوجيا بين المواطنين، تهتم الحكومات باتخاذ نهج جديد في تقديم المعلومات والتطبيقات لصالح المواطنين. وتعتبر الحكومة الإلكترونية والحوكمة الإلكترونية والحوكمة المتنقلة هي بعض المجالات التي تتعامل مع هذا الموضوع. وهذه المفاهيم تتصل ببعضها البعض إنما لا تعتبر متماثلة تماما.

مجالات التدقيق

لتحقيق أهداف التدقيق، يجب أن يدرك المدقق أن الحكومات مطلوب منها أن تقدم الخدمات بطريقة تتميز بالاقتصاد والكفاءة والفعالية. وفي كثير من الأحيان تتيح الخدمات الإلكترونية تواصل أكبر قدر من الناس بتكلفة معقولة.

من المنظور الرقابي، فإن التدقيق على نظم المعلومات أو إجراءات العمل المؤثرة في استراتيجية الحكومة الإلكترونية أو المتنقلة لا تختلف عن التدقيق التقليدي على تكنولوجيا المعلومات. وقد يحتاج المدقق أن يلقي نظرة على بعض السياسات وآليات التنفيذ (مثل، السياسة التنظيمية بخصوص الحوسبة المتنقلة، وبرنامج التشفير، وحدود استخدام الهواتف الذكية الشخصية، إلخ).

المراجع / للمزيد من الاطلاع:

1. Electronic Governance. Wikipedia
2. http://en.wikipedia.org/wiki/E-Governance
3. Mobile Governance. Ministry of Communications and Information Technology. Government of India
4. http://mgov.gov.in/msdpbasic.jsp
5. United Nations E-Governance Survey
6. http://www2.unpan.org/egovkb/global_reports/10report.htm

5. التجارة الإلكترونية (E-commerce)

تشير التجارة الإلكترونية (E-commerce) إلى أي نوع من التعاملات التجارية التي تتم من خلال الشبكات. وتشمل، على سبيل المثال لا الحصر، بيع وتداول المعلومات والسلع والخدمات.

على الرغم أن لغة التجارة الإلكترونية عادة ما تشير إلى تجارة السلع والخدمات عبر الانترنت، إلا أنها تشمل كذلك أنشطة اقتصادية أوسع نطاقا. فالتجارة الإلكترونية تتكون من الأعمال التجارية الموجهة إلى المستهلك والأعمال التجارية الموجهة إلى الأعمال التجارية بالإضافة إلى معاملات الجهات الداخلية التي تدعم هذه الأنشطة[48].

في الوقت الحاضر، توجد مجموعة واسعة من التقنيات وإجراءات العمل ذات علاقة بالتجارة الإلكترونية مثل البوابات الإلكترونية، والتحويل الإلكتروني للأموال، والخدمات المصرفية عبر الانترنت، وإدارة سلسلة الموارد، والتسويق، والتسوق عبر الانترنت، والتجارة المتنقلة، وإدارة المخزون، إلخ.

---

[48] E-Commerce. Encyclopedia Britannica
http://www.britannica.com/EBchecked/topic/183748/e-commerce

مجالات التدقيق

توجد جوانب متعددة ذات أهمية كبيرة لأنظمة التجارة الإلكترونية، ويجب أخذها في عين الاعتبار عند تحديد أهداف التدقيق، مثل:

التوافر.
أمن المعاملات.
نطاق الحل.
خبرة المستخدم.
إجراءات العمل التي تتولاها استراتيجية التجارة الإلكترونية.

إن إجراءات العمل التي تتم من خلال استراتيجيات التجارة الإلكترونية تتطلب وجود آليات أمنية قوية من أجل أن تتميز المعاملات على الانترنت بشكل أساسي بالسلامة والسرية وعدم الرفض والتخويل المناسب. وهكذا، يتم تبني مجموعة من العمليات والتقنيات التي تسمى "البنية التحتية للمفتاح العام" (Public-Key Infrastructure PKI).

تضم البنية التحتية للمفتاح العام مجموعة من منهجيات وتقنيات التشفير المعيارية لتمكين المستخدم من الاتصال بشكل آمن عبر الشبكات العامة الغير آمنة لضمان توصيل المعلومات للمتلقي المقصود. وبدون هذه التكنولوجيا من المستحيل أن تكون التجارة الإلكترونية بالشكل الذي نعرفه[49].

من أجل التدقيق على أنظمة التجارة الإلكترونية، غالبا ما يتعين على المدقق أن يتعرف على المكونات الرئيسية للبنية التحتية للمفتاح العام PKI:

المفاتيح العامة والخاصة
آليات التوقيع الرقمي
الشهادات الرقمية
سلطات التصديق والتسجيل
منهجيات التشفير

[49] برنامج تدقيق / ضمان التجارة الإلكترونية والبنية التحتية للمفتاح العام، ISSACA 2012.

لا يحتاج المدقق أن يكون خبيرا في هذه المجالات، إلا أنه يجب أن يكون على دراية بالمعايير المقبولة على نحو واسع وما إذا الجهة قد تبنتها أم لا.

المراجع / للمزيد من الاطلاع:

1. E-Commerce. Encyclopedia Britannica. http://www.britannica.com/EBchecked/topic/183748/e-commerce
2. E-Commerce and Public Key Infrastructure Audit/Assurance Program. Isaca http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Ecommerce-and-Public-Key-Infrastructure-PKI-Audit-Assurance-Program.aspx
3. Audit Trails in an E-commerce Environment http://www.isaca.org/Journal/Past-Issues/2002/Volume-5/Pages/Audit-Trails-in-an-Ecommerce-Environment.aspx

الملحق الاول

القائمة العامة للتقييم حسب الأهمية

مفتاح القائمة:

d. يجب على جهاز الرقابة الأعلى تحديد وزن (درجة الأهمية) لكل سؤال. وان دعت الحاجة، يمكن للجهاز أن يحدد درجة الأهمية بالتشاور مع الجهة. وان كان من غير الضروري تحديد الوزن فيمكن للجهاز أن يوحد الأوزان لجميع الأسئلة.

e. تشير الأرقام الواردة بين القوسين إلى نتائج الردود. والنتائج المشار إليها تتراوح ما بين 1 إلى 5 حيث يشير 1 إلى أقل المجالات خطورة و5 إلى أعلى المجالات خطورة. ويمكن لأجهزة الرقابة العليا اعتماد درجات مختلفة حسب طريقتهم.

f. لا تعتبر الأسئلة شاملة. ويمكن لأجهزة الرقابة العليا أن تختار أسئلة من الجدول المذكور أدناه أو وضع الأسئلة وفقاً لاحتياجاتهم.

g. ينبغي على جهاز الرقابة الأعلى جمع المعلومات المطلوبة في القائمة لجميع الجهات الخاضعة للتدقيق. ويمكن للأجهزة البحث أن تسعى لجمع أكبر قدر من المعلومات لتكون النتائج والمقارنات متصلة بالموضوع.

h. يمكن لجهاز الرقابة الأعلى أن يقرر جعل النتائج والتصنيفات سرية أو يتم إطلاع أصحاب المصلحة عليها وفقا للسياسة المتبعة بالجهاز.

I. اسم نظام وإدارة تكنولوجيا المعلومات:

	المعـــايير	درجة الأهمية	النتيجة
	حوكمة تكنولوجيا المعلومات		
1	**الوضع العام للحوسبة في الجهة. تمت حوسبة المجالات التالية في الجهة:**		

	المعـــايير	درجة الأهمية	النتيجة
	جميع إجراءات الأعمال (5)		
	غالبية إجراءات الأعمال (4)		
	بعض الإجراءات فقط (3)		
	لم يستخدم في أي من الإجراءات (1)		
2	**لدى الجهة سياسات خاصة بتكنولوجيا المعلومات وسياسات أخرى متعلقة بها**		
	نعم (1)		
	جزئيا (3)		
	لا (5)		
3	**قامت الجهة بالتالي:**		
	انشاء قسم مستقل لتكنولوجيا المعلومات (2)		
	قامت الجهة بالاستعانة بمصادر خارجية لأداء بعض مهام تكنولوجيا المعلومات (5)		
	قامت الجهة بالاستعانة بمصادر خارجية لمرافق تكنولوجيا المعلومات (5)		
4	**هل للجهة**		
	مدير تنفيذي للمعلومات (CIO) مسئول عن الأنشطة المرتبطة بتكنولوجيا المعلومات (1)		
	لدى الجهة مدير تنفيذي مسئول عن الأنشطة المرتبطة بتكنولوجيا المعلومات بالإضافة إلى مهامه (3)		
	لدى الجهة مسئول فرعي عن الأنشطة المرتبطة بتكنولوجيا المعلومات (3)		
	لا يوجد لدى الجهة شخص مسئول عن الأنشطة المرتبطة بتكنولوجيا المعلومات (5)		

	المعـــايير	درجة الأهمية	النتيجة
التطوير، والحيازة، والاستعانة بمصادر خارجية			
5	**تم تطوير النظام**		
	بواسطة الجهة وفق امكانيات كافية (1)		
	بواسطة الجهة وفق امكانيات غير كافية (5)		
	بواسطة مقاول / جهة حكومية أخرى (4)		
	مزيج من المصادر الداخلية والخارجية (5)		
6	**تم اقتناء النظام**		
	بواسطة الجهة وبإمكانات كافية لحيازة تكنولوجيا المعلومات (3)		
	بواسطة الجهة وبإمكانات غير كافية لحيازة تكنولوجيا المعلومات (5)		
	بواسطة الانتفاع من الخدمات الاستشارية (4)		
7	**وثائق النظام**		
	متوفرة (1)		
	متوفرة بشكل جزئي (3)		
	غير متوفرة (5)		
8	**عدد المرات التي تجرى فيها التغييرات على التطبيقات**		
	أكثر من 5 مرات في السنة (5)		
	أقل من خمس مرات وأكثر من مرتين في السنة (3)		
	أقل من مرتين في السنة (2)		
	لا يتم إجراء أي تغيير في السنة (1)		

	المعـــايير	درجة الأهمية	النتيجة
عمليات تكنولوجيا المعلومات وأمن المعلومات			
9	**عدد نقاط الدخول / مواقع العمليات / المستخدمين**		
	أكثر من Y (5)		
	أكثر من X وأقل من Y وأكثر من هذه المستويات، ان تطلب الأمر (3)		
	أقل من X (1)		
	(جهاز الرقابة الأعلى يقرر أعداد Y و X)		
10	**نظام قائم على الشبكة**		
	لا توجد شبكة (1)		
	شبكة اتصالات محلية (LAN) (3)		
	شبكة اتصالات واسعة (WAN) (4)		
	النظام له موقع إلكتروني قائم على الانترنت (5)		
11	**عدد المواقع** (جهاز الرقابة الأعلى يقرر أعداد Y و X)		
	موقع واحد فقط (1)		
	أكثر من موقع، أقل من عدد X من المواقع (3)		
	أكثر من عدد X من المواقع (3)		
12	**هل يستفيد النظام من الروابط المباشرة إلى أطراف ثالثة مثل التبادل الإلكتروني للبيانات EDI**		
	نعم (5)		
	لا (1)		
13	**عدد المستخدمين للنظام** (نقطة الانطلاق / أعداد المستخدمين تحدد ب X و Y وفق ما يقرره جهاز الرقابة الأعلى)		
	أقل من X (1)		

	المعـــايير	درجة الأهمية	النتيجة
	أكثر من X وأقل من Y وأكثر من هذه المستويات، ان تطلب الأمر (3)		
	أكثر من Y (5)		
14	**هل تحتفظ الجهة بالبيانات والتطبيقات**		
	داخل الجهة (1)		
	جزء منها داخل الجهة والآخر في جهات أخرى تم الاستعانة بها لبعض الخدمات (3)		
	تستضيفها جهات أخرى تم الاستعانة بها لبعض الخدمات (5)		
15	**النظام يعمل منذ**		
	أكثر من 10 سنوات (1)		
	بين 5 و10 سنوات		
	بين سنتان وخمس سنوات		
	أقل من سنتان (5)		
16	**حجم البيانات في النظام (شاملا البيانات خارج الاتصال الشبكي)**		
	أكثر من 10 جيجابايت (5)		
	بين 2 و10 جيجابايت		
	أقل من 2 جيجابايت (1)		

	المعـــايير	درجة الأهمية	النتيجة
	المخاطر المالية		
17	**الاستثمار في النظام** (نقطة الانطلاق/ المستويات تحدد ب X و Y وفق ما يقرره جهاز الرقابة الأعلى)		
	أكثر من Y (5)		
	أكثر من X و أقل من Y وأكثر من هذه المستويات، ان تطلب الأمر (3)		
	أقل من X (1)		
18	**طريقة تمويل النظام**		
	من مصادر داخلية (3)		
	اقتراض (4)		
	قرض من منظمات دولية (5)		
19	**النفقات المتكررة في النظام** نقطة الانطلاق/ المستويات تحدد ب X و Y وفق ما يقرره جهاز الرقابة الأعلى)		
	أكثر من Y (5)		
	أكثر من X وأقل من Y وأكثر من هذه المستويات، ان تطلب الأمر (3)		
	أقل من X (1)		

	المعـــايير	الأهمية	النتيجة
المخاطر التشغيلية / استخدامات النظام			
20	**يستخدم النظام في**		
	العمليات الداخلية فقط (3)		
	العمليات الخارجية فقط (4)		
	العمليات الداخلية والخارجية (5)		
21	**هل يقدم النظام خدمات للمواطنين؟**		
	نعم (5)		
	لا (3)		
الرقابة الداخلية وضمانات التدقيق			
22	**هل صادق طرف ثالث على النظام**		
	نعم (1)		
	لا (5)		
23	**هل تم التدقيق على النظام من قبل مدققين مختصين بتكنولوجيا المعلومات في جهاز الرقابة الأعلى**		
	من قبل ثلاث سنوات (2)		
	من قبل خمس سنوات (4)		
	لم يتم التدقيق عليه (5)		
24	**هل تم وضع ملاحظات خلال عمليات التدقيق السابقة (التدقيق المالي / تدقيق الالتزام / وتدقيق الأداء)**		
	يوجد عدة ملاحظات تدقيق متكررة (5)		
	يوجد ملاحظات تدقيق قليلة متكررة (3)		
	لا توجد ملاحظات تدقيق متكررة (1)		
	لا تعد هذه القائمة شاملة. ويمكن لأجهزة الرقابة العليا أن تحدد المعايير المتعلقة بعملها وتدرجها في الجدول أعلاه		
	النتيجة الاجمالية		

II. تصنيف نظم تكنولوجيا المعلومات

بعد الانتهاء من قائمة تقييم درجة الأهمية المذكورة أعلاه، يمكن لمدقق تكنولوجيا المعلومات استخدام الجدول التالي لتلخيص تقييم نظم تكنولوجيا المعلومات داخل الجهة الخاضعة للتدقيق. ويمكن إنجاز ذلك عن طريق استخدام النتيجة الاجمالية المستخلصة من القائمة واشتقاق تصنيف للمخاطر (وفقا للقسم الثالث أدناه) بالإضافة إلى التصنيف المتوافق لذلك.

اسم نظام تكنولوجيا المعلومات	النتيجة الاجمالية	تصنيف الخطر	الترتيب

III. تصنيف المخاطر

أولويات نظام تكنولوجيا المعلومات	نطاق النتيجة الاجمالية*
أ	L1–L2
ب	>L2 and <L3
ج	>L3 and <L4
د	> L4

*L1, L2, L3, L4 هي نطاقات للنتائج يقررها جهاز الرقابة الأعلى لتصنيف نظم تكنولوجيا المعلومات

وهكذا، يقدم الإطار المذكور أعلاه تصنيفاً لنظم تكنولوجيا المعلومات بالإضافة إلى ترتيب أولويات التدقيق عليها. التصنيف "أ" يمثل أدنى مستوى للخطر، والتصنيف "د" يمثل أعلى مستوى للخطر.

الملحق الثاني

المصفوفة المقترحة للتدقيق على حوكمة تكنولوجيا المعلومات

<table>
<tr><th colspan="2">تحديد وتوجيه ومراقبة احتياجات الأعمال</th></tr>
<tr><td colspan="2">هدف التدقيق: تقييم ما إذا كان قيادة الجهة تقوم بالتوجيه والتقييم والمراقبة على استخدام تكنولوجيا المعلومات في الجهة بشكل فعال لتحقيق اهداف المنظمة.</td></tr>
<tr><td colspan="2">موضوع التدقيق الأول: تحديد متطلبات تكنولوجيا المعلومات
كيف تقوم الجهة بتحديد واعتماد متطلبات الأعمال وتكنولوجيا المعلومات؟</td></tr>
<tr><td colspan="2">المعايير:
توفر خطة لدى الجهة حول الطريقة التي يتم من خلالها تحديد الأعمال المستجدة أو احتياجات تكنولوجيا المعلومات ومدى توفر المعلومات الوافية لدى اللجنة التوجيهية التي تقوم باعتماد المتطلبات لاتخاذ قراراتها.</td></tr>
<tr><td>المعلومات المطلوبة</td><td>وسائل التحليل</td></tr>
<tr><td>• عملية إدارة المتطلبات
• ميثاق اللجنة التوجيهية وقواعد التشغيل بما فيها النطاق المقبول للاعتماد والرفض.
• قائمة بالمتطلبات المعتمدة والمرفوضة.</td><td>• مراجعة الوثائق لضمان أن متطلبات الأعمال الجديدة يتم تحديدها وتحليلها وفقا لإجراءات الجهة حول إدارة المتطلبات.
• مراجعة المتطلبات المعتمدة والمرفوضة لضمان أنها تمت وفقا لقواعد التشغيل المقبولة.
• مقابلة الإدارة أو الأشخاص المسئولين عن اعتماد المشاريع لضمان أنهم يضعون بالاعتبار الإمكانات والمهارات والمصادر والتدريب في مجال تكنولوجيا المعلومات بالجهة، وقدرة المستخدمين على استخدام الأدوات والوسائل أو الإجراءات الجديدة بالشكل الأمثل.</td></tr>
</table>

موضوع التدقيق الثاني: القيادة كيف تقوم القيادة بتوجيه ومراقبة أداء الأعمال وأهداف تكنولوجيا المعلومات بشكل دوري؟	
المعايير: يتم وضع مقاييس الأداء وتقوم اللجنة التوجيهية أو ما يعادلها من اللجان رفيعة المستوى بإجراء مراجعات واجتماعات دورية لاتخاذ القرارات الملائمة، أو أن يكون هناك نظام لتقديم التقارير التي تُطلع الإدارة على حالة مؤشرات الأداء الرئيسية.	
المعلومات المطلوبة	**وسائل التحليل**
• مقاييس الأداء للأعمال وتكنولوجيا المعلومات. • التقارير الدورية حول وضع المشروع. • محاضر اجتماع المراجعات الدورية. • قائمة ببنود الإجراءات وحالتها، إلخ.	• مراجعة نماذج من قرارات أو مذكرات الإدارة للتأكد من أنها واضحة ومثبتة وليست مبهمة. • مراجعة مقاييس الأداء للتأكد أنها تغطي كل من نظم العمل ونظم تكنولوجيا المعلومات. • مراجعة التقارير الخاصة بحالة المشاريع (أو أي وثائق أخرى تستعرض حالة المشاريع مثل (محاضر الاجتماع، والرسائل الإلكترونية، إلخ) لضمان أنها تحتوي على التكلفة، والجدول الزمني ومؤشرات الأداء والاختلافات عن الخطة. • مراجعة بنود إجراءات الإدارة للتأكد من أنه قد تم تكليف أشخاص بأدائها وقد تم متابعها حتى النهاية وتضمين الدروس المستفادة.
موضوع التدقيق الثالث: استثمارات تكنولوجيا المعلومات كيف تدير الجهة استثمارات تكنولوجيا المعلومات؟	
المعلومات المطلوبة	**وسائل التحليل**
• خطة وإجراءات إدارة الاستثمار. • محفظة مشاريع تكنولوجيا المعلومات.	• مقابلة الإدارة لتحديد إجراءات إدارة الاستثمار. • مراجعة المحفظة لتقدير ما إذا تم تحديد أولوية المشاريع وفقا للمعيار المعتمد. • مراجعة تقارير الحالة لتقييم ما إذا كانت تذكر التكلفة ومتابعة الجدول الزمني لتنفيذ المشروع.

• نموذج من تقارير تحليل المنفعة مقابل التكلفة. • قائمة بالمشاريع المعتمدة والمرفوضة والمؤجلة. • تقارير حالة المشاريع المعتمدة. • نموذج عن تقارير تقييم المشاريع بعد انتهائها.	• مراجعة تقارير تحليل المنفعة مقابل التكلفة لتقييم ما إذا كانت مكتملة وتعكس الوضع الفعلي ولا تبالغ في ذكر الفائدة أو تقلل من التكلفة أو الجدول الزمني (يتم الاستعانة باقتصادي أو خبير تكاليف للاستفادة بالشكل الأمثل من الخدمات التي يقدمونها). • بالنسبة للمشاريع المتعثرة، يجب تحديد ما إذا كانت المنهجية المتبعة مناسبة لنوع المشروع وتم تطبيقها بشكل ملائم، وما إذا تم تضمين ضمان الجودة خلال دورة المشروع. • مقابلة الإدارة لتحديد ما إذا تم انهاء أي مشروع بسبب تحقيق فائدة منخفضة او ضعف الأداء. • مقابلة الإدارة لتحديد الطريقة المتبعة في إصدار القرارات حول البناء مقابل شراء الحلول الجاهزة (على سبيل المثال، وفقا للإمكانات والمهارات والتكلفة، والمخاطر، إلخ).
نتائج التدقيق: يقوم المدقق بتعبئتها.	

استراتيجية تكنولوجيا المعلومات
هدف التدقيق: التأكد من وجود استراتيجية لتكنولوجيا المعلومات، تشتمل على خطة لتكنولوجيا المعلومات والعمليات التي من خلالها تم وضع واعتماد وتطبيق وتحديث الاستراتيجية التي تتماشى مع استراتيجيات وأهداف الجهة. وأن يتم إدارة المخاطر والموارد بفعالية خلال انجاز أهداف تكنولوجيا المعلومات.
موضوع التدقيق الرابع: جودة استراتيجية تكنولوجيا المعلومات **هل يوجد لدى الجهة استراتيجية لتكنولوجيا المعلومات تقوم بخدمة وتوجيه وظائف تكنولوجيا المعلومات الخاصة بالجهة؟**
المعايير: وجود خطة استراتيجية لتكنولوجيا المعلومات على مستوى الجهة، تقوم بترجمة أهداف العمل إلى أهداف ومتطلبات لتكنولوجيا المعلومات، وتحدد مصادر تكنولوجيا المعلومات المطلوبة لدعم العمل، على أن يتم مراجعتها وتحديثها بصورة دورية.

المعلومات المطلوبة	وسائل التحليل
• الخطة الاستراتيجية لتكنولوجيا المعلومات أو ما يعادلها. • محاضر الاجتماعات تكنولوجيا المعلومات واللجنة التوجيهية في الجهة.	• مراجعة الوثائق. • مقابلة أصحاب العمل لتحديد ما إذا تم تلبية احتياجاتهم من قبل إدارة تكنولوجيا المعلومات. • المراجعة محاضر اجتماعات لجنة تكنولوجيا المعلومات واللجنة التوجيهية التنظيمية الدورية لضمان تمثيل أصحاب العمل وأن القرارات الاستراتيجية لتكنولوجيا المعلومات قد تم اتخاذها على مستوى اللجنة التوجيهية. • مراجعة استراتيجية تكنولوجيا المعلومات أو مقابلة الإدارة لتحديد متطلبات الموارد والطريقة التي يتم من خلالها تحديدها واعتمادها، ومن الذي يعتمد حيازة الأدوات والموارد الأخرى (الموظفين، والمقاولين، واكتساب المهارات من خلال التدريب، إلخ).

موضوع التدقيق الخامس: إدارة المخاطر كيف تقوم الجهة بإدارة المخاطر؟
المعايير لدى الجهة سياسة وخطة لإدارة المخاطر، وقد خصصت موارد كافية لتحديد وإدارة المخاطر.

المعلومات المطلوبة	وسائل التحليل
• خطة إدارة المخاطر. • قائمة بالمخاطر (بما فيها تكنولوجيا المعلومات) واستراتيجيات المعالجة. • محاضر الاجتماعات الدورية لتقييم المخاطر أو أي اجتماعات أخرى إن وجدت.	• مراجعة خطة إدارة المخاطر أو أي وثائق أخرى لضمان أن مسئوليات إدارة المخاطر قد تم تحديدها بوضوح وأن لا لبس فيها. • مراجعة الوثائق للتأكد من أن مخاطر تكنولوجيا المعلومات تشكل جزءا من الإطار العام لحوكمة المخاطر وتوفقها مع إطار (GRC). • مراجعة محاضر الاجتماعات لضمان أن المخاطر الجديدة قد تم إضافتها وتحليلها بشكل ملائم.

	• مقابلة الأشخاص المسئولين عن إدارة المخاطر لتحديد ما إذا كانت المخاطر التي سيتم تخفيها تم تقدير تكلفتها بشكل ملائم وتم توفير الموارد الملائمة. • مقابلة الإدارة او مراجعة محاضر الاجتماع لتحديد أن القيادة على وعي بمخاطر تكنولوجيا المعلومات والمخاطر الأخرى وأنها تراقب وضع المخاطر بشكل دوري.
نتائج التدقيق: يقوم المدقق بتعبئتها	

الهياكل التنظيمية والسياسات والإجراءات	
هدف التدقيق: التأكد من وجود هياكل تنظيمية وسياسات وإجراءات تمكن الجهة من الوفاء بالمهام الموكلة إليها لتحقيق أهداف العمل.	
موضوع التدقيق السادس: **هل هيكل تكنولوجيا المعلومات في الجهة يمكنها من تحقيق أهداف تكنولوجيا المعلومات واحتياجات العمل؟**	
المعايير: يتم وضع تنظيم تكنولوجيا المعلومات في مستوى عالي في الجهة ويتم تحديد الأدوار والمسئوليات بوضوح بما فيها مهام ومسئوليات مدير تكنولوجيا المعلومات (CIO) أو ما يعادله؟	
المعلومات المطلوبة	**وسائل التحليل**
• الهيكل التنظيمي العام للجهة. • الهيكل التنظيمي لتكنولوجيا المعلومات.	• مراجعة الهياكل التنظيمية للتأكد أن إدارة تكنولوجيا المعلومات تحتل مستوى استراتيجي (على سبيل المثال، يوجد مدير تكنولوجيا المعلومات يرفع التقارير للجنة التوجيهية أو أنه عضوا فيه). • مراجعة الهيكل التنظيمي لتكنولوجيا المعلومات للتأكد أنه يدعم العمل (يوجد مكتب للمساعدة، مدراء لقاعدة البيانات، موظفين أو مقاولين مختصين بالصيانة للمساعدة في تسهيل أعمال تكنولوجيا المعلومات).

موضوع التدقيق السابع: السياسة والإجراءات هل اعتمدت الجهة واستخدمت سياسات وإجراءات ملائمة لإرشاد أعمالها وعمليات تكنولوجيا المعلومات؟	
المعايير: تقوم الجهة بتوثيق واعتماد ونشر السياسات والإجراءات الملائمة لإرشاد عملها ومهامها في مجال تكنولوجيا المعلومات لتحقيق مهامها.	
المعلومات المطلوبة	**وسائل التحليل**
سياسات الجهة بخصوص: • الموارد البشرية بما فيها أمن التوظيف وإنهاء الخدمة، وحفظ الوثائق، التعاقد و/أو الاستعانة بمصادر خارجية، تطوير و/ أو حيازة البرامج وغيرها. • الإجراءات الخاصة بالجوانب المختارة من السياسة. • الرسائل الإلكترونية أو أي وسائل أخرى لإيصال السياسة للمستخدمين وأصحاب المصلحة. • تقارير دورية حول ضمان الجودة للإدارة للإبلاغ عن مدى	• مراجعة السياسات لضمان أنها معتمدة ومحدثة. • على سبيل المثال، مراجعة سياسة الموارد البشرية للتأكد من تحديد متطلبات المهارات، وتحديد التدريب للمعينين الجدد والموظفين الآخرين. • مراجعة مواد التدريب الأساسية والمحدثة أو العمليات الداخلية الأخرى التي يتم من خلالها إيصال هذه السياسات والإجراءات داخل الجهة. • مقابلة أعضاء ضمان الجودة أو المجموعات الأخرى المسئولة عن تطبيق السياسة للاطلاع على عملهم لضمان الالتزام بالسياسات. • مقابلة مجموعة عمل ضمان الجودة أو المسئولين عن الالتزام بالسياسات للاطلاع على طريقة ووقت تقديمهم للتقارير حول النتائج للإدارة العليا. • مقابلة المسئولين عن الالتزام بالسياسات والإجراءات لتحديد عدد التقارير المتعلقة بالنتائج التي يرفعونها للإدارة العليا وكيفية اشارتهم الى عدم الالتزام بسرية أو بصورة مستقلة. • مقابلة المدراء والمستخدمين لاستيعاب مفهومهم وسلوكهم حيال السياسات والإجراءات التي تم تحليلها. وفي حال وجود آراء متكررة: "الإجراءات معقدة" يجب الاستفهام عن كيف يمكن تبسيطها. • مراجعة تاريخ ضوابط التغيير للتأكد من السياسات تحدث بشكل دوري أو حسب الحاجة. • مراجعة تقارير ضمان الجودة للتأكد من أنها تشتمل على الأمور المرتبطة بعدم الالتزام بالسياسات والإجراءات وفق ما هو مناسب.

الالتزام بالسياسات والإجراءات والأمور الأخرى. • طلب التغييرات على السياسة والمراجعة الدورية والنتائج.	• مراجعة الرسائل الإلكترونية أو أي آليات أخرى (البريد العادي، التدريب، الخ) لضمان أن السياسات قد وزعت على المستخدمين وأصحاب المصلحة المناسبين عندما تم تحديثها أو عندما اقتضت الضرورة. • مراجعة السياسات لتحديد كفايتها من خلال البحث عن (على سبيل المثال): نطاق السياسة والتفويض. تحديد الأدوار والمسئوليات. الموارد والأدوات المطلوبة. الربط بين الإجراءات. القوانين التي تحكم التعامل مع عدم الالتزام بالسياسات والإجراءات.
نتائج التدقيق: يقوم المدقق بتعبئتها.	

الأشخاص والموارد	
هدف التدقيق: لتقييم ما إذا يتم تعيين الموظفين المؤهلين والمدربين بشكل كافي وأن لديهم صلاحية للدخول على الموارد الملائمة التي تمكن الجهة من تحقيق أهداف العمل.	
موضوع التدقيق الثامن: الموارد البشرية والخدمات اللوجستية **كيف تتعامل الجهة مع تلبية المتطلبات الحالية والمستقبلية من الأشخاص والموارد؟**	
المعايير: يجب أن يكون لدى الجهة خطة لتلبية متطلباتها الحالية والمستقبلية للوفاء باحتياجات العمل.	
المعلومات المطلوبة	**وسائل التحليل**
سياسات الجهة المتعلقة بالتالي: • الموارد البشرية والتدريب.	• مراجعة السياسات لضمان أنها معتمدة ومحدثة. • مراجعة السياسات لضمان أنها تتطلب من المجموعات المختلفة (تكنولوجيا المعلومات، ضمان الجودة، المستخدمين) تحديد احتياجاتهم الحالية والمستقبلية بخصوص الموظفين والموارد. • مراجعة خطط التوظيف والتدريب لضمان أنها تعكس الاحتياجات المحددة.

• استراتيجية تكنولوجيا المعلومات أو الخطة الاستراتيجية. • خطط التوظيف والتدريب.	• على سبيل المثال، مراجعة سياسة الموارد البشرية للتأكد من تحديد المتطلبات المتعلقة بالكفاءة والتدريب للمعينين الجدد والموظفين الآخرين. • مقابلة مدراء الموارد البشرية أو العمل لتقييم آلية شغل المناصب الهامة في حالات الطوارئ أو الغياب الطويل. • مراجعة مواد التدريب وتجديد المعلومات أو العمليات الداخلية الأخرى التي يتم من خلالها إيصال هذه السياسات والإجراءات داخل الجهة. • مراجعة الخطة الاستراتيجية لتكنولوجيا المعلومات لضمان أنها تتضمن متطلبات الأشخاص والموارد للاحتياجات الحالية والمستقبلية.
نتائج التدقيق: يقوم المدقق بتعبئتها.	

تقدير المخاطر وآليات الالتزام

موضوع التدقيق التاسع: الآلية

كيف تتأكد الجهة أن لديها آلية التزام كافية وفاعلة لضمان أن جميع السياسات والإجراءات يتم اتباعها؟

المعايير:

أن يكون لدى الجهة آلية (من خلال مجموعة عمل ضمان الجودة، أو التدقيق الداخلي، أو الفحص الميداني، إلخ) لضمان أن جميع السياسات والإجراءات يتم اتباعها.

المعلومات المطلوبة	وسائل التحليل
• سياسات وإجراءات الجهة (الأمن، دورة حياة تطوير النظام SDLC، التدريب، إلخ). • الهيكل التنظيمي. • خطة ضمان الجودة.	• اختيار نماذج عن سياسات وإجراءات الجهة لتقييم مدى الالتزام. • مقابلة الإدارة لتحديد المسئولين عن ضمان الالتزام بالسياسات والإجراءات المرتبطة بـ (جزئية التدقيق الذي تم اختياره). • مقابلة فريق أو مجموعة العمل المسئولة عن الالتزام بـ (جزئية التدقيق الذي تم اختياره) لتحديد كيفية إنجازهم لمهامهم. • مراجعة التقارير الواردة من مجموعات العمل المختلفة المعنية بالالتزام للاطلاع على النتائج المسجلة فيها والإجراءات التي تم اتخاذها وما تم إبلاغه للإدارة.

• تقارير فرق أو مجموعات العمل المعنية بالالتزام. • محاضر اجتماع اللجنة التوجيهية.	• مراجعة محاضر اجتماع اللجنة التوجيهية للاطلاع على ما إذا تمت مناقشة موضوعات الالتزام عالية المستوى في هذا الاجتماع أو غيره من الاجتماعات. • مقابلة المسئولين لتحديد أسباب تحديث السياسات والإجراءات. • مراجعة موضوعات عدم الالتزام السابقة والحلول التي تمت. • مراجعة التدريب أو آليات النشر الأخرى (البريد الإلكتروني، المذكرات، الملاحظات) للتأكد من أنه تم ذكر أمور تتعلق بعدم الالتزام.
نتائج التدقيق: يقوم المدقق بتعبئتها.	
انظر الملحق الثالث والملحق الرابع للاطلاع على مصفوفات التدقيق حول التطوير والحيازة وعمليات تكنولوجيا المعلومات.	

الملحق الثالث

المصفوفة المقترحة للتدقيق على التطوير والحيازة

<table>
<tr><th colspan="2">تحديد وإدارة المتطلبات</th></tr>
<tr><td colspan="2">هدف التدقيق: تقييم كيفية قيام الجهة بتحديد متطلباتها من نظم تكنولوجيا المعلومات وترتيبها من حيث الأولوية وإدارتها.</td></tr>
<tr><td colspan="2">موضوع التدقيق الأول:
كيف تحدد الجهة متطلبات المستخدم من نظم تكنولوجيا المعلومات؟</td></tr>
<tr><td colspan="2">المعايير:
لدى الجهة خطة أو إجراءات حول طريقة جمع ومراجعة وتصنيف المتطلبات للوظائف الجديدة أو المضافة.</td></tr>
<tr><td>المعلومات المطلوبة</td><td>وسائل التحليل</td></tr>
<tr><td>• خطة أو إجراءات إدارة المتطلبات.
• عينة من المتطلبات التي تقدم من المستخدمين.</td><td>• مراجعة خطة أو إجراءات إدارة المتطلبات للتأكد أن المستخدمين وأصحاب المصلحة والمستخدمين الآخرين من ذوي الصلة قد شاركوا في تحديد المتطلبات.
• في مسائل تطوير الوظائف الرئيسية لتحسينها، يمكن تنفيذ عملية استشارة المستخدمين وعملية تطوير النموذج التجريبي في نفس الوقت. ويجب النظر في أمر تبادل المعلومات بين أصحاب الأعمال وإدارة تكنولوجيا المعلومات.
• مراجعة عينة من المتطلبات لضمان وجود مراجعة مبدئية وحصر للمتطلبات المتشابهة أو المكررة في مجموعة واحدة.</td></tr>
<tr><td colspan="2">موضوع التدقيق الثاني:
كيف تقوم الجهة بتحليل وإدارة متطلبات المستخدم وترتيبها من حيث الأولويات؟</td></tr>
<tr><td colspan="2">المعايير:
تقوم الجهة بتحليل وإدارة المتطلبات وترتيبها من حيث الأولويات لضمان تلبية احتياجات المستخدم بالشكل الأمثل وبتكلفة فعالة.</td></tr>
</table>

المعلومات المطلوبة	وسائل التحليل
• قائمة بالمتطلبات. • تحليل عينة من المتطلبات. • مصفوفة لتتبع المتطلبات. • معيار لتحديد أولويات المتطلبات.	• مراجعة المتطلبات للتأكد أنها تشمل اسم الكاتب والتاريخ والأولوية والتكلفة والمخاطر والعناصر الأخرى. • مراجعة تحليل المتطلبات أو الملاحظات عليها المقدمة من قبل أصحاب العمل أو أصحاب المصلحة للتأكد أن جميع الآراء تم جمعها وتلخيصها لإجراء التحليل المناسب (القبول، التأجيل، الرفض، إلخ). • مراجعة مصفوفة التتبع للتأكد أن المتطلبات المعتمدة تم تخصيصها لمشاريع التطوير أو الحيازة وأنها تتم متابعتها حتى النهاية عند التنفيذ. • مراجعة المعيار لوضع أولويات المتطلبات لتقييم ما إذا كانت تشمل عناصر مثل التكلفة وحاجة العمل والأمور الطارئة والتفويضات الجديدة.
نتائج التدقيق: يقوم المدقق بتعبئتها.	

إدارة ومراقبة المشاريع	
هدف التدقيق: تقييم الطريقة التي تقوم بها الجهة في إدارة ومراقبة التطوير أو الحيازة لمشاريع تكنولوجيا المعلومات المعتمدة.	
موضوع التدقيق الثالث: كيف تقوم الجهة بالتخطيط للتطوير أو الحيازة لمشاريع تكنولوجيا المعلومات؟	
المعايير: أن يكون لدى الجهة خطة لإدارة كل مشروع معتمد للاسترشاد بها أثناء التنفيذ.	
المعلومات المطلوبة	**وسائل التحليل**
• خطة إدارة المشروع أو ما يعادلها.	• مراجعة خطة إدارة المتطلبات أو ما يعادلها للتأكد أنها تشمل الوصف والنطاق والتكلفة والجدول الزمني والمخاطر والهيكل الإداري للمشروع وأنها تحدد أصحاب المصلحة (الداخليين والخارجيين). • مراجعة الخطة للتأكد من اعتمادها من قبل الإدارة العليا وأنها تشتمل على ملاحظات أصحاب المصلحة.

	• مراجعة الهيكل التنظيمي للمشروع لتحديد أدوار المسئولين عن ضمان أو اختبار الجودة وتطوير وتركيب النظام على البنية التحتية لتكنولوجيا المعلومات في الجهة ومجموعة الدعم، إلخ. • بالنسبة لمشاريع الحيازة، يجب التأكد أن الخطة أو ما يعادلها تشتمل على الاشخاص المسئولين عن مراقبة المقاول ومراجعة اعتمادات المسئولين. • مقابلة مدراء المشاريع لتحديد طريقة دورة حياة تطوير النظام المستخدمة في تطوير المشروع.
موضوع التدقيق الرابع: **كيف تقوم الجهة بالرقابة على مشاريع تكنولوجيا المعلومات؟**	
المعايير: تقوم الجهة بالرقابة على المشاريع ومتابعتها للتأكد من تنفيذها حسب المتطلبات من حيث التكلفة والجدول الزمني والأداء.	
المعلومات المطلوبة	**وسائل التحليل**
• تكلفة المشروع والجدول الزمني الأساسي (التقديرات التي وضعت في الخطة المشروع). • تقارير حالة المشروع • تقارير الحالة الخاصة بالمقاولين (اتفاقية مستوى الخدمة SLA). • نتائج المراجعات. • بنود العمل.	• مقارنة تكلفة المشروع والجدول الزمني الأساسي مع تقارير حالة المشروع لتقييم الاختلافات بين كل من تكلفة وزمن تنفيذ المشروع الأساسية والفعلية. • مقابلة مدير المشروع/ مراجعة التقارير للتأكد أنه تم اتخاذ الإجراءات التصحيحية اللازمة للاختلافات الرئيسية (بين الخطة والتنفيذ). • مقابلة فريق إدارة المشروع ومراجعة محاضر الاجتماعات مع المقاولين لتقييم تكرار وفعالية مراقبة أنشطة المشروع التي تم فيها الاستعانة بمصادر خارجية. • مراجعة اتفاقية مستوى الخدمة أو العقد للتأكد من تطبيق الشروط المنصوص عليها في العقد، على سبيل المثال، مقابلة المقاولين الذين يجرون مراجعات دورية، وتوفير تقارير الحالة، وتتبع بنود العمل، وعمل أنشطة لإدارة المخاطر وفقا لعقد ومقابلة المسئول عن العقد في الجهة لتحديد كيف تتم إدارة المقاول في حال عدم وجود اتفاقية مستوى الخدمة.

ضمان الجودة والفحص

هدف التدقيق: تقييم الطريقة التي تتأكد فيها الجهة أن مشاريع تكنولوجيا المعلومات الخاضعة للتطوير أو الحيازة تحقق أهداف الجودة التي وضعت لها.

موضوع التدقيق الخامس:

هل لدى الجهة هيكل لضمان الجودة وهل الأدوار والمسئوليات محددة؟

المعايير:

وجود إجراءات لأداء أنشطة ضمان الجودة.

المعلومات المطلوبة	وسائل التحليل
• سياسة أو خطة ضمان الجودة. • إجراءات ضمان الجودة. • أدوار ومسئوليات مجموعة العمل المعنية بضمان الجودة أو الأفراد القائمين عليها. • دورة حياة تطوير النظم التي تم تبنيها للمشروع.	• مراجعة سياسة أو خطة ضمان الجودة لتحديد المجموعات أو الأفراد المسئولين عن القيام بأنشطة ضمان الجودة في المشروع (على سبيل المثال، يتعين على مجموعة العمل المعنية بضمان الجودة مراجعة الوثائق لضمان أنها تعكس بدقة المتطلبات ومراجعة أدلة المستخدم للتأكد من وضوحها وتكامل العناصر أو الخطوات فيها). • مراجعة إجراءات ضمان الجودة أو مقابلة القائمين عليها للتأكد من الأنشطة التي يقومون بها (مراقبة مراجعات النظراء والوقوف على التصميم وغيرها من المراجعات، إلخ). • مراجعة التقارير الواردة من جهة ضمان الجودة لتحديد ما تم مشاهدته أثناء التدقيق على الجودة (مدى التزام فريق المشروع بخطة إدارة المشروع، ودورة حياة تطوير النظم التي تم تبنيها والمراجعات الأخرى المرتبطة بذلك، إلخ) ولمن تقدم هذه التقارير.

موضوع التدقيق السادس:

كيف تقوم الجهة بالتخطيط وإنجاز عمليات اختبار نظم تكنولوجيا المعلومات؟

المعايير:

تقوم الجهة باختبار نظم تكنولوجيا المعلومات وبناء على نتائج الفحص يتم اعتماد أو رفض النظام.

المعلومات المطلوبة	وسائل التحليل
• خطة الفحص. • جدول الفحص الزمني. • نتائج الفحص • معيار القبول والرفض.	• مراجعة خطط الفحص. • مقارنة التكلفة التقديرية والجدول الزمني التقديري مع تقارير حالة المشروع لتقييم الاختلافات إن وجدت. • مقابلة مدير المشروع/ مراجعة التقارير للتأكد من اتخاذ الإجراءات التصحيحية اللازمة للاختلافات الرئيسية بين الخطة والتنفيذ. • مقابلة فريق إدارة المشروع ومراجعة محاضر الاجتماعات مع المقاولين لتقييم تكرار وفعالية مراقبة أنشطة المشروع التي تم فيها الاستعانة بمصادر خارجية. • مراجعة اتفاقية مستوى الخدمة أو العقد للتأكد من تطبيق الشروط المنصوص عليها في العقد، على سبيل المثال، التأكد من ان المقاولين يجرون مراجعات دورية، ويقدمون تقارير عن حالة المشروع، ويقومون بتتبع بنود العمل، ويقومون بعمل أنشطة لإدارة المخاطر وفقا للعقد ومقابلة المسئول عن العقد في الجهة لتحديد كيف تتم إدارة المقاول في حال عدم وجود اتفاقية مستوى الخدمة.
نتائج التدقيق: يقوم المدقق بتعبئتها.	

استدراج العروض (Solicitation)
هدف التدقيق: تقييم الطريقة التي تضمن الجهة فيها أن عمليات استدراج العروض (مجموعة المهام مثل توثيق الاحتياجات وصياغة مستند طلب تقديم العروض، وتقييم العروض، والاستيضاح قبل تقديم العروض، وتصميم وطرح المناقصة، والتقييم، إلخ وصولا الى ترسية المناقصة) متوافقة مع الخطة أو الإجراءات المعتمدة لهذا الموضوع.
موضوع التدقيق السابع: **ما هي الخطة أو الإجراءات المعتمدة لأنشطة استدراج العروض؟**
المعايير: يجب إنجاز أنشطة استدراج العروض بما فيها اختيار الموردين وفقا لخطة الجهة المعتمدة لاستدراج العروض.

المعلومات المطلوبة	وسائل التحليل
• خطة أو إجراءات استدراج العروض. • حزمة استدراج العروض. • مراجعة المستخدم للمتطلبات. • مراجعة المستخدم لحزمة استدراج العروض. • القوانين المنطبقة التي تحكم عملية استدراج العروض.	• مراجعة خطة استدراج العروض للتأكد أنها تشمل جوانب مثل مشاركة المستخدم، استدراج العروض على أساس تنافسي، دراسة حالة السوق قبل التعاقد ان انطبق ذلك، اختيار المورد يتم بناء عن جدارة. • مقابلة المسئولين الرئيسيين عن التعاقد لتقييم كيفية ضمان تكامل حزمة دراسة العروض (على سبيل المثال، عن طريق قيام المستخدمين وأصحاب المصلحة والخبراء، حسب الملاءمة، بمراجعتها). • مقابلة المستخدمين أو أصحاب المصلحة لضمان أنه قد تم استشارتهم خلال فترة وضع المتطلبات أو أنهم قد اعتمدوا المتطلبات الفنية لعملية استدراج العروض والحزمة النهائية للمناقصة. • مقابلة المسئولين عن التعاقد لتقييم الطريقة التي يتم من خلالها التأكد من التزام عملية استدراج العروض بالقوانين واللوائح.

موضوع التدقيق الثامن:

على أي أساس تقوم الجهة باختيار الموردين؟

المعايير

تقوم الجهة باستخدام معايير نزيهة ومعلنة لاختيار جميع الموردين.

المعلومات المطلوبة	وسائل التحليل
• معايير اختيار الموردين. • مصفوفة نتائج تقييم الموردين أو ما يعادلها.	• مراجعة معايير اختيار الموردين لضمان أنها تعكس الغاية من استدراج العروض (على سبيل المثال، في عقد شراء برنامج كمبيوتر لا يجب على المورد أن يضع مقاييس غير ضرورية للجهة). • مقابلة أصحاب المصلحة الرئيسيين لتقييم مدى موافقتهم على معايير الاختيار. • مراجعة مصفوفة نتائج تقييم الموردين أو ما يعادلها للتأكد أنها تتوافق مع معايير الاختيار.

نتائج التدقيق: يقوم المدقق بتعبئتها.

إدارة الإعدادات (Configuration Management)	
هدف التدقيق: تقييم الطريقة التي تقوم بها الجهة في إدارة الإعدادات المرتبطة بالتطوير والحيازة	
موضوع التدقيق التاسع: ما السياسة التي تستخدمها الجهة لإدارة الإعدادات؟	
المعايير: يتم إنجاز أنشطة إدارة الإعدادات بالتوافق مع سياسات وإجراءات الجهة.	
المعلومات المطلوبة	**وسائل التحليل**
• سياسة أو إجراءات إدارة الإعدادات أو ما يعادلها.	• مراجعة مدى ملاءمة سياسة إدارة الإعدادات عن طريق بحث التالي (على سبيل المثال): • نطاق السياسة والتفويض. • تحديد الأدوار والمسئوليات. • الموارد والأدوات المطلوبة. • الربط مع الإجراءات. • القوانين التي تتعامل مع عدم الالتزام. • مقابلة المسئولين عن إدارة الإعدادات في حال عدم وجود سياسة محددة وذلك لتقييم كيفية قيامهم بالتأكد من أن المهام يتم أداؤها بشكل موحد في الجهة.

موضوع التدقيق العاشر:

من المسئول عن التصريح بإجراء التغييرات والتثبيت النهائي في بيئة الإنتاج؟

المعايير:

يجب إدخال التغييرات المصرح بها والمعتمدة فقط في بيئة الإنتاج.

المعلومات المطلوبة	وسائل التحليل
• المجموعة أو الأفراد المسئولين عن التصريح بالتغييرات. • عمليات الاعتماد وتقديم التغييرات المعتمدة والتي تم اختبارها لبيئة الإنتاج.	• التأكد من وجود مجموعة تقوم بالسماح بعمل تغييرات على منتجات العمل. يمكن أن تكون المجموعة مجلس الرقابة على التغييرات أو ما شابه ذلك وتكون مهمته مراجعة واعتماد التغييرات. • مقابلة الموظف المسئول عن الموافقة على تقديم برامج جديدة لبيئة الإنتاج لضمان أن البرنامج الذي تم اختباره (بما في ذلك فحص الانحدار regression testing مع النظم الأخرى إذا لزم الأمر)، ويتوافق مع معايير القبول ويتضمن الوثائق المناسبة ويتضمن تدريب المستخدمين (ان لزم الأمر) قبل استخدامه في العمل. • مقابلة الموظف المسئول عن الموافقة على عمل التغييرات على النظام الفعلي المستخدم لتحديد كيف يقوم بمراقبة ومنع عمل تعديلات على النظام لم يتم الموافقة عليها (على سبيل المثال، عن طريق التحكم بالدخول على نظام المستخدم في البيئة الفعلية، وفصل بيئات الإنتاج والتطوير، إلخ).

نتائج التدقيق:

يقوم المدقق بتعبئتها.

الملحق الرابع

المصفوفة المقترحة للتدقيق على عمليات تكنولوجيا المعلومات

إدارة الخدمات	
هدف التدقيق: تقييم ما إذا كانت إدارة تكنولوجيا المعلومات تراقب بشكل فعال عمليات تكنولوجيا المعلومات ضمن اتفاقية مستوى الخدمة الداخلية أو عقد.	
موضوع التدقيق الأول: المقاييس الرئيسية **ما هي المقاييس الرئيسية للخدمة المشمولة في اتفاقية مستوى الخدمة الداخلية بين إدارة العمل وإدارة تكنولوجيا المعلومات؟**	
المعايير: أفضل ممارسات اتفاقية مستوى الخدمة وهي عبارة عن التالي: توزيع المسئوليات بين أصحاب العمل ومجموعة دعم تكنولوجيا المعلومات، ووضع أهداف عمل موثقة لإدارة الشبكات، وتقديم وقياس الخدمات، وتحديد أنواع المشاكل ومسئوليات مكتب المساعدة.	
المعلومات المطلوبة	**وسائل التحليل**
• اتفاقية مستوى الخدمة الداخلية في الجهة بين أصحاب العمل وإدارة تكنولوجيا المعلومات. مسئوليات مكتب المساعدة. تقارير الخدمة. وقت استجابة المستخدم/ التطبيق.	• مراجعة اتفاقية مستوى الخدمة للتأكد من احتوائها على العناصر الملائمة من حيث وجود أهداف مستوى الخدمة وبشكل تفصيلي وقابل للقياس، والنظم والخدمات المشمولة، وجودة الخدمات، والخدمات غير المشمولة، ودعم التطبيقات وحل المشاكل بها، ومدى توفر النظام، وساعات عمل مكتب المساعدة، والزمن المستغرق في الاستجابة وحل المشاكل وفقاً لتصنيف أهمية المشكلة، والانتاجية، وجداول الصيانة، وغيرها. • مراجعة ما إذا كانت طرق الاحتفاظ بالبيانات الاحتياطية واستردادها تتوافق مع معايير خطة استمرارية الأعمال في الجهة. • مراجعة ما إذا كان أصحاب العمل قد وقعوا على الاتفاقية. • مقابلة عينة من المستخدمين لمعرفة مستوى الوعي لديهم.

موضوع التدقيق الثاني: الالتزام ما هي الآليات الموضوعة لضمان التقيد المستمر باتفاقية مستوى الخدمة؟	
المعايير: أن يتم تطبيق ومتابعة اتفاقية مستوى الخدمة وتعديلها عند الضرورة.	
المعلومات المطلوبة	**وسائل التحليل**
• المؤشرات التشغيلية في اتفاقية مستوى الخدمة. • مواعيد تقديم التقارير. • الجداول أو الرسوم البيانية التي توضح نجاح أو فشل هذه الاتفاقيات بمرور الوقت. • وثائق الاجتماعات الدورية التي تستعرض تحليل الأسس والاتجاهات الحديثة. • المؤشرات التشغيلية مثل معدلات القصور، الطلبات المقدمة إلى مكتب المساعدة، مسارات الاتصالات الأخرى، والمدة المستغرقة في الاستجابة، ووقت تنفيذ المهام الجديدة، ووثائق التغييرات، والمواقع التي يتم فيها تقديم الخدمات والحوافز والشروط الجزائية (يكون لها أهمية خاصة إذا كانت خدمات دعم تكنولوجيا المعلومات قد تمت بالاستعانة بمصادر خارجية).	• مراجعة التقارير اليومية أو الدورية أو غيرها التي تعدها إدارة تكنولوجيا المعلومات، والتأكد من أنه يتم مراقبة جميع المؤشرات المتفق عليها من خلال التقارير أو الرسوم البيانية أو غيرها. • مراجعة التقارير لفحص البنود التي خضعت للقياس وتعتبر هامة للإدارة. • مراجعة الوثائق للتحقق مما إذا كانت تقارير أنشطة مكتب المساعدة تنظر فيها الإدارة ويتم مقارنتها بطلبات المساعدة، وتتم الإشارة إلى القضايا الأساسية فيها للمساعدة في اتخاذ قرار الشراء، ولإجراء المراجعة الدورية على اتفاقية مستوى الخدمة بحد ذاتها. • مقابلة موظفي تكنولوجيا المعلومات في الجهة والنظر في طبيعة الإشراف على موظفي مكتب المساعدة، وأدوات المراقبة المستخدمة، وتحديد أولويات مهام الدعم، وتوفير أساسيات الشبكة والتطبيقات، وتوفير البيانات في الوقت المناسب، ومدى تكرار عمليات النسخ الاحتياطي للبيانات، والتحقق من صلاحية البيانات الاحتياطية، وذلك للتحقق من مدى اذعان اتفاقية مستوى الخدمة للمتطلبات. • التحقق من الإجراءات المتخذة من قبل وحدة تكنولوجيا المعلومات أو من قبل إدارة الجهة في حالة الاستعانة بمصادر خارجية لأداء مهام تكنولوجيا المعلومات – إذا كانت المؤشرات التشغيلية لا تتفق مع متطلبات اتفاقية مستوى الخدمة.

موضوع التدقيق الثالث: الفعالية هل تكفل إدارة خدمات تكنولوجيا المعلومات رضا المستخدمين وتساعد على تحقيق أهداف الجهة؟	
المعايير: تحقيق مقاييس الأداء التي تتفق مع احتياجات وأهداف العمل.	
المعلومات المطلوبة	**وسائل التحليل**
• يقوم مكتب المساعدة بتسجيل محاضر الاجتماعات بين أصحاب العمل وإدارة تكنولوجيا المعلومات. • مراجعة اتفاقية مستوى الخدمة بشكل دوري.	• مقابلة عينة من المستخدمين (مستويات مختلفة) أو إجراء مسح حول عن مدى الرضا على جودة خدمات مكتب المساعدة، ومجموعة دعم تكنولوجيا المعلومات. • مراجعة تقارير مكتب المساعدة للتحقق مما إذا كانت نسبة كبيرة من القضايا المهمة للخدمات تم منعها قبل أن تدون عليها ملاحظة من قبل المستخدمين. • التحقق ما إذا كان الوقت المحدد لحل القضايا المنظورة أقل مما حددته معايير اتفاقية مستوى الخدمة. • التحقق ما إذا كان يتم مراجعة بنود اتفاقية مستوى الخدمة من قبل الإدارة بشكل دوري ودراسة مشاكل جودة الخدمات.
نتائج التدقيق: يقوم المدقق باستيفائها.	

إدارة القدرات
هدف التدقيق: تقييم ما إذا كانت إدارة تكنولوجيا المعلومات تضمن أن قدرة النظام وأدائه تفي باحتياجات العمل الحالية والمستقبلية.
موضوع التدقيق الرابع: الاتفاق على البنود هل توجد اتفاقية موثقة بين الإدارة ووحدة تكنولوجيا المعلومات يتم استخدامها كقاعدة لاختيار المقاييس التشغيلية لعمليات تكنولوجيا المعلومات؟
المعايير: حوكمة تكنولوجيا المعلومات – متابعة ومراقبة تنفيذ الاستراتيجية بطرق قياسية.

المعلومات المطلوبة	وسائل التحليل
• اتفاقية داخلية لمستوى الخدمة أو أي نوع آخر من الاتفاقيات. • من المؤشرات التشغيلية لتكنولوجيا المعلومات – توفر معالج الموارد، متوسط وقت تسجيل الدخول على النظام، والنسبة المئوية لتوقف النظام عن العمل، ومتوسط الزمن المستغرق في استجابة النظام، وغيرها.	• مراجعة الاتفاقية أو إرشادات التشغيل التي يستخدمها فريق تكنولوجيا المعلومات، والتأكد من أنه قد تم مراجعتها واعتمادها من قبل المستخدمين المعنيين أو الإدارة التنفيذية العليا. • مقارنة مؤشرات الأداء الأساسية (مثل توافر موارد الشبكة، وزمن الاستجابة) التي حددتها إدارة تكنولوجيا المعلومات مع إرشادات التشغيل التي وضعها أصحاب العمل للتحقق من أن إدارة تكنولوجيا المعلومات تتبع ارشادات التشغيل.

موضوع التدقيق الخامس: المراقبة

هل تقوم إدارة تكنولوجيا المعلومات بجمع ومراجعة بيانات أداء النظام بصورة دورية ليتوافق مع احتياجات العمل؟

المعايير:

أفضل الممارسات من جانب مسئولي النظام والشبكات محددا خط الأساس للأداء، وجمع معلومات حول حركة البيانات وتشغيل النظام، وتوفر الموارد للنظام، ومراقبة إحصائيات البيانات ونزعة حركتها، وتحليلات–ماذا–إذا، واستخدام الأدوات لتحديد أسباب تدهور الأداء.

المعلومات المطلوبة	وسائل التحليل
• التقارير، وبنود العمل، والوقت المستغرق لاستجابة مكتب المساعدة، والقياسات الأخرى.	• استخدام قضايا الالتزام في مصفوفة اتفاقية مستوى الخدمة، والاهتمام بشكل خاص بجميع العناصر التي تؤثر على القدرات، مثل، مقارنة مقاييس القدرات الفعلية مع متطلبات اتفاقية مستوى الخدمة، وغيرها.

موضوع التدقيق السادس: تحليل بيانات الأداء

هل تم تحليل وضبط بيانات الأداء لتحقيق الكفاءة وتجنب القيود المفروضة على القدرة؟ وإن لزم الأمر، هل خططت إدارة تكنولوجيا المعلومات للحصول على موارد اضافية لتلبية احتياجات العمل؟ هل تقوم إدارة تكنولوجيا المعلومات بتوظيف أو تدريب، أو إبرام عقود للتوظيف لتلبية احتياجات العمل للتغيير؟

المعايير:

تحديد المؤشرات في الاتفاقية كما جاءت في دليل أفضل الممارسات في ضبط الأداء (الذاكرة، وتحسين الوقت المستغرق لاستجابة الشبكة، ونظام التشغيل، المدخلات/المخرجات، وكفاءة تصميم مخطط قاعدة البيانات، وجدولة المهام وفقا للأولويات والموارد المطلوبة، وتحسين أو ضبط إجراءات التعامل مع قضايا القدرات سواء على أساس ردود الفعل أو على المدى الطويل).

المعلومات المطلوبة	**وسائل التحليل**
• التقارير، والإجراءات، وتقارير الحالة، والرسوم البيانية لقياس الأداء. • محضر اجتماع على مستوى أعلى إدارة لتكنولوجيا المعلومات.	• مراجعة التقارير التي تصدرها إدارة تكنولوجيا المعلومات يوميا أو في أي إطار زمني آخر، والتأكد أنها تنتج وتحلل نزعة البيانات، وتحدد معوقات البحث عن بنود الإجراءات، وتسجيل الاستثناءات بالنسبة لقضايا القدرات، ثم مقارنتها بمتطلبات اتفاقية مستوى الخدمة. • مقارنة التقارير/ الرسوم البيانية للتحقق من الأعمال الإجرائية التي اتخذت استجابة للتقارير. • مناقشة محاضر الاجتماعات وإيجاد ما إذا كانت قضايا التوظيف في إدارة تكنولوجيا المعلومات ومشاكل القدرات وأي احتياجات إضافية من الموارد قد أبرزت في الوقت المناسب.

نتائج التدقيق:

يقوم المدقق باستيفائها.

إدارة المشاكل والحوادث الطارئة	
هدف التدقيق: تقييم فعالية السياسات والإجراءات المتبعة في إدارة المشاكل والحوادث في الجهة.	
موضوع التدقيق السابع: الوعي بالسياسات هل توجد سياسة موثقة للاستجابة للحوادث الطارئة وهل المستخدمين على علم بها؟	
المعايير: أفضل الممارسات في الاستجابة للحوادث الطارئة.	
المعلومات المطلوبة	**وسائل التحليل**
• سياسة الجهة في الاستجابة للحوادث الطارئة. • إرشادات للتواصل مع الأطراف الخارجية بخصوص الحوادث الطارئة.	• مراجعة السياسات للتأكد أنها تحتوي على مراحل مناسبة مثل الإعداد، والتحري والتحليل، والاحتواء والقضاء على المشكلة، ونشاط ما بعد الحادث الطارئ. • التحقق مما إذا كانت السياسة تحدد المسئوليات والنطاق ومتطلبات إعداد التقارير. • مراجعة الإجراءات الفعلية التي يتم من خلالها توعية المستخدمين بالسياسة العامة وطبيعة الاتصالات بين فريق الاستجابة للحوادث الطارئة وأصحاب المصلحة. • مقابلة عينة من المستخدمين في الجهة للتأكد من مدى وعيهم بخطة الاستجابة للحوادث الطارئة.

موضوع التدقيق الثامن: الكفاءات والموارد هل هناك فريق عمل مختص بالاستجابة للحوادث الطارئة يتمتع بكفاءة مناسبة ومزود بالأدوات والموارد، ومدعوم من قبل الإدارة العليا لمعالجة هذه الحوادث الطارئة؟
المعايير: أفضل الممارسات في الاستجابة للحوادث الطارئة – الإرشادات المقدمة من المعهد الوطني للمعايير والتكنولوجيا NIST – وفق ما ورد في اتفاقية مستوى الخدمة.

المعلومات المطلوبة	وسائل التحليل
• سياسة وخطة الاستجابة للحوادث الطارئة. • ميثاق فريق الاستجابة للحوادث الطارئة، المحتوى والخبرة. • اتفاقية مستوى الخدمة SLA. • التدريب في مجال التوعية في الاستجابة للحوادث، ورفع مستوى استراتيجية كفاءة فريق عمل الاستجابة للحوادث الطارئة. • قائمة أدوات التسجيل والتطبيقات المستخدمة في مراقبة الشبكة واستخدامها.	• التحقق من وجود ميثاق يتبعه الفريق في التحقيق بالحوادث الطارئة. • البحث في خبرات أعضاء الفريق في مجال الشبكات ونظم التشغيل والأمن وكيفية إدارتهم للعمل. • مراجعة إجراءات مكتب الخدمة للتحقق من وجود إجراءات تصعيدية للأحداث التي لا يمكن حلها فورا وفقا لفئات المخاطر المحددة في اتفاقية مستوى الخدمة. • مراجعة الإجراءات التي تم اتخاذها سابقا في معالجة الحوادث الطارئة. • مراجعة تقارير الحالة للتحقق من أن الموظفين المناسبين قد شاركوا في التحقيق في الحوادث الطارئة. • التحقق من الأدوات المستخدمة في إدارة الحوادث الطارئة – وهل هي ملائمة لاحتياجات الجهة؟ • التحقق من أن الجهة قد وضعت معايير وإجراءات لتسجيل الدخول وذلك لضمان دقة المعلومات المجمعة بواسطة التسجيل وبرنامج الأمن وأن البيانات يتم مراجعتها بانتظام.

موضوع التدقيق التاسع: فعالية الاستجابة

هل ينتج عن استراتيجية الاستجابة استجابات فعالة للأحداث الطارئة؟

المعايير:

أفضل الممارسات في الاستجابة للحوادث الطارئة (مثل COBIT 5 DSS domain ومكتبة البنية التحتية لتكنولوجيا المعلومات في مجال دعم الخدمات ITIL).

المعلومات المطلوبة	وسائل التحليل
• بنود إجراءات الاستجابة للحوادث	• التحقق من تحديد أولويات الاستجابة / التعامل مع الحوادث الطارئة لكل من الأصول أو الخدمات.

الطارئة كسجلات الاستمارات وغيرها. • التدريب الدوري على الوعي الأمني. • إجراءات التعامل مع الحوادث الطارئة – إرشادات لتحديد أولويات الحوادث الطارئة. • تقارير الحالة والإجراءات التي تم اتخاذها.	• التحقق ما إذا كانت الإجراءات تسهل التقاط وتحليل البيانات سريعة الزوال[50] والبيانات الثابتة في الوقت المناسب. • التحقق مما إذا كان فريق الاستجابة يقوم بشكل دوري بتوعية المستخدمين بالسياسات والإجراءات فيما يتعلق بالاستخدام الملائم للشبكات والنظم ووسائل الإعلام الخارجية والتطبيقات. • مراجعة الوثائق لمعرفة ما إذا كانت أنشطة ما بعد الحوادث مثل الدورات التدريبية التذكيرية قد أعطيت للمستخدمين لتجنب تكرار حوادث كبيرة مكلفة. • التأكد من أنه تم تحديد مصدر الحادث الطارئ، ومعرفة المبادرات التي اتخذت، (تغيير في الإجراءات، لفت نظر، التدريب، وغيرها). • التحقق مما إذا كانت سجلات فريق الاستجابة للحوادث الطارئة قد سجلت جميع الحوادث التي تم حلها بالتفصيل وتم مراجعة المعلومات لاحتمال القيام بتحديث على قاعدة بيانات الخبرات المكتسبة.
نتائج التدقيق: يقوم المدقق باستيفائها.	

إدارة التغيير
هدف التدقيق: تقييم ما إذا نفذت الجهة إجراءات معيارية للتحكم بكافة التغييرات على أنظمة وتطبيقات تكنولوجيا المعلومات الأساسية.
موضوع التدقيق العاشر: السياسات **هل لدى الجهة سياسة معتمدة لإدارة التغيير وتشتمل على الضوابط المطلوبة خلال دورة التغيير؟**
المعايير: أفضل الممارسات في ضوابط التغيير: طلب التغيير – التحقق من صحة المطلوب – القبول – تحديد الأولويات – تصميم التغيير – اختبار التغيير – التنفيذ – التوثيق.

[50] البيانات سريعة الزوال هي البيانات التي يتم تغييرها مع مرور الوقت أو إعادة الكتابة عليها، حيث لا يمكن الحصول على صورة سريعة للمعلومات بدون التقاطها بشكل تفاعلي، أو من خلال عملية مجدولة بانتظام لاستخلاص البيانات.

المعلومات المطلوبة	وسائل التحليل
• سياسات وإجراءات إدارة التغيير، والمخططات البيانية للعمليات. • ميثاق مجلس إدارة مراقبة التغيير. • الجدول الزمني لمراجعة السياسة. • توثيق التغيير: طلب التغيير، إجراءات اختبار ضوابط التغيير، خطة ضمان الجودة، وخطة وإجراءات الاختبار. • تقارير وسجلات برنامج إدارة التغيير. • محاضر اجتماع مجلس إدارة مراقبة التغيير. • التقارير الموجزة الصادرة عن إدارة التغيير التي تنظر فيها الإدارة.	• الرجوع للمتطلبات العامة للسياسات والإجراءات في جزئية حوكمة تكنولوجيا المعلومات. • مراجعة وثيقة سياسة إدارة التغيير للتحقق من أن قبل مباشرة الإجراءات، ومراجعة التغيير والموافقة عليه، أنه يتم تحديد المسئوليات الخاصة بهذه المهام. • مراجعة ميثاق مجلس مراقبة التغيير لتحديد المسئوليات ومستوياتها. • مقابلة الموظفين، وملاحظة الممارسات الفعلية ومراجعة الوثائق للتأكد من أنه يتم اتباع إجراءات إدارة التغيير: طلب التغيير، ومتابعة التغيير إلى البيئة التشغيلية، التأكد من اتباع الإجراءات المطلوبة مثل تنقيح الإدارة وتحديد الأولويات قد تم اتباعها، والبحث عن الموافقات والتوثيقات. • التحقق من قيام قسم ضمان الجودة الداخلية بالتدقيق، والتحقق من وجود مراجعة وافية للسجلات والتقارير من قبل الإدارة التي تم فيها استخدام برنامج إدارة التغيير. • التأكد أن صلاحية الدخول على مكتبة البرامج (مثل رمز المصدر، والتهيئة البرمجية) يقتصر على موظفي إدارة التغيير وأن إدارة تكنولوجيا المعلومات تمنع التغييرات غير المصرح بها في البيئة التشغيلية. • مراجعة الوثائق وملاحظة الممارسات للتأكد أن المستخدمين لهم دور في اختبار التغييرات لضمان صحتها. • التأكد أن التغييرات على البرنامج تم الموافقة عليها من قبل أصحاب المصلحة قبل تطبيقها فعليا.

موضوع التدقيق الحادي عشر: إجراءات التراجع كيف تضمن إدارة تكنولوجيا المعلومات أن بإمكان الجهة الرجوع للنسخة السابقة ان دعت الحاجة لذلك؟	
المعايير: أفضل الممارسات في إدارة التغيير – توثيق الإجراءات والمسئوليات لاسترجاع الجوانب المتضررة من تأثير التغييرات غير المرغوب بها.	
المعلومات المطلوبة	**وسائل التحليل**
• إجراءات إدارة التغيير. • توثيق اختبار وتنفيذ التغيير. • وثائق استعادة الأوضاع وسجلات ضبط النظام (Configuration). • الإجراءات الاحتياطية واستعادة الأوضاع.	• مراجعة الوثائق، ومقابلة المستخدمين لاكتشاف ما إذا كانت هناك تأثيرات غير مقصودة للتغييرات/التطويرات التشغيلية وأنها تم تصنيفها إلى أولويات تتوافق مع اهتمامات الأعمال.

موضوع التدقيق الثاني عشر: التغييرات الطارئة هل يتم مراقبة التغييرات الطارئة بشكل مناسب عندما يتعذر اتباع إجراءات إدارة التغيير المعتمدة لتحديد التغييرات ومنح الصلاحية للقيام بها واختبارها وتوثيقها؟	
المعلومات المطلوبة	**وسائل التحليل**
• إجراءات الرقابة على التغييرات الطارئة. • توثيق التغييرات الطارئة التي تمت خلال فترة التدقيق.	• مراجعة إجراءات إدارة التغيير لتحديد ما إذا كانت تشتمل على قسم متخصص ومجموعة إجراءات لمراقبة التغييرات الطارئة على النظام. • طلب مثال عن تغيير طارئ، ومقارنته بالإجراءات الموثقة، ومراجعة الاختبار الذي أجري قبل إدخاله على بيئة الإنتاج، وفي حال عدم وجود إجراءات موثقة، يتم الاستفسار عن كيفية معرفة التصرف ومن الذي يعتمد التغييرات. • التأكد من أن التغييرات الطارئة معتمدة من قبل عضو مناسب في الإدارة قبل الانتقال إلى الإنتاج.

موضوع التدقيق الثالث عشر: الانتهاء من التغيير وتوثيقه هل هناك إجراءات مناسبة متبعة لتحديث النظم المرتبطة بهذا التغيير ووثائق المستخدم بعد أن يتم تطبيق التغيير؟	
المعايير: أفضل الممارسات في إدارة التغيير (مثل COBIT 5–BAI domain، ومكتبة البنية التحتية لتكنولوجيا المعلومات في مجال دعم الخدمات ITIL).	
المعلومات المطلوبة	**وسائل التحليل**
• عملية توثيق الوظائف المتأثرة بالتغيير. • الإجراءات المعمول بها في التوثيق.	• مراجعة الوثائق لضمان الشمول والاستقامة في تنفيذ التغييرات، وهل الإجراءات التنفيذية، ومعلومات تكوين النظام (Configuration)، ووثائق التطبيق، وشاشات المساعدة ومواد التدريب تتبع نفس إجراءات إدارة التغيير، وهل اعتبرت أنها جزء لا يتجزأ من التغيير. • معرفة ما إذا كانت فترة حفظ وثائق التغيير مناسبة، وكذلك وثائق النظام والمستخدم ما قبل التغيير وبعده. • معرفة ما هي الآليات الموجودة لتحديث إجراءات العمل للتغييرات في أجهزة أو برامج الكمبيوتر لضمان استخدام وظائف جديدة أو محسنة.
نتائج التدقيق: يقوم المدقق باستيفائها.	

الملحق الخامس

المصفوفة المقترحة للتدقيق على الاستعانة بمصادر خارجية

سياسة الاستعانة بمصادر خارجية	
هدف التدقيق: تقييم ما إذا كان لدى الجهة سياسة مناسبة حول الاستعانة بمصادر خارجية	
موضوع التدقيق الأول: العناصر الأساسية لسياسة الاستعانة بمصادر خارجية هل يوجد لدى الجهة سياسة مناسبة حول الاستعانة بمصادر خارجية؟	
المعلومات المطلوبة	**وسائل التحليل**
• وثيقة السياسة. • عملية اعتماد الاستعانة بمصادر خارجية لأداء وظيفة أو خدمة. • قائمة بالوظائف/الخدمات التي تم فيها الاستعانة بمصادر خارجية. • قائمة بالوظائف/الخدمات التي تم فيها الاستعانة الجزئية بمصادر خارجية. • طريقة تقديم الخدمة من قبل مقدمها. • تحليل فائدة التكلفة في الاستعانة بمصادر خارجية لأداء الوظائف /الخدمات. • قائمة بمقدمي الخدمات الخارجية ومواقعهم. • الوثائق المرتبطة باعتمادات الوظائف / الخدمات التي تم فيها الاستعانة بمصادر خارجية.	• مراجعة السياسة لضمان اعتمادها. • مراجعة السياسة للتحقق (على سبيل المثال) من أنها تحتوي على معلومات حول أصول الجهة التي يمكن الاستعانة من خلالها بمصادر خارجية أم لا، وتحدد قائمة بالوظائف/ الخدمات التي يمكن ايعازها إلى مصادر خارجية. • مراجعة وثائق اعتمادات الإدارة العليا للحيازة أو الاستعانة بمصادر خارجية. • مراجعة الوثائق لتقييم أن الجهة حددت المخاطر المرتبطة بالطرق المختلفة للاستعانة بمصادر خارجية ومواقع مقدمي الخدمات الخارجية. • مراجعة الوثائق للتحقق مما إذا كانت الجهة على إحاطة بالمخاطر المرتبطة باحتمالية الاستحواذ على مقدم الخدمات. • مراجعة الوثائق للتحقق مما إذا كانت الجهة قد ضمنت استمرارية العمل وحقوق البيانات والأمن والملكية والتكلفة

• وضع استراتيجية لضمان الاستمرارية في تقديم الخدمات في حالة استحواذ جهة أخرى على مقدم الخدمات. • المعلومات الخاصة بأي استحواذ على مقدم الخدمات. • مراقبة الوثائق/التقارير.	في اتفاقية الخدمات التي تشمل حالة الاستحواذ على مقدم الخدمات. • مراجعة الوثائق لتقييم ما إذا كانت السياسة تشمل تحديد مؤشرات المراقبة للوظائف التي تم الاستعانة بمصادر خارجية لأدائها ويطلب منهم تضمينها في اتفاقية الاستعانة بمصادر خارجية.
نتائج التدقيق: يقوم المدقق باستيفائها.	

استدراج العروض	
هدف التدقيق: التحقق من وجود سياسة لدى الجهة حول كيفية إدارة عملية استدراج العروض	
موضوع التدقيق الثاني: سياسة وإجراءات استدراج العروض • هل لدى الجهة سياسة للاستحواذ؟ • هل لدى الجهة إجراءات محددة لتحديد واختيار مقدم الخدمة؟ • هل لدى الجهة إجراءات تضمن احتواء المتطلبات التعاقدية لمستوى الخدمة على متطلبات المستخدم؟ • هل يتم اتخاذ القرارات ذات الصلة بمستويات ملائمة؟	
المعايير: شروط سياسة الجهة حول الاستعانة بالمصادر الخارجية والسياسة حول شراء خدمات تكنولوجيا المعلومات المتعلقة باستدراج العروض والحيازة.	
المعلومات المطلوبة	**وسائل التحليل**
• سياسة للحيازة أو ما يعادلها. • قائمة بالقوانين التي تنظم عملية الحيازة والاستعانة بالمصادر الخارجية. • عملية الاختيار لتحديد واختيار مقدم الخدمات.	• مراجعة الوثائق للتحقق من أن لدى الجهة سياسة لاستدراج العروض أو الحيازة. • مراجعة السياسة للتأكد أنها تشمل شروط لطلب البيانات من المقاولين بالباطن في حالة أن المقاول الرئيسي قد أدرج مقاولين بالباطن كجزء من العرض المقدم.

• قائمة بالمهام / الخدمات التي تم من خلالها الاستعانة بمصادر خارجية. • متطلبات المستخدم من الخدمات المتعاقد عليها أو بالاستعانة بمصادر خارجية. • اتفاقية مستوى الخدمة / العقد. • الوثائق المرتبطة بالاعتمادات الخاصة باختيار مقدم الخدمات.	• مراجعة الوثائق لتقييم هل أن السياسات المتعلقة باستدراج العروض والحيازة تلتزم بالقوانين الخاصة بالاستعانة بمصادر خارجية وقوانين الاستحواذ (التحقق أن المراجع المقدمة مربوطة بالقوانين واللوائح المعمول بها). • مراجعة عملية الاختيار لكل من العقود أو خدمات الاستعانة بمصادر خارجية لتحديد مدى التزامها بهذه السياسة (التحقق من أن عملية الاختيار تمت بشفافية، وبمعايير موضوعية، ويتألف فريق الاختيار من الموظفين الذين هم على معرفة بالمتطلبات، ويمثلها موظفين مختصين بالعقود والموظفين القانونيين، والتشاور مع المستخدمين للتوضيح). • التأكد من أن المتطلبات التعاقدية نالت موافقة المستخدمين وأصحاب المصلحة ذوي الصلة. • الاجتماع مع مكتب العقود لضمان أن مستوى إداري مناسب قد اعتمد استدراج العروض والعقد.
نتائج التدقيق: يقوم المدقق باستيفائها.	

مراقبة المورد أو المقاول
هدف التدقيق: تقييم ما إذا كانت الجهة تقوم بإدارة العمل مع المقاول أو المورد وتتخذ الإجراءات المناسبة عندما ينحرف الأداء أو الجودة عن الحد الأدنى المتفق عليه.
موضوع التدقيق الثالث: إدارة عمل المورد • هل هناك عقد مع مقدم الخدمة؟ • هل تم تحديد مستويات الخدمة والاتفاق عليها من خلال اتفاقية مستوى الخدمة؟ • هل هناك ترتيبات لمراقبة الخدمات مع مقدم الخدمة؟ • هل يتم ضمان مستويات الخدمة من خلال هذه الترتيبات؟ • هل يتم اتخاذ الإجراء المناسب عند عدم الالتزام بشروط اتفاقية مستوى الخدمة؟

المعايير:

الشروط/ المؤشرات المحددة في اتفاقية مستوى الخدمة، وإجراءات المتابعة من قبل الجهة.

المعلومات المطلوبة	أساليب التحليل
• العقد/اتفاقية مستوى الخدمة. • الجداول الزمنية المعتمدة، الحدود الدنيا المقبولة، والتكلفة وغيرها من المؤشرات التقنية التي تقوم بتعريف المنتج أو الخدمة التي يتم تحصيلها أو الاستعانة بمصادر خارجية للحصول عليها. • مراقبة الوثائق/التقارير/محاضر الاجتماعات حول عمليات المراجعة التي أجريت، وبنود العمل، والإرشادات الموجهة للمورد (أوامر المهمة، وبيان العمل، إلخ). • تقييم أثر المخالفات. • بنود العمل أو الإرشادات الخاصة بالمورد. • تقارير الإجراءات المتخذة حول المخالفات المتعلقة بمستويات الخدمة.	• مراجعة الوثائق لتقييم ما إذا كان عقد اتفاقية مستوى الخدمة معترف به قانونيا. • مراجعة تقارير المراقبة التي قدمها المقاول لضمان أنها تشمل العناصر الواردة في العقد أو اتفاقية مستوى الخدمة (التكلفة، الجدول، الأداء، المخاطر، الحالة، الأمور، وحالة بنود العمل أو المهام السابقة). • مراجعة تقارير الرقابة لتحديد أوجه القصور في الخدمة /المخالفات وتقييم الأثر الناجم عنها. • مراجعة الإشعارات وتقارير الإجراءات المتخذة بحيث تكون متناسبة مع التأثير على العمل والشروط التعاقدية.

نتائج التدقيق:

يقوم المدقق باستيفائها.

حقوق ملكية البيانات

هدف التدقيق: تقييم ما إذا تم تحديد متطلبات حماية البيانات في الجهة، وأنها جزء من المتطلبات التعاقدية.

موضوع التدقيق الرابع: حماية البيانات وإدارة البيانات

- **هل حماية البيانات وحقوق الوصول للبيانات متضمنة في عقد الخدمة؟**
- **هل تم تعريف البيانات بشكل مناسب لتغطية بيانات المعاملات، بالإضافة إلى البرامج التي تدعم البيانات، أيا كانت؟**

- **هل هناك آلية لضمان أن متطلبات أمن وحماية البيانات حسب اتفاقية مستوى الخدمة قد تم اعتمادها وتنفيذها من قبل مقدم الخدمة؟**

المعايير:

تفرض متطلبات حماية البيانات والوصول إليها في الجهة على المقاول بما هو مناسب.

المعلومات المطلوبة	**وسائل التحليل**
• متطلبات الجهة من حيث حماية بياناتها وحقوق الدخول عليها. • تعريف البيانات (للحماية وحقوق الدخول). • العقد المبرم مع مقدم الخدمة. • قائمة بسجلات الدخول على البيانات من مقدم الخدمة. • تقارير عمليات التدقيق التي أجراها طرف ثالث أو عمليات التدقيق الداخلية مع التوصيات ومتابعتها. • تقارير المراقبة. • المراسلات مع مقدم الخدمة حول الموضوع المعني. • تقارير التعامل مع الحوادث. • اتفاقية عدم الإفصاح مع الجهة اللي تم الاستعانة بها كمصدر خارجي. • قائمة بالمعلومات التي أفصحت عنها الشركة التي تم الاستعانة بها كمصدر خارجي لطرف ثالث أو لأطراف غير معنية.	• مراجعة الوثائق للتأكد من مدى كفاية حماية البيانات وحقوق الدخول عليها. • مراجعة وثيقة العقد مع مقدم الخدمة للتحقق من إدراج متطلبات حماية البيانات وحقوق الدخول عليها. • مراجعة تقارير التدقيق الداخلي أو التي قام بها طرف ثالث. • مراجعة تقارير المراقبة وتقارير التعامل مع الحوادث لتقييم أنشطة المتابعة من قبل الجهة. • مراجعة اتفاقية عدم الافصاح للتحقق من أن جميع المعلومات ذات الصلة قد تم إدراجها. • التحقق مما إذا كان الافصاح عن المعلومات من قبل الجهة التي تم الاستعانة بها كمصادر خارجية قد تم اعتمادها.

نتائج التدقيق:

يقوم المدقق باستيفائها.

مقدم الخدمة الأجنبي

هدف التدقيق: تحديد ما إذا كان لدى الجهة استراتيجية بشأن التعاقد على الخدمات مع الموردين من الخارج.

موضوع التدقيق الخامس: إدارة عمل المورد من الخارج

هل الجهة تتفهم المسائل المعنية في الاستعانة بمصادر خارجية أجنبية عند قيامها بهذا الأمر؟

المعايير:

- شروط سياسة الاستعانة بمصادر خارجية المتعلقة بالموردين من الخارج.
- القوانين الخاصة بالدول التي تنظم العمل مع الوكالات الأجنبية.

المعلومات المطلوبة	وسائل التحليل
• قائمة بالقوانين واللوائح المتعلقة بخدمات الاستعانة بمصادر خارجية. • معلومات عن وجود مقدم الخدمة داخل البلاد. • قائمة بالمكاتب الخارجية للجهة. • قائمة بالقوانين واللوائح التي تنظم عمل مقدم الخدمة في بلده. • اتفاقية ثنائية بين الدولة التي فيها الجهة ومقدم الخدمة لتسهيل اتفاقية الاستعانة بمصادر خارجية. • تقارير الأداء السابقة للمورد الخاصة بمواعيد التسليم والجودة. • تحليل المنفعة من وراء التكلفة لخدمة السكان المحليين ومقدم الخدمة الأجنبي. • عقد الاستعانة بمصادر خارجية واتفاقية مستوى الخدمة. • معلومات عن مبلغ الضمان المالي المتصل بالأداء. • قائمة بالمخالفات على اتفاقية مستوى الخدمة وعقد الاستعانة بمصادر خارجية.	• مراجعة الوثائق لتقييم ما إذا كانت الجهة قامت بتحديد المخاطر المتعلقة بالاستعانة بمقدم خدمة أجنبي. • مراجعة الوثائق لتقييم تحليل التكلفة مقابل المنفعة الموجهة للمخاطر المتصلة بالاستعانة بمقدم خدمة أجنبي. • مراجعة الوثائق لتقييم أن الجهة قد قامت بالتحقق من حالة مقدم الخدمة بشكل مناسب. • مراجعة الوثائق لتقييم أن هناك نظام قوي تم وضعه لضمان الأداء في اتفاقية مستوى الخدمة وعقد الاستعانة بمصادر خارجية. • مراجعة الوثائق لتقييم أن أي مخالفات على اتفاقية مستوى الخدمة والعقد يتم متابعتها في الوقت المناسب لضمان الحد الأدنى من زمن التوقف عن العمل وخسارة الجهة.

• تقارير مراقبة ومتابعة التدابير المتخذة على مخالفات موفر الخدمة.	
نتائج التدقيق: يقوم المدقق باستيفائها.	

حفظ المعلومات المتعلقة بالأعمال/ ملكية الأعمال	
هدف التدقيق: تقييم ما إذا كانت الجهة تحتفظ بالمعلومات المتعلقة بالأعمال وملكية الاعمال.	
موضوع التدقيق السادس: السياسة المتعلقة بملكية المعلومات والإجراءات الخاصة بالأعمال • **هل عملية ملكية الأعمال واضحة المعالم وموثقة؟** • **هل هناك ضمانات على عدم فقدان المعلومات بسبب الاستعانة بمصادر خارجية؟** • **هل هناك قدرة على القيام بالخدمات التي تقدمها المصادر الخارجية من داخل الجهة؟** • **هل يمكن ضمان استمرارية الأعمال في حال عدم مقدرة مقدم الخدمة على توفير الخدمات في أي وقت في المستقبل؟**	
المعايير: • تحتفظ الجهة بالمعلومات الخاصة بالأعمال، وتكون قادرة على مواصلة العمليات من داخل الجهة في الحالات الطارئة عند عدم مقدرة المقاولين أو الموردين على توفير الخدمة. • الاحتفاظ بملكية إجراء الأعمال. • الاحتفاظ بالمعلومات الخاصة بالأعمال. • مقارنة الأداء باستمرارية الأعمال فيما يتعلق بفشل مقدم الخدمة بتوفير الخدمة في أي وقت.	
المعلومات المطلوبة	**وسائل التحليل**
• تحديد العمليات والمهارات الضرورية التي يجب الاحتفاظ بها داخل الجهة. • توثيق إجراءات العمل. • وثيقة مفصلة لتصميم نظام الخدمة المقدمة من مصادر خارجية لأدائها.	• مراجعة الوثائق لتقييم أن ملكية العمليات، والبيانات وبرامج التطبيقات تحتفظ بها الجهة من خلال ضمانات كافية في العقد. • مراجعة الوثائق لتقييم أن المعلومات المتوفرة حول الأعمال فيما يتعلق بالبيانات، وبرنامج التطبيقات، وتصميم النظام

• قائمة بالدورات التدريبية للموظفين المختصين بإجراءات العمل، وتصميم النظام، والبيانات، وتطبيق البرمجيات. • تقارير حول الحوادث الطارئة / المراسلات المتعلقة بتوقف الخدمة / النزاع مع مقدم الخدمة، شاملا بذلك ما يتعلق بملكية النظام / البيانات. • محاضر الاجتماعات مع المقاول.	موثقة جيدا، وأن الموظفين يتم تحديث معلوماتهم حولها بشكل دوري من خلال التدريب وما إلى ذلك. • مراجعة الوثائق للتأكد أن الجهة وموظفيها يشاركون في أي تحديثات على النظام تقوم بها الجهة التي تم الاستعانة بها كمصدر خارجي وأنها تقدم للجهة وثيقة مفصلة عن هذا التحديث. • مراجعة الوثائق للتحقق من عدم وجود حوادث أو منازعات مع مقدم الخدمة فيما يتعلق بملكية النظام والبيانات. • مراجعة محاضر الاجتماع مع المقاول لضمان أنه في حالة وجود أي مخاطر رفيعة المستوى فقد تم تتبعها والتعامل معها من خلال إدارة مشتركة لضمان استمرارية العمل.
نتائج التدقيق: يقوم المدقق باستيفائها.	

مراقبة وإدارة التكاليف
هدف التدقيق: تقييم ما إذا كانت الجهة قد ضمنت أقل تكلفة اقتصادية خلال فترة عقد الاستعانة بمصادر خارجية.
موضوع التدقيق السابع: تقييم التكلفة مقابل المنفعة • هل تم تحديد جميع التكاليف (بما فيها التكلفة المستقبلية) المتعلقة بالاستعانة بمصادر خارجية؟ • هل تم إجراء تحليل للتكلفة والمنفعة، وهل تم اختيار الخيار الأفضل؟ • هل هناك مسؤوليات محددة على الجهة عند الاستعانة بمصادر خارجية؟ وهل توجد لديها عناصر أو تأثيرات تكلفة حرجة متضمنة بها؟ • هل تتحمل الجهة تكاليف إضافية أو زيادة في التكاليف؟
المعايير: إجراء تحليل واقعي للتكلفة مقابل المنفعة وأنه الأساس الذي يتم من خلاله إدارة ومراقبة البرنامج.

المعلومات المطلوبة	وسائل التحليل
• التحليل المبدئي للتكلفة مقابل المنفعة. • التكلفة التقديرية لعقد الاستعانة بمصادر خارجية. • عملية اختيار مقدم الخدمة بالمقارنة مع عنصر التكلفة. • وثائق إجراءات الاعتماد المتعلقة بالاختيار. • حالات التكاليف الإضافية / زيادة التكلفة من قبل مقدم الخدمة. • اتفاقية مستوى الخدمة والعقد. • التقارير الرقابية الخاصة بالأعمال أو الأنشطة التي أدت إلى تكبد تكاليف إضافية أو زيادة في التكاليف. • الوثائق الإجرائية الخاصة بطلبات التكاليف الإضافية أو زيادة التكاليف من قبل مقدم الخدمة.	• مراجعة الوثائق لتقييم ما إذا قامت الجهة بتحديد جميع التكاليف ومراجعتها واعتمادها من قبل أصحاب المصلحة المعنيين. • مراجعة الوثائق الخاصة بإجراءات الاختيار والاعتماد. • مراجعة الوثائق للتأكد أن جميع التكاليف قد تم ذكرها في العقد وأنه لا توجد أي تكاليف مخفية بما فيها التكاليف المستقبلية. • مراجعة أن جميع التكاليف تخضع لتحليل التكلفة والمنفعة قبل الالتزام بها من قبل الجهة. • مراجعة ومقارنة جميع التكاليف التقديرية بالمصروفات الفعلية. • مراجعة أداء مقدم الخدمة حول الأنشطة أو المهام التي تغيرت تكلفتها عن طريق تقارير المراقبة وتقييم الحاجة إلى مثل هذا التغيير. • مراجعة إجراءات الجهة المتخذة حول التكاليف الإضافية أو زيادة التكاليف من قبل مقدم الخدمة.
نتائج التدقيق: يقوم المدقق باستيفائها.	

اتفاقية مستوى الخدمة
هدف التدقيق: تقييم ما إذا كانت الجهة قد صممت اتفاقية مستوى الخدمة وضمنت فيها تفاصيل جميع احتياجاتها وأنها تراقب أداء مقدم الخدمة مقابل التزاماته في الاتفاقية.
موضوع التدقيق الثامن: مدى كفاية اتفاقية مستوى الخدمة • هل تم وضع اتفاقية مستوى الخدمة بين الجهة ومقدم الخدمة؟

- هل اتفاقية مستوى الخدمة مفصلة بدرجة كافية بحيث حددت جميع الأدوار والمسؤوليات التي تقع على الجهة وعلى مقدم الخدمة؟
- هل تم تنفيذ اتفاقية مستوى الخدمة بجدية؟
- هل يوجد لدى الجهة آلية لمراقبة تنفيذ اتفاقية مستوى الخدمة؟
- هل هناك آلية لمعالجة الاستثناءات من اتفاقية مستوى الخدمة؟

المعايير:

اتفاقية مستوى الخدمة هي الأساس الذي يتم من خلاله رصد ومراقبة المقاول أو المورد مقابل المتطلبات التقنية وغيرها.

المعلومات المطلوبة	وسائل التحليل
• اتفاقية أو عقد مستوى الخدمة. • المتطلبات التقنية وغيرها من المتطلبات (قائمة الخدمات التي يؤديها المورد). • قائمة بمسئوليات الجهة والمورد. • قاعدة أساس الخدمات التي سيتم قياسها، وفترة القياس، والمدة، والموقع، والجداول الزمنية للتقارير (معدل الأعطال، وقت الاستجابة، وساعات عمل مكتب المساعدة، وما إلى ذلك). • التقارير الدورية لأداء المورد.	• مراجعة الوثائق لتقييم أن جميع متطلبات المستخدم تم ترجمتها إلى متطلبات مستوى الخدمة. • مراجعة الوثائق لتقييم أن أدوار ومسئوليات الجهة ومقدم الخدمة محددة بوضوح. • مراجعة الوثائق لتقييم أن مؤشرات مستويات الأداء محددة بوضوح ومتضمنة في اتفاقية مستوى الخدمة. • مراجعة الوثائق لتقييم أنه تم وضع والاتفاق على آلية لمراقبة مستوى الخدمة بين الجهة ومقدم الخدمة. • مراجعة تقارير حالة المورد للتأكد من تسجيل المؤشرات في اتفاقية مستوى الخدمة من قبل المقاول وأنه قد تم مراجعتها من قبل الموظفين المختصين في الجهة. • تقييم مدى الالتزام بمؤشرات وقواعد الأساس التقنية لاتفاقية مستوى الخدمة. • التحقق من الإجراءات المتخذة من قبل الجهة في حالة المخالفات لاتفاقية مستوى الخدمة.

نتائج التدقيق:

يقوم المدقق باستيفائها.

الأمن

هدف التدقيق: تقييم ما إذا كانت المتطلبات الأمنية توضع في عين الاعتبار عند الاستعانة بمصادر خارجية وأنه يتم الالتزام بها.

موضوع التدقيق التاسع: الاستجابة لمتطلبات الأمن

- **هل حددت الجهة المتطلبات الامنية فيما يتعلق بالاستعانة بمصادر خارجية؟**
- **هل هناك آليه لضمان أن المتطلبات الأمنية للجهة يضعها مقدم الخدمة في عين الاعتبار؟**
- **هل هناك آلية لدى الجهة لمراقبة الالتزام بالمتطلبات الأمنية من قبل مقدم الخدمة؟**

المعايير:

يجوز للجهة أن تزيد من المتطلبات الأمنية المفروضة على المقاول ان دعت الحاجة لذلك.

المعلومات المطلوبة	وسائل التحليل
• السياسة الأمنية في الجهة. • عقد الاستعانة بمصادر خارجية. • اتفاقية مستوى الخدمة. • قائمة جرد البيانات، والتطبيقات والأجهزة مع مقدم الخدمة. • سجلات الدخول على ملفات البيانات والتطبيقات والأجهزة في المواقع التي يتم فيها الاستعانة بمصادر خارجية. • الخطة الأمنية لموقع الدعم وموقع استعادة الأوضاع بعد الكوارث. • تقارير المراقبة المتعلقة بالأمور الأمنية. • المراسلات بين الجهة ومقدم الخدمة بخصوص الأمور الأمنية.	• مراجعة الوثائق لتقييم ما إذا قامت الجهة بتحديد المتطلبات الأمنية وأدرجتها في عقد الاستعانة بمصادر خارجية أو اتفاقية مستوى الخدمة. • التحقق من أن الجهة تحتفظ بقائمة عن ملفات البيانات وبرامج التطبيقات. • التحقق من أن الجهة تقوم بالمراقبة وتدرك حالة ملفات البيانات وبرامج التطبيقات والأجهزة وأنه يتم الحفاظ عليها أثناء النسخ الاحتياطي وعملية استرداد البيانات التي تقوم بها المصادر الخارجية المستعان بها. • التحقق إن كان لدى الجهة ضمانات على التخويل بأي تغيير في البيانات، وبرامج التطبيقات والأجهزة عند الاستعانة بمصادر خارجية. • التحقق مما إذا كان للجهة ضمانات على الوصول إلى البيانات، وبرامج التطبيقات والأجهزة في موقع الجهة التي تم الاستعانة بمصادر خارجية لخدمتها من خلال دراسة سجلات الدخول (المادية والمنطقية).

	• التحقق إن كان لدى الجهة ضمانات على الآليات الأمنية التي يوفرها مقدم الخدمة. • التحقق من أن الجهة تتلقى تقارير منتظمة حول المعلومات في تقارير المراقبة وتتصرف حيالها.
نتائج التدقيق: يقوم المدقق باستيفائها.	

الدعم الاحتياطي واستعادة الأوضاع بعد الكوارث للخدمات التي تتم بالاستعانة بمصادر خارجية	
هدف التدقيق: تقييم ما إذا كانت الخدمات التي تم الاستعانة بمصادر خارجية لأدائها تمتثل لخطط استمرارية العمل وخطط استعادة الأوضاع بعد الكوارث وفق العقد أو اتفاقية مستوى الخدمة.	
موضوع التدقيق العاشر: إجراءات الدعم الاحتياطي واستعادة الأوضاع **هل استوفى المورد شروط العقد أو شروط اتفاقية مستوى الخدمة الخاصة بخطة استمرارية العمل واستعادة الأوضاع بعد الكوارث؟**	
المعايير: العقد أو اتفاقية مستوى الخدمة الخاص بخطة استمرارية العمل وخطة استعادة الأوضاع بعد الكوارث لدى المورد.	
المعلومات المطلوبة	**وسائل التحليل**
• العقد أو اتفاقية مستوى الخدمة. • التدقيق الداخلي أو شهادة إقرار من طرف ثالث بجهوزية خطة المورد لاستمرارية العمل وخطة استعادة الأوضاع بعد الكوارث.	• مراجعة الوثائق أو اتفاقية مستوى الخدمة للتأكد أن المورد يجب عليه ضمان خطة استمرارية العمل وخطة استرداد البيانات بعد الكوارث حول البيانات والتطبيقات والخدمات التي تم الاستعانة بها من الخارج. • مراجعة عقد أو اتفاقية مستوى الخدمة (SLA) للتأكد أن المورد يقدم تقارير تدقيق مستقلة أو داخلية تؤكد على وجود أنشطة لخطة استمرارية العمل وخطة الانتعاش بعد الكوارث وأن المورد يقوم باختبار الإجراءات بشكل دوري.

• التقارير الدورية لاختبار وتحديث خطة استمرارية العمل وخطة استعادة الأوضاع بعد الكوارث.	• مراجعات التقارير التي يقدمها المورد للتأكد من أنه قد تم إجراء الاختبارات وفقا لشروط العقد و/أو اتفاقية مستوى الخدمة. • مراجعة التقارير الدورية للتأكد من تحديث الإجراءات إن دعت الحاجة.
نتائج التدقيق: يقوم المدقق باستيفائها.	

الملحق السادس

المصفوفة المقترحة للتدقيق على خطة استمرارية العمل وخطة استعادة الأوضاع بعد الكوارث

<table>
<tr><th colspan="2">سياسة استمرارية الأعمال</th></tr>
<tr><td colspan="2">هدف التدقيق: التأكد من وجود سياسة فعالة لاستمرارية الأعمال في الجهة.</td></tr>
<tr><td colspan="2">موضوع التدقيق الأول: السياسة
هل توجد خطة طوارئ وسياسة لاستمرارية الأعمال لدى الجهة؟</td></tr>
<tr><td colspan="2">المعايير:
أن يكون لدى الجهة خطة طوارئ معلنة ومعتمدة مع سياسة جاهزة تغطي بشكل شامل جميع مجالات عمليات الطوارئ وتحدد بوضوح متطلبات التدريب وجداول الاختبار.</td></tr>
<tr><td>المعلومات المطلوبة
• وثيقة سياسة استمرارية الأعمال.
• وثيقة سياسة تكنولوجيا المعلومات.
• خطوات الاعتماد الخاصة بتبني أهداف سياسة العمل.
• المراسلات ومحاضر الاجتماع المتعلقة باستمرارية الأعمال.</td><td>وسائل التحليل
• مراجعة الوثائق لتقييم ما إذا كانت السياسة متوافقة مع سياسات تكنولوجيا المعلومات في الجهة.
• مراجعة الوثائق لتقييم ما إذا كانت السياسة تضع في عين الاعتبار متطلبات استمرارية الأعمال من خلال تحديد أهداف الطوارئ وإطار العمل والمسئوليات عند التخطيط للطوارئ في الجهة.
• مراجعة الوثائق أو مقابلة الموظفين لتحديد ما إذا كان يتم تحديث السياسة كلما تغيرت الظروف.
• مراجعة السياسة لمعرفة من قام باعتمادها ومتى تم نشرها آخر مرة أو يتم مقابلة عدد من الموظفين من أصحاب المصلحة لتقييم ما إذا كانت السياسة يتم تداولها بشكل كاف داخل الجهة.</td></tr>
<tr><td colspan="2">نتائج التدقيق:
يقوم المدقق باستيفائها.</td></tr>
</table>

تنظيم مهام استمرارية الأعمال

هدف التدقيق: التأكد من وجود فريق مناسب لاستمرارية الأعمال في الجهة.

موضوع التدقيق الأول: مهام استمرارية الأعمال

هل يوجد فريق لاستمرارية الأعمال أو ما شابه؟

المعايير:

- تغطية جميع المجالات المهمة في الجهة من قبل الفريق.
- متطلبات الأدوار والمسئوليات الخاصة بأعضاء الفريق.

المعلومات المطلوبة	وسائل التحليل
• الهيكل التنظيمي للجهة. • الهيكل التنظيمي لفريق استمرارية الأعمال. • وصف أدوار ومسئوليات أعضاء فريق استمرارية الأعمال. • المراسلات ومحاضر الاجتماع المتعلقة باستمرارية الأعمال. • خطة استمرارية الأعمال.	• مراجعة الوثائق ومقابلة الموظفين المختصين لتقييم ما إذا كانت جميع الجوانب الهامة في الجهة قد تم تقديمها لفريق استمرارية العمل. • مراجعة الوثائق للتأكد من أنه تم تعيين مسئوليات استمرارية العمل على مستوى الادارة العليا، على سبيل المثال، هل حددت الإدارة مستوى وسرعة استعادة الأوضاع بعد الكوارث، وهل هذا ينعكس على السياسة؟ • مراجعة الوثائق للتأكد أن جميع الإدارات الهامة قد شكلت فرق عمل لاستعادة الأوضاع بعد الكوارث، وأنها قد حددت الأدوار والمسئوليات بوضوح. • مقابلة عينة من أعضاء فريق استمرارية الأعمال للتأكد من إدراكهم للدور الذي يقومون به في ضمان استمرارية الأعمال في كل وحدة إدارية هامة.

نتائج التدقيق:

يقوم المدقق باستيفائها.

تقييم مدى التأثير على الأعمال

هدف التدقيق: التأكد من إنجاز تقييم مدى التأثير على الأعمال وتقييم المخاطر، ووجود نظام لإدارة المخاطر.

موضوع التدقيق الثالث: تقييم المخاطر

هل تم القيام بتقييم المخاطر وتحليل التأثير على الأعمال، وهل تم تحديد البيانات الهامة، وبرامج التطبيقات والعمليات والموارد وتحديد أولويتها؟

المعايير:

إطار عمل إدارة المخاطر في المؤسسة أو ما يعادله.

سياسة استمرارية الأعمال أو ما يعادلها.

استكمال تقييم مدى التأثير على الأعمال وتحديد البيانات الهامة وبرامج التطبيقات والعمليات والموارد.

المعلومات المطلوبة	وسائل التحليل
• تقارير تقييم المخاطر. • تقارير تقييم التأثير على الأعمال. • قائمة بالبيانات الهامة، وبرامج التطبيقات، والعمليات والموارد لكل مهمة. • قائمة بالمخاطر المتبقية. • قائمة بأصحاب المصلحة المعنيين. • مراجعة التقارير حول تقييم المخاطر ومدى التأثير على الأعمال. • سياسة وإطار عمل تقييم المخاطر في المؤسسة.	• مراجعة الوثائق للتأكد من أنه تم القيام بتقييم المخاطر وتم تحديد التهديدات المحتملة وتأثيراتها. • مراجعة الوثائق للتأكد من أن جميع الجوانب العملية تم أخذها بعين الاعتبار في تقييم المخاطر وتقييم التأثير على الأعمال. • مراجعة الوثائق للتأكد أن تحليل التأثير على الأعمال قام بتقييم أثر أي اضطراب يتعلق بالوقت وغيرها من الموارد والنظم ذات الصلة. • مراجعة الوثائق للتأكد أن القرار الذي اتخذ بشأن المخاطر المتبقية كان على المستوى المناسب. • مراجعة الوثائق للتأكد أن الجهة قد حددت زمن استعادة الأوضاع ونقطة استعادة الأوضاع المناسبة لجميع التطبيقات الهامة. • مراجعة الوثائق للتأكد أن أهداف زمن استعادة الأوضاع وأهداف نقطة استعادة الأوضاع عملية ومعقولة لجميع التطبيقات والمهام. • مراجعة الوثائق للتأكد من مشاركة الإدارة العليا في الموضوع واعتمادها للنتائج.

• محاضر الاجتماعات حول تقييم المخاطر وتقييم تأثير الأعمال.	• مراجعة الوثائق للتأكد أن أصحاب المصلحة المعنيين قد ساهموا في تحديد المخاطر وتقييم التأثير على الأعمال.

نتائج التدقيق:

يقوم المدقق باستيفائها.

موضوع التدقيق الرابع: إدارة المخاطر

هل هناك إجراءات محددة لإدارة المخاطر (بما فيها التعديلات والمتابعة، وما إلى ذلك) وهل تم تحديد أولويات الإجراءات الطارئة؟

المعايير:

- تغطية إجراءات إدارة المخاطر مقابل تقييم المخاطر وتقييم التأثير على الأعمال.
- المعالجة الفورية للمخاطر والطوارئ وفقا للمقاييس المعتمدة في الجهة.

المعلومات المطلوبة	وسائل التحليل
• وثيقة إجراءات إدارة المخاطر. • تقارير تقييم المخاطر وتقييم التأثير على الأعمال. • قائمة بجميع الموظفين ذوي الصلة، وأعضاء فريق خطة استمرارية الأعمال مع تحديد الأدوار والمسئوليات. • قائمة بالبنود ذات الأولوية للإجراءات الطارئة. • قائمة بالمخاطر المتبقية. • قائمة بالإجراءات الطارئة التي تم اتخاذها. • تقارير الإجراءات والاستجابات للحوادث الطارئة.	• مراجعة الوثائق للتأكد أن إجراءات إدارة المخاطر تعالج جميع البنود ذات الأولوية القصوى. • إجراء المقابلات ومراجعة الوثائق للتأكد أن جميع الموظفين المعنيين، بما فيهم الإدارة العليا، على إدراك تام بأدوارهم ومسئولياتهم وأنهم يقومون بها. • مراجعة الوثائق للتأكد أن المخاطر المتبقية ليس لها تأثير مادي على الجهة. • مراجعة الوثائق والملاحظة للتأكد أنه تم التعامل مع الحالات الطارئة بشكل مناسب. • مراجعة الوثائق لتقييم تأثير الحالات الطارئة. • مراجعة محاضر الاجتماع أو قائمة المخاطر للتأكد أن المخاطر قد تم تخصيصها وأن أنشطة المعالجة تم تحديدها والتأكد أن المخاطر بتم متابعتها بشكل دوري وأنه يتم تحديث الحالة.

نتائج التدقيق: يقوم المدقق باستيفائها.

خطة استعادة الأوضاع بعد الكوارث	
هدف التدقيق: التأكد أن خطة استمرارية الأعمال تشتمل على خطط الدعم الاحتياطي واسترداد الأوضاع بعد الكوارث من حيث الأجهزة والبيانات وبرامج التطبيقات ومركز البيانات وأن ذلك تم بإتقان؟	
موضوع التدقيق الخامس: إجراءات النسخ الاحتياطي هل تم وضع وتطبيق إجراءات الدعم الاحتياطي للبيانات والبرامج بفعالية؟	
المعلومات المطلوبة	**وسائل التحليل**
• خطط الدعم الاحتياطي والإجراءات للأجهزة والبيانات وبرامج التطبيقات. • سجلات النسخ الاحتياطي / سجلات الإصدار. • الأدوار والمسئوليات للدعم الاحتياطي. • قائمة بمواقع التخزين ودورية التخزين. • جدول الحفظ. • الترتيبات الأمنية لموقع الدعم الاحتياطي. • سجلات الكوارث. • أدوار ومسئوليات أنشطة استعادة الأوضاع.	• مراجعة الوثائق للتأكد أن خطة النسخ الاحتياطي تشمل جميع الأجهزة والبيانات وبرامج التطبيقات الهامة. • مراجعة الوثائق للتأكد من وضع إجراءات تفصيلية للدعم الاحتياطي. • مراجعة الوثائق للتأكد من أن خطة الدعم الاحتياطي قد تم وضعها بشكل مناسب. • تحليل السجلات للتأكد من أن النسخ الاحتياطية تم أخذها من خلال جدول زمني محدد وأنه يتم الاحتفاظ بها لفترة معينة. • التحقق من أن النسخة الاحتياطية الصحيحة متوفرة. • مراجعة الوثائق لتقييم مدى ملاءمة موقع الدعم الاحتياطي وطريقة نقل الملفات الاحتياطية وغيرها إلى موقع الدعم الاحتياطي. • التحقق من ملاءمة موقع الدعم الاحتياطي من الناحية الأمنية سواء المنطقية أو المادية. • التحقق من صلاحية النسخ الاحتياطية وإمكانية استخدامها لاستعادة الأوضاع بعد الكوارث. • مراجعة الوثائق للتأكد أن إجراءات النسخ الاحتياطي يتم تطبيقها بحد أدنى من الوقت والموارد. • مراجعة الوثائق للتأكد من وضع إجراءات تفصيلية لاستعادة الأوضاع، وأنها تشمل إعادة تعيين مؤشرات النظام، وتثبيت التصحيحات، وضبط

• سجلات التدريب الخاصة بالموظفين المسئولين. • تقييم تأثير الكوارث. • تقرير حول أنشطة استعادة الأوضاع بعد الكوارث.	إعدادات النظام، وتوفير وثائق النظام وإجراءات التشغيل، وإعادة تثبيت برامج النظام والتطبيقات، وتوفير أحدث نسخ احتياطية، واختبار النظام. • مراجعة الوثائق للتأكد أن إجراءات استعادة الأوضاع يتم تطبيقها بحد أدنى من الوقت والموارد. • مراجعة الوثائق ومقابلة الموظفين للتأكد من أن الموظفين المعنيين قد تم تدريبهم على الدعم الاحتياطي واستعادة الأوضاع.
نتائج التدقيق: يقوم المدقق باستيفائها.	

الرقابة البيئية	
هدف التدقيق: تقييم ما إذا كان لدى الجهة رقابة بيئية مناسبة في مواقع الدعم الاحتياطي.	
موضوع التدقيق السادس: الآليات الرقابية **هل هناك آلية للرقابة البيئية وضعت في موقع الدعم الاحتياطي.**	
المعايير: مؤشرات الرقابة البيئية في آلية الرقابة البيئية.	
المعلومات المطلوبة	**وسائل التحليل**
• برنامج الرقابة البيئية. • قائمة بالمخاطر البيئية المحتملة خلال عملية تقييم المخاطر المتعلقة بالمواقع. • قائمة بخطوات الحد من المخاطر البيئية التي تم اتخاذها.	مراجعة الوثائق والملاحظة والتدقيق على الإجراءات لتقييم التالي: توافر إمدادات غير منقطعة من الطاقة (UPS). وضع نظام ملائم للحماية من الحرائق. التحكم في الرطوبة والحرارة والتيار الكهربائي في نطاق الحدود. وضع نظام ملائم للحماية من المياه/الفيضان. وضع عناصر الرقابة البيئية حسب القواعد. الالتزام بتدابير الرقابة البيئة من قبل جميع الموظفين المعنيين.
نتائج التدقيق: يقوم المدقق باستيفائها.	

التوثيـــــــق	
هدف التدقيق: تكون خطة استمرارية الأعمال موثقة بشكل مناسب للقيام بأنشطة الأعمال المؤقتة الفعالة وإجراءات استعادة الأوضاع بعد فترة انقطاع الأعمال.	
موضوع التدقيق السابع: خطط موثقة لإجراءات الدعم الاحتياطي واستعادة الأوضاع والأدوار والمسؤوليات. هل لدى الجهة خطة موثقة لما بعد الكوارث ومتاحة بسهولة للدعم الاحتياطي واستعادة الأوضاع؟	
المعايير: توافر ومدى حداثة خطة استمرارية الأعمال واستعادة الأوضاع بعد الكوارث.	
المعلومات المطلوبة	**وسائل التحليل**
• خطة استمرارية الأعمال. • خطة استعادة الأوضاع بعد الكوارث. • الإصدار الأخير من خطة استمرارية الأعمال واستعادة الأوضاع بعد الكوارث. • قائمة بالمعنيين الذين يتم تزويدهم بخطط استمرارية الأعمال واستعادة الأوضاع بعد الكوارث.	• مراجعة الوثائق للتأكد من حداثة خطة استمرارية الأعمال. • مراجعة الوثائق للتأكد من حداثة خطة استعادة الأوضاع بعد الكوارث. • التحقق من توفر وثائق الإصدار الأخير لخطة استمرارية الأعمال وخطة استعادة الأوضاع بعد الكوارث لدى جميع المعنيين. • التحقق من توفر وثائق الإصدار الأخير لخطة استمرارية الأعمال وخطة استعادة الأوضاع بعد الكوارث في موقع خارجي للاستفادة منها في حالة الكوارث. • التحقق من وضوح تحديد أدوار ومسئوليات فريق الدعم الاحتياطي واستعادة الأوضاع بعد الكوارث والموظفين المعنيين. • مقابلة عينة من الموظفين للتأكد من أنهم على علم وإدراك بإجراءات استعادة الأوضاع بعد الكوارث.
نتائج التدقيق: يقوم المدقق باستيفائها.	

اختبار خطة استمرارية الأعمال / خطة استعادة الأوضاع بعد الكوارث	
هدف التدقيق: التأكد من أنه تم اختبار إجراءات استمرارية الأعمال واستعادة الأوضاع بعد الكوارث.	
موضوع التدقيق الثامن: الاختبارات هل قامت الجهة بتجربة إجراءات استمرارية الأعمال واستعادة الأوضاع بعد الكوارث، وما هي التغييرات التي تم إجراؤها (إن وجدت) نتيجة لهذه التجربة؟	
المعايير: يجب على الجهة اختبار الإجراءات الموثقة الخاصة باستمرارية الأعمال واستعادة الأوضاع بعد الكوارث من خلال التدريبات أو الكوارث الوهمية لضمان صلاحيتها في الحالات الفعلية، ويتعين على الموظفين المسئولين عن ضمان استمرارية الأعمال أن يدركوا الأدوار المطلوبة منهم.	
المعلومات المطلوبة	**وسائل التحليل**
• إجراءات عمليات استمرارية الأعمال واستعادة الأوضاع بعد الكوارث وإجراءات الاختبار. • قائمة بالبنود الخاصة بخطط استمرارية الأعمال واستعادة الأوضاع بعد الكوارث التي لا بد أن يتم اختبارها. • مدى تكرار اختبار خطط استمرارية الأعمال واستعادة الأوضاع بعد الكوارث. • قائمة بالاختبارات التي تم إجراؤها. • قائمة بمجالات الاختبار مثل زمن الاسترداد المرجو ونقطة الاسترداد المرجوة وغيرها. • قائمة بوسائل الاختبار المستخدمة. • نتائج الاختبار والإجراءات المتخذة أو توصيات الاختبارات. • إجراءات متابعة نتائج الاختبار.	• مراجعة الوثائق للتأكد من تغطية جميع البنود ذات الصلة للاختبار. • مراجعة الوثائق للتأكد من أن الاختبارات أجريت في الأوقات المناسبة. • مراجعة الوثائق للتأكد من أن الاختبارات أجريت وفقا لمعايير محددة. • مراجعة الوثائق للتأكد من أن الاختبارات أجريت باستخدام الوسائل المناسبة. • مراجعة الوثائق للتأكد من رفع التوصيات للسلطات الملائمة للمتابعة. • مراجعة الوثائق للتأكد من أن متابعة التوصيات الخاصة بالاختبار تتم بشكل مناسب وأن خطة استمرارية الأعمال أو خطة استعادة الأوضاع بعد الكوارث يتم تحديثهم على نحو كاف.
نتائج التدقيق: يقوم المدقق باستيفائها.	

الأمـــــــن	
هدف التدقيق: التأكد أن خطة استمرارية الأعمال وخطة استعادة الأوضاع بعد الكوارث تضمن أمن البيانات وبرامج التطبيقات والأجهزة ومركز البيانات.	
موضوع التدقيق التاسع: كفاءة المؤشرات الأمنية **التأكد من توفير أمن البيانات وبرامج التطبيقات والأجهزة ومركز البيانات بشكل ملائم خلال إجراءات استعادة الأوضاع بعد الكوارث.**	
المعايير: قاعدة الأساس الأمنية للجهة مثل الإجراءات المطروحة في سياسة أمن تكنولوجيا المعلومات وخطط استعادة الأوضاع بعد الكوارث.	
المعلومات المطلوبة	**وسائل التحليل**
• جرد البيانات وبرامج التطبيقات والأجهزة. • جرد الملفات الاحتياطية الخاصة بالبيانات والتطبيقات. • سجلات مراقبة الوصول إلى ملفات البيانات، وبرامج التطبيقات والأجهزة. • الخطة الأمنية لموقع الدعم الاحتياطي وموقع استعادة الأوضاع بعد الكوارث.	• التحقق من أعداد وحالة ملفات البيانات والأجهزة وبرامج التطبيقات كما تم تخزينها خلال عملية استرداد النسخ الاحتياطية. • التحقق مما إذا تعرضت البيانات والأجهزة وبرامج التطبيقات إلى أي تغييرات خلال عملية الدعم الاحتياطي واستعادة الأوضاع بعد الكوارث من خلال دراسة الضوابط حول عدد من السجلات وحجم الملفات المتعلقة بالبيانات وبرامج التطبيقات. • التحقق من عدم وقوع أي مخالفات أمنية من خلال فحص سجلات مراقبة الوصول للبيانات (المادية والمنطقية).
نتائج التدقيق: يقوم المدقق باستيفائها.	

الدعم واستعادة الأوضاع بعد الكوارث للخدمات التي تم الاستعانة بأدائها من الخارج	
هدف التدقيق: التأكد أن الخدمات التي تم الاستعانة بها من الخارج تلتزم بخطط استمرارية الأعمال واستعادة الأوضاع بعد الكوارث.	
موضوع التدقيق العاشر: التأكد أن مقدم الخدمات الخارجية يضمن تبني خطط الجهة في استمرارية الأعمال واستعادة الأوضاع بعد الكوارث.	
المعايير: قاعدة الأساس الأمنية للجهة مثل الإجراءات المطروحة في سياسة أمن تكنولوجيا المعلومات وخطط استعادة الأوضاع بعد الكوارث.	
المعلومات المطلوبة	**وسائل التحليل**
• جرد البيانات وبرامج وأجهزة التطبيقات الخاصة بالجهة مع الوكالة التي تم الاستعانة بها خارجيا. • جرد ملفات بيانات الدعم الاحتياطي وبرامج التطبيقات الاحتياطية الخاصة بالجهة مع الوكالة التي تم الاستعانة بها خارجيا. • سجلات مراقبة الوصول إلى ملفات البيانات، وبرامج التطبيقات والأجهزة الموجودة لدى الوكالة التي تم الاستعانة بها خارجيا. • نتائج اختبار خطة الدعم الاحتياطي وخطة استعادة الأوضاع بعد الكوارث في الوكالة التي تم الاستعانة بها خارجيا. • الخطة الأمنية لموقع الدعم الاحتياطي وموقع استعادة الأوضاع بعد الكوارث الخاصة بالوكالة التي تم الاستعانة بها خارجيا.	• التحقق مما إذا كانت الجهة تتحقق من أعداد وحالة ملفات البيانات والأجهزة وبرامج التطبيقات خلال عملية الدعم واسترداد البيانات في الوكالة التي تم الاستعانة بها خارجيا. • التحقق مما إذا كانت الجهة تتحقق من تعرض البيانات والأجهزة وبرامج التطبيقات إلى تغييرات خلال عملية الدعم أو استعادة الأوضاع بعد الكوارث من خلال دراسة الضوابط حول عدد من السجلات وحجم الملفات المتعلقة بالبيانات وبرامج التطبيقات في الوكالة التي تم الاستعانة بها خارجيا. • التحقق مما إذا كانت الجهة تتحقق من عدم وقوع أي مخالفات أمنية من خلال فحص سجلات مراقبة الوصول للبيانات (المادية والمنطقية). • التحقق مما إذا كانت الجهة تتحقق من صحة اختبار الدعم واستعادة الأوضاع بعد الكوارث في الوكالة التي تم الاستعانة بها خارجيا.

• الاستراتيجية الموضوعة لضمان الاستمرارية في الحصول على الخدمات في حالة استحواذ شركة أخرى على مقدم الخدمات. • معلومات عن أي عملية استحواذ على مقدم الخدمات.	• التحقق من أن الجهة على إدراك بالمخاطر المتعلقة باحتمال استحواذ شركة أخرى على مقدم الخدمات. • التحقق من أن الجهة قد ضمّنت استمرارية الأعمال في اتفاقية الخدمات.
نتائج التدقيق: يقوم المدقق باستيفائها.	

الملحق السابع

المصفوفة المقترحة للتدقيق على أمن المعلومات

<table>
<tr><th colspan="2">تقييم المخاطر</th></tr>
<tr><td colspan="2">هدف التدقيق: التأكد من تحديد جميع المخاطر المرتبطة بأمن المعلومات ومن وضع استراتيجية للحد من أثر المخاطر.</td></tr>
<tr><td colspan="2">موضوع التدقيق الأول: آلية التقييم
هل يوجد لدى الجهة آلية فعالة وموثقة بشكل جيد لتقييم المخاطر المرتبطة بأمن المعلومات؟</td></tr>
<tr><td colspan="2">المعايير:
السياسات الداخلية والإجراءات واللوائح تعكس استعداد الجهة لإدارة المخاطر الحرجة.</td></tr>
<tr><td>المعلومات المطلوبة</td><td>وسائل التحليل</td></tr>
<tr><td>• سياسة أمن نظم المعلومات.
• الإجراءات الرسمية لإدارة المخاطر.
• وثائق اعدادات النظام.</td><td>تحليل سياسة إدارة المخاطر، ووثائق تقييم المخاطر، ومقابلة الإدارة العليا والإدارة التشغيلية بالجهة للقيام بالتالي:
فهم الدور الحقيقي للجهة في إجراءات تقييم المخاطر.
تحديد الأطراف المرتبطة بتقييم المخاطر.
اكتشاف التكاليف التشغيلية لآلية تقييم المخاطر.
التحقق من إجراء تقييم المخاطر يتم على أساس منتظم، أو عند تغير الظروف.
التحقق مما إذا تم توثيق اعدادات النظام الحالي، بما في ذلك ارتباطه مع الأنظمة الأخرى.
التحقق مما إذا كانت الوثائق تشتمل على وصف للمخاطر الرئيسية لنظام الجهة والأعمال والبنية التحتية؟
في حال عدم وجود إجراءات ووثائق رسمية بشأن تقييم المخاطر، يجب على المدقق ألا يقلل من أهمية الضوابط المضمنة في الإجراءات العملية للجهة – وأن يتحقق من أن آليه هذه الضوابط التعويضية المضمنة في العمليات فعالة. ويمكن التحقق من ذلك من خلال دراسة عينة من العمليات خطوة بخطوة وما إلى ذلك.</td></tr>
</table>

موضوع التدقيق الثاني: التغطية هل يشمل تقييم المخاطر كافة المخاطر الداخلية والخارجية الهامة؟ وهل تم تقييم الآثار المحتملة لاختراقات أمن المعلومات؟	
المعايير: يتم تحديد جميع المخاطر الهامة وتقييمها بشكل صحيح (أفضل الممارسات في تقييم المخاطر[51]).	
المعلومات المطلوبة	**وسائل التحليل**
• تقييم المخاطر الموثقة. • تسجيل المخاطر. • تقارير التعامل مع الأحداث الطارئة.	• مراجعة الوثائق للتحقق إذا كان تقييم المخاطر الذي قامت به الجهة يستند إلى معلومات شاملة بالقدر الكافي. والتحقق مما إذا تم الحصول على البيانات والتقارير من نظام إدارة الحوادث الطارئة في الجهة. (يدعم المدقق تحليله بنتائج وسائل التحليل الخاصة بعمليات تكنولوجيا المعلومات التي تركز على نظام إدارة الحوادث الطارئة وخاصة إذا كان التعامل مع الحوادث الطارئة في أمن المعلومات يشكل نظام منفصل عن النظام العام لإدارة الحوادث). • ***اختبار التحقق من الصحة 1:*** سجل التدقيق الإلكتروني: تحديد ما إذا كان سجل التدقيق الإلكتروني يلتقط هوية المستخدم، ونوع الحدث، والبيانات والوقت، والإشارة إلى النجاح أو الفشل، ونشأة الحدث، وهوية أو اسم العنصر المتأثر. • مقابلة الموظفين المعنيين للتحقق مما إذا كان هناك معايير لإعادة تقييم مستوى المخاطر كلما كانت الجهة تخطط لطرح نظم معلومات وتحديثات، وإصدارات جديدة. • التحقق من تصميم تقييم المخاطر من حيث اكتماله، ومدى ارتباطه بالخطر، وتوقيته وقابليته للقياس. • التحقق من أنه تم دراسة نتائج عدم قابلية البنية التحتية للعمل عند حدوث المخاطر. والتحقق من الوثائق لمعرفة إذا ما تم القيام بإجراء تحليل التأثير

[51] ISO 27005 Information security risk management, ISACA RiskIT Framework, COSO Enterprise Risk Management Framework.

	على الأعمال للنتائج المترتبة على عدم توفر المعلومات الهامة، أو تلفها أو فقدانها أو وصولها لآخرين. • مراجعة التقارير الخاصة بالاستجابة للحوادث الطارئة وسجلات المخاطر السابقة لفحص مدى فعالية منهجية تقييم المخاطر في السابق.

موضوع التدقيق الثالث: الحد من أثر المخاطر **هل تم الحد من أثر المخاطر الهامة بصورة كافية وفعالة؟**	
المعايير: وجود ممارسات ملائمة للحد من أثر المخاطر.	
المعلومات المطلوبة	**وسائل التحليل**
• تقارير معالجة المشاكل والحوادث الطارئة. • التقارير الدورية حول الأنشطة.	• مراجعة تقارير معالجة الحوادث الطارئة والتحقق مما إذا كانت هناك إجراءات مناسبة لمنع وكشف ومراقبة المخاطر الأمنية المحددة في وثيقة تقييم المخاطر. • في الجهات التي لا تتبع آلية فاعلة لتقييم المخاطر، على المدقق أن يحدد ما هي الضوابط التعويضية المستخدمة، ويقوم بتحليل ما إذا وقعت أي حوادث خطيرة تتعلق بالأمن وذات صلة بالمخاطر التي كان من الممكن ان يتم السيطرة عليها بشكل أفضل بوجود آلية عمل مناسبة لتقييم المخاطر، ومقارنة الضوابط التعويضية الموجودة. • يجب الأخذ في الاعتبار أن تقارير المشاكل والحوادث قد تكون غير مكتملة في بعض الحالات. ومع ذلك، فالأحداث الهامة قد تنعكس بشكل مباشر أو غير مباشر في مستندات أخرى، مثل تقارير النشاط السنوي أو غيرها من التقارير الدورية.
نتائج التدقيق: يقوم المدقق بتعبئتها.	

سياسة أمن المعلومات

هدف التدقيق: تقييم وجود توجيه ودعم استراتيجي ملائم لأمن المعلومات فيما يتعلق بسياسة الأمن، النطاق الذي تغطيه، والوعي والالتزام على مستوى الجهة.

موضوع التدقيق الرابع: سياسة أمن المعلومات

هل لدى الجهة سياسة لأمن المعلومات؟ وهل تم تنفيذها وتوثيقها بشكل صحيح؟ وهل تشكل خطة أمنية ملائمة ومحكمة؟

المعايير:

أن تغطي سياسة أمن المعلومات في الجهة جميع المخاطر التشغيلية وأن تكون قادرة على حماية جميع معلومات العمل المهمة من الفقدان أو التلف أو سوء الاستغلال.[52]

المعلومات المطلوبة	وسائل التحليل
• استراتيجية تكنولوجيا المعلومات. • التصرفات القانونية التي تحدد متطلبات أمن المعلومات. • السياسة الرسمية والموثقة لأمن المعلومات. • الهيكل التنظيمي والوصف الوظيفي. • الترتيبات التعاقدية مع	• فحص الوثائق للتحقق من أن استراتيجية تكنولوجيا المعلومات سلطت الضوء بنحو كاف على الدور الهام لأمن المعلومات. أيضا يجب الرجوع إلى مصفوفة حوكمة تكنولوجيا المعلومات لاستراتيجية تكنولوجيا المعلومات. وفي حال غياب استراتيجية موثقة لتكنولوجيا المعلومات، يتم مقابلة الإدارة العليا والإدارة الوسطى والموظفين لمعرفة مدى فهمهم للدور الاستراتيجي لأمن المعلومات. • تقييم مدى التزام استراتيجية تكنولوجيا المعلومات في الجهة وسياسة أمن المعلومات بالمتطلبات الخارجية للالتزام. • المقارنة بين أهداف السياسات والإجراءات الأمنية لتحديد فعالية التكامل من متطلبات أمن المعلومات في الخطة الأمنية لتكنولوجيا المعلومات (الميثاق، إطار العمل، والدليل وما الى ذلك) والتحقق مما إذا كانت تتم المراجعة المنتظمة على مستويات الادارة المناسبة. • دراسة العناصر التي تغطيها خطة أمن تكنولوجيا المعلومات، والتحقق مما إذا كانت تأخذ بعين الاعتبار الخطط التكتيكية وتصنيف البيانات، ومعايير التكنولوجيا، وسياسات الأمن والرقابة وإدارة المخاطر.

[52] راجع سلسلة ايزو 2700 انظمة إدارة امن المعلومات والسياسات الداخلية والإجراءات او القوانين ذات العلاقة.

الأطراف الخارجية. • خطة أمن تكنولوجيا المعلومات.	• التحقق من أن الخطة الأمنية تحدد: الادوار والمسؤوليات (مجلس الإدارة، والإدارة التنفيذية، والمدراء، والموظفين وجميع مستخدمين البنية الأساسية لتقنية المعلومات في المؤسسة)، والاحتياجات من الموظفين، والوعي الأمني والتدريب، والممارسات المفروضة، والحاجة إلى الاستثمار في الموارد الأمنية المطلوبة. • مراجعة وتحليل الميثاق للتحقق من أنه يشير إلى المخاطر التنظيمية المتعلقة بأمن المعلومات، وأنه يشمل بوضوح نطاق وأهداف مهمة إدارة الأمن. • فحص التقارير الخاصة بالحوادث الأمنية ووثائق المتابعة للتعرف على الإجراءات التي تتخذها الجهة ضد الأفراد الذين ينتهكون السياسة الأمنية. • التحقق من تقارير الحوادث لتحديد عدد الاختراقات لأمن المعلومات من قبل الموظفين أو أطراف خارجية خلال فترة معينة لتقييم فعالية سياسة الأمن.

موضوع التدقيق الخامس: السرية

هل متطلبات الجهة من السرية أو اتفاقيات عدم الإفصاح تعكس الحاجة إلى حماية المعلومات؟ وهل السياسات تُأمن المعلومات فيما يتعلق بعلاقة الجهة مع الأطراف الخارجية؟

المعايير:

أن تكون سياسة أمن المعلومات في الجهة قادرة على حماية جميع المعلومات السرية المتعلقة بأصحاب المصلحة في الجهة والأطراف الثالثة.

المعلومات المطلوبة	وسائل التحليل
• اللوائح الخارجية والداخلية المتعلقة بالمعلومات السرية. • على سبيل المثال، بنود عدم الافصاح الخاصة بالموظفين. • الترتيبات التعاقدية مع الأطراف الخارجية.	• التحقق من التدابير الإجرائية التي اتخذتها الجهة للوفاء بمتطلبات السرية. • عندما تكون صلاحية الاطلاع على حالات خرق السرية مقتصرة على بعض الجهات المتخصصة فقط، يبنى المدقق رأيه استنادا الى تقارير وتوصيات هذه الجهات الصادرة إلى إدارة الجهة – إذا كانت متوفرة. • مراجعة الترتيبات التعاقدية التي تمت مع أطراف خارجية أو مع المقاولين. وهل تشمل إعطاء وسحب صلاحية الدخول، والمعالجة، والتواصل أو إدارة الأصول المعلوماتية للجهة؟

• سياسة أمن المعلومات. • خطة أمن تكنولوجيا المعلومات.	• التحقق مما إذا كانت الشروط التعاقدية والالتزامات تحدد القيود والالتزامات الأمنية التي تتحكم في كيفية استخدام المقاولين لأصول الجهة والوصول إلى نظم المعلومات والخدمات. • التحقق من وجود أي اختراقات أمنية للمعلومات تمت من قبل المقاولين. والتحقق من ردود فعل الإدارة حيال مثل هذه الانتهاكات.
نتائج التدقيق: يقوم المدقق بتعبئتها	

تنظيم أمن تكنولوجيا المعلومات	
هدف التدقيق: ضمان التشغيل الآمن لمرافق معالجة تكنولوجيا المعلومات.	
موضوع التدقيق السادس: الهيكل التنظيمي **هل يوجد لدى الجهة الخاضعة للتدقيق تنظيم واضح لأمن تكنولوجيا المعلومات؟ هل تم تحديد الأدوار والمسئوليات الأمنية فيما يتعلق بسياسة أمن المعلومات؟**	
المعايير: أدوار ومسئوليات موثقة وواضحة لتكنولوجيا المعلومات خاصة بسياسة أمن المعلومات[53].	
المعلومات المطلوبة	**وسائل التحليل:**
• الهيكل التنظيمي لتكنولوجيا المعلومات. • اللوائح الداخلية المتعلقة بأمن نظم المعلومات. • الوصف الوظيفي. • محاضر اجتماعات الأشخاص المعنيين بالأمن.	• التأكد أن مسئوليات امن تكنولوجيا المعلومات مذكورة بشكل رسمي وواضح. • التحقق من وجود إجراءات لتصنيف المبادرات الأمنية المقترحة حسب الأولوية، بما في ذلك المستويات المطلوبة للسياسات والمعايير والإجراءات. • التحقق من طريقة الإدارة العليا في المحافظة على مستوى مناسب من الاهتمام بأمن المعلومات داخل الجهة.

[53] انظر سلسة ايزو 27000

موضوع التدقيق السابع: التنسيق كيف تقوم الجهة بتنسيق أنشطة أمن المعلومات من مختلف أنحاء الجهة؟	
المعايير: عدم وجود تضارب في المسئوليات، أو عدم انسجام أو احتكار لأنشطة أمن المعلومات[54].	
المعلومات المطلوبة	**وسائل التحليل**
• المتطلبات القانونية المتعلقة بالمعلومات السرية. • الهيكل التنظيمي. • اللوائح الداخلية المرتبطة بأمن نظم المعلومات. • محاضر اجتماع لجنة أمن تكنولوجيا المعلومات. • تقارير حالات الإخفاق.	• التحقق من الوثائق، ومراقبة الممارسات وإجراء مقابلات مع الموظفين للتحقق من وجود تضارب/ تداخل/ فجوات بين الإجراءات الأمنية التي يتبعها العاملين في مختلف الإدارات/ الوحدات. • التحقق من إجراءات سير العمل التشغيلية لتحديد ما إذا يتم نقل بعض المعلومات إلى أطراف خارجية خارج نطاق رقابة ومسئولية الوحدات/ الموظفين. • التحقق من علم الإدارة العليا بمشاكل التنسيق وعما إذا كانت تشرف على عمليات التفتيش وتنسيق الأنشطة. • مراجعة الاجراءات للتحقق من وجود إجراءات متبعة للإدارة بخصوص التصريح لوسائل جديدة بمعالجة المعلومات.
نتائج التدقيق: يقوم المدقق بتعبئتها.	

[54] انظر سلسة ايزو 27000: نظام إدارة امن المعلومات

إدارة الاتصالات والعمليات	
هدف التدقيق: التأكد من أن الاتصالات الداخلية والخارجية آمنة.	
هدف التدقيق الثامن: السياسة والإجراءات **هل السياسات والإجراءات ملائمة بحيث تكون الاتصالات الداخلية والخارجية آمنة وذات كفاءة؟**	
المعايير: أن تشكل السياسات والإجراءات بيئة إدارية مستقرة للاتصالات الداخلية والخارجية[55].	
المعلومات المطلوبة	**وسائل التحليل**
• السياسة الرسمية والموثقة للاتصالات وعمليات تكنولوجيا المعلومات. • توثيق الإجراءات التشغيلية.	• التحقق مما إذا كانت السياسات والإجراءات المتبعة في الجهة تشمل التواصل مع المواطنين ووسائل الإعلام والجهات الخارجية. • التحقق من كيفية توثيق الجهة لإجراءاتها التشغيلية واتاحتها لكافة المستخدمين. إجراء عينة من المقابلات مع مجموعة من المستخدمين على مختلف المستويات لدراسة ما إذا كانت الإجراءات الخاصة بالتعامل مع البيانات معروفة بشكل جيد من قبل الموظفين. • التحقق من عدد المرات التي يتم فيها مراجعة وتحديث إجراءات الاتصالات ومعالجة البيانات.
موضوع التدقيق التاسع: ضوابط الشبكة **كيف تقوم الجهة بإدارة ورقابة المعلومات في الشبكة؟**	
المعايير: أن يتم إدارة وأداء عمليات الشبكة بطريقة آمنة وفعالة[56].	

[55] راجع المعايير: ISO-27002, S15-IT Control (ISACA Standard), COBIT

[56] المرجع السابق نفسه

المعلومات المطلوبة	وسائل التحليل
• سياسة القيود على المعلومات. • سجلات المشرف على الشبكة. • نتائج تحليل السجلات. • تقرير اختبار قبول المستخدم. • اتفاقيات مستوى الخدمة. • المعلومات المتوفرة للعامة أو الموجودة على الانترنت.	• التحقق من الأدوات التي يتم استخدامها لمراقبة وتحليل الشبكة. والتحقق مما إذا كان المستخدمين وأنظمة تكنولوجيا المعلومات من الجهة الخاضعة للتدقيق محمية من البريد غير المرغوب فيه (Spam). • التحقق مما إذا كان يتم تحليل أنظمة كشف الاختراق، وسجلات الدخول من قبل الموظفين المناسبين لضمان أمن المعلومات من هجمات القرصنة والبرامج الضارة. والتحقق مما إذا كانت الهجمات (منها الفاشلة والناجحة) قد تم تحليلها والابلاغ عنها. • التحقق من إحصائيات الرسائل غير المرغوب فيها، وهجمات القرصنة والبرامج الضارة. • الاستفسار حول الطريقة التي توفر بها الجهة النقل الآمن للمعاملات عبر الشبكات العامة. على سبيل المثال، التعاميم والإخطارات الخاصة بإجراءات التشغيل للمستخدمين للتجارة الإلكترونية/ المعاملات عبر الإنترنت. • مراجعة السياسات للتحقق مما إذا كان نقل البيانات خارج الجهة يتطلب عمل نموذج مشفر منها قبل الإرسال. • الاستفسار عما إذا كانت سياسات أمن المعلومات قد نفذت وفقا لتصنيف مدى حساسية البيانات في الجهة (على سبيل المثال، السرية، الحساسة). • من خلال الاستفسار يتم تحديد ما إذا كان العميل يستفيد بالشكل الأمثل من التشفير لمعالجة المعلومات الحساسة. • في حال ذلك، يقوم المدقق بإجراء اختبار للتحقق من الصحة. **إجراءات اختبار التحقق من الصحة:** **اختبار التحقق الأول:** فاعلية تشغيل ضوابط التشفير: التأكد من: وجود إجراءات لدورة حياة مفاتيح التشفير الرئيسية. اتلاف مفتاح التشفير. فصل المهام بين المصرح لهم بحفظ مفاتيح التشفير.

موضوع التدقيق العاشر: إدارة اعدادات النظام هل ضوابط إعدادات النظام المستخدمة ملائمة لتطبيقات تكنولوجيا المعلومات؟	
المعايير: أن يكون نظام الاعدادات واضحا ويدار بشكل جيد بحيث يدعم أمن المعلومات في الاتصالات والعمليات.	
المعلومات المطلوبة	**وسائل التحليل**
• السياسات والإجراءات التي تشير إلى الأمور المتعلقة بإعدادات النظام في مناطق العمل. • قوائم / مكتبة اعدادات النظام.	• مراجعة مصفوفات المهام لتحديد من هو المسؤول عن إدارة إعدادات النظام، وما هو نطاق ضوابط الإعدادات في العمليات. • التحقق من الطريقة التي تم بها التسجيل والرقابة والتحديث. • التحقق مما إذا حدث أي مشاكل في الماضي بسبب اختلافات في إعدادات النظام. وإذا كان الأمر كذلك، إجراء مقابلات مع المدراء للتحقق من الإجراءات التي نفذت لتغييرات إعدادات النظام.
نتائج التدقيق: يقوم المدقق بتعبئتها.	

إدارة الأصول	
هدف التدقيق: تشجيع الحماية الملائمة لأصول تكنولوجيا المعلومات.	
موضوع التدقيق الحادي عشر: إدارة الأصول هل لدى الجهة نظام ملائم لإدارة الأصول بحيث يدعم أمن المعلومات؟	
المعايير: ضمان حماية مناسبة لأصول المعلومات: (راجع: سلسلة أيزو 2700 لنظام إدارة أمن المعلومات، COBIT، والسياسات الداخلية الأخرى، والإجراءات أو القوانين المطبقة).	
المعلومات المطلوبة	**وسائل التحليل**
• سياسة إدارة الأصول. • تصنيف الأصول. • تصنيف المعلومات.	• مراجعة السياسات للتحقق من وجود سياسة استخدام مقبولة للأجهزة والبرمجيات تكنولوجيا المعلومات (مثال، يمكن استخدام الكمبيوتر المحمول للاستخدام الشخصي ما لم يتعارض مع الأعمال الرسمية).

• إجراءات التخلص من الأصول. • تقارير التدقيق المالي (ان كانت تشير إلى الأصول والمخزون).	• التحقق مما إذا كانت قاعدة بيانات الأصول حديثة. • التحقق من سجلات التخزين للتأكد أن الأصول مصنفة من حيث القيمة، والحساسية، أو وفق فئات أخرى. • مراجعة إجراءات التخلص من الأصول والمستوى الوظيفي للمشرف على الاجراءات. والتحقق من شرط الحصول على تصريح لأي موضوع يتعلق بالتخلص من الأصول أو إعادة استخدام المعدات. والاستفسار من الأشخاص والتحقق من الأحكام التي تضمن أن يتم مسح البيانات قبل التخلص من الأصول أو إعادة استخدام المعدات.
نتائج التدقيق: يقوم المدقق بتعبئتها.	

أمن الموارد البشرية	
هدف التدقيق: التأكد من أن جميع الموظفين (بما في ذلك المقاولين وأي مستخدم للبيانات الحساسة) مؤهلين للتعامل مع البيانات ومدركين لأدوارهم ومسؤولياتهم، وأن يتم إلغاء صلاحية الوصول حال انتهاء خدمة الموظف أو انتهاء عقد العمل.	
موضوع التدقيق الثاني عشر: وعي ومسئوليات الموظفين **هل الموظفين على وعي وإدراك بأدوارهم ومسئولياتهم فيما يتعلق بمهامهم ومسئولياتهم الأمنية؟**	
المعايير وجود موظفين مدربين بإتقان على حماية أمن المعلومات.	
المعلومات المطلوبة	**وسائل التحليل**[57]
سياسة الموارد البشرية وإجراءات التوظيف.	• فحص عينة من وثائق التوظيف الخاصة ممثلة لموظفي تكنولوجيا المعلومات للتأكد من إتمام تقييم مؤهلاتهم والتحري عن خلفيتهم.

[57] الموارد البشرية –مقارنة بأمن المعلومات تعتبر أحد المواضيع الرئيسية في الأقسام الأخرى بما في ذلك حوكمة تكنولوجيا المعلومات، وأجزاء من هذه المصفوفة مثل سياسة أمن المعلومات (الوعي والمسؤولية، وطريقة تدفق المعلومات والجزاءات) وضوابط الدخول (حقوق المستخدم الفردية).

سياسة وإجراءات أمن المعلومات. معيار الكفاءة لموظفي تكنولوجيا المعلومات. تقارير تقييم الموظفين. تقارير الحوادث الأمنية (تشمل انتهاك أخلاقيات المهنة أو السلوك المهني). حملة للتوعية بالأمور الأمنية. أدوار ومسئوليات إدارة المستخدم.	• فحص معايير الاختيار لأداء عمليات التدقيق على الخلفية الأمنية للمتقدم والموافقة عليها. • يجب أن يكون دور كل منصب واضح. ويجب تفعيل الأنشطة الإشرافية للتحقق من الالتزام بالسياسات والإجراءات الإدارية، وميثاق أخلاقيات المهنة، والسلوك المهني. • التحقق من أن الأدوار الهامة لأمن المعلومات محددة وموثقة بوضوح وموثقة. وأن الموظفين والأطراف الأخرى الموكلة لهم هذه المهام على دراية بمسئولياتهم فيما يتعلق بحماية أصول المعلومات للجهة، بما في ذلك البيانات الإلكترونية، البنى التحتية لنظم المعلومات، والوثائق. وإجراء المراجعة لتحديد الأدوار الهامة التي تتطلب موافقة أمنية. وهذا يجب أن ينطبق على الموظفين والمقاولين والموردين. • التحقق من وجود فصل مناسب بين الواجبات المناسب بين إدارة أمن تكنولوجيا المعلومات، والعمليات. • التأكد من أن سياسة التوظيف في تكنولوجيا المعلومات، والتدوير والنقل، وإنهاء خدمات الموظفين واضحة لتخفيف الاعتماد على الفرد الواحد. والتحقق من آليات نقل المعرفة التي يتم ممارستها.

موضوع التدقيق الثالث عشر: التدريب

هل التدريب على إجراءات أمن المعلومات فعال في تعزيز المهارات المهنية للموظفين لحماية أمن المعلومات؟

المعايير:

طريقة التدريب على أمن المعلومات في الجهة والنطاق الذي يغطيه والفترات الدورية التي يتم عمل التدريب خلالها.

المعلومات المطلوبة	وسائل التحليل
• جدول التدريب. • نتائج الاختبارات النهائية.	• تقييم عملية قياس فعالية التدريب، ان وجدت، للتأكد من أنها تتضمن التدريب على مواضيع أمن تكنولوجيا المعلومات الهامة ومتطلبات التوعية.

• تقييم فعالية التدريب.	• فحص محتوى برنامج التدريب على أمن تكنولوجيا المعلومات للتأكد من اكتماله ومدى ملاءمته. وفحص آليات التنفيذ لتحديد ما إذا كان يتم تقديم المعلومات إلى كافة المستخدمين لموارد تكنولوجيا المعلومات، بما في ذلك الاستشاريين والمقاولين والموظفين المؤقتين، وان اقتضى الأمر، الزبائن والموردين. • فحص محتوى البرنامج التدريبي للتأكد من تضمين كافة أطر المراقبة الداخلية ومتطلبات الأمن استناداً إلى السياسات الأمنية للجهة والضوابط الداخلية (مثل، أثر عدم الالتزام بالشروط الأمنية، والاستخدام المناسب لموارد ومرافق الشركة، التعامل مع الحوادث الطارئة، ومسؤولية الموظف تجاه أمن المعلومات). • الاستفسار والتأكد من أن المواد والبرامج التدريبية تتم مراجعتها بصورة منتظمة للتأكد من ملاءمتها. • فحص السياسة لتحديد الاحتياجات التدريبية، والتأكد أن سياسة التدريب تضمن وجود المتطلبات الضرورية للجهة في برامج التدريب والتوعية. • مقابلة الموظفين للتأكد أنهم خضعوا للتدريب المؤسسي، وعما إذا كانوا يدركون بوضوح مسئوليات الحفاظ على أمن وسرية المعلومات.
نتائج التدقيق	

الأمن المادي
هدف التدقيق: منع سرقة أو تلف اجهزة تكنولوجيا المعلومات، والدخول غير المصرح به، ونسخ أي معلومات حساسة أو الاطلاع عليها.
موضوع التدقيق الرابع عشر: سلامة أماكن العمل **هل المباني والأراضي التابعة للجهة آمنة ضد المخاطر المادية والبيئية؟**
المعايير: التأكد من استمرار التزام الأمن المادي والبيئي بمتطلبات السلامة وتصنيف الحساسية لأصول تكنولوجيا المعلومات.

المعلومات المطلوبة	وسائل التحليل
• مخطط الشبكة. • خطة أمن الموقع. • تقرير الفحص المادي الدوري. • تقارير واردة من قبل الخدمات ذات الصلة (مثل إدارة المطافئ).	• تحليل الضوابط الأمنية المادية الرئيسية للجهة الخاضعة للتدقيق. والتحقق من أنها تتماشى مع تحاليل المخاطر الحديثة. • مراجعة التدابير الاحترازية المادية وفي الموقع للعناصر الرئيسية للبنية التحتية. والتحقق من الضوابط البيئية الموجودة (مطفأة الحريق، صفارة الإنذار، أنظمة الطاقة، إلخ). • التحقق من تنفيذ التوصيات المقدمة من الخدمات ذات الصلة (خاصة رجال الإطفاء، وتفتيش المساكن، والوقاية من الكوارث). • (بالنسبة للخطط الأمنية المتعلقة بالكوارث، الرجاء الرجوع لقسم خطة استمرارية الأعمال وخطة استعادة الأوضاع بعد الكوارث من هذا الدليل).

موضوع التدقيق الخامس عشر: الدخول المادي

كيف تضمن الجهة دخول الموظفين المصرح لهم فقط إلى مرافق العمل؟

المعايير:

تضع الجهة تدابير أمنية لضمان عدم الدخول الأشخاص غير المصرح لهم إلى المرافق الهامة لتكنولوجيا المعلومات (غرف الأجهزة، مخزن البيانات، إلخ)

المعلومات المطلوبة	وسائل التحليل
• مخطط تركيب أجهزة تكنولوجيا المعلومات. • خطة أمن الموقع. • اعدادات الأجهزة. • التقرير الدوري للفحص المادي. • تقارير الحوادث الطارئة.	• مراجعة التعليمات الأمنية، وخطط للشبكة والوثائق ذات الصلة والتحقق من الطريقة التي تتحكم من خلالها الجهة في الوصول إلى المناطق الحساسة من مبانيها. • مراجعة ومراقبة حركة الدخول والخروج وكيف يعمل نظام الأمن المادي. • تحديد ما هي الوسائل المستخدمة. الحصول على السياسات والإجراءات فيما يتعلق بأمن المرافق (البوابات، الهويات، بوابات الدخول، الحراس، الحواجز، المفتاح، بطاقة التصريح بالدخول إلخ) وتحديد إذا كانت تلك الإجراءات يمكن الاعتماد عليها للتعرف على الأشخاص والسماح لهم بالدخول.

	• التحقق من الأشخاص الذين يتحكمون ويحافظون على الاعتمادات المخصصة للتحكم في الوصول إلى المواقع الحساسة. والتحقق من أن مستوى الإدارة ملائم لأمن المعلومات. • التأكد أن الدخول إلى المناطق الأمنية /الغرف المؤمنة/ مواقع الخوادم محظور. • اختيار عينة من الموظفين/المستخدمين، وتحديد ما إذا كانت إجراءات دخولهم إلى المرافق ملائمة، استناداً إلى مسؤولياتهم الوظيفية. • التحقق مما إذا كان يتم الإبلاغ عن الحوادث لنظام إدارة الحوادث والمشاكل. والتأكد من أنه تم تحليلها والاستفادة منها.
موضوع التدقيق السادس عشر: الدفاع عند اقتحام الأجهزة **التأكد من وجود سياسة في الجهة لكشف محاولات الاقتحام وأنه يتم العمل بها.**	
المعايير: وجود إجراء في سياسة الأمن الداخلي لاتخاذ ما هو مناسب في التصدي للاقتحام.	
المعلومات المطلوبة	**وسائل التحليل**
• الخطة الأمنية للموقع. • اعدادات الأجهزة. • تقارير الحوادث الطارئة.	• الاستفسار حول الطريقة التي تعرف وحدة الأمن في الجهة من خلالها وقوع حوادث الاقتحام في المواقع المؤمنة. • التحقق من الإرشادات لمعرفة الطريقة التي يتم من خلالها التعامل مع الاقتحام لتأمين المباني أو المساحات. • التحقق من التقارير حول الحوادث لتحديد ما إذا قد تم اكتشاف الاقتحام في وقت مبكر. • التحقق إذا كان لدى الجهة سياسة واضحة لمنع الدخول غير المصرح به.
نتائج التدقيق	

ضوابط الدخول	
هدف التدقيق: ضمان وصول الأشخاص المصرح لهم فقط الى المعلومات ذات الصلة.	
موضوع التدقيق السابع عشر: سياسة الدخول هل لدى الجهة سياسة واضحة وفعالة للتحكم بالدخول؟	
المعايير: أن تقدم سياسة الدخول أساسا سليما للضوابط على توزيع المعلومات ذات الصلة.	
المعلومات المطلوبة	**وسائل التحليل**
• سياسة وإجراءات الدخول. • قائمة بالمستخدمين. • قائمة أو مصفوفة لضوابط الدخول.	• تحليل سياسة وإجراءات الدخول لضمان أن يتم فصل واجبات الموظف ومجالات المسؤولية من أجل تقليل فرص الدخول غير المصرح به واعتماد تصريح الدخول. • ***اختبار التحقق من الصحة:*** فاعلية تصريح الدخول المعمول به للسماح للمستخدم بالدخول إلى الشبكة المحلية (يجب إجراء اختبار منفصل لدخول المستخدم إلى التطبيقات ويجب أن يتم بالتزامن مع مراجعة التطبيق). • اختيار عينة من حسابات المستخدم والنظام لتحديد وجود (يمكن استخدام برنامج لمراقبة الدخول) التالي: ○ الأدوار والصلاحيات المطلوبة محددة بوضوح ومرتبطة بالمهام الوظيفية. ○ شرح أسباب حاجة العمل الداعية للحصول على تصريح الدخول. ○ اعتماد مالك البيانات والتصريحات الإدارية (مثل التوقيع / والاعتمادات المكتوبة). ○ تبرير الأعمال/ المخاطر والاعتمادات الإدارية للطلبات التي لا تتوافق مع المعايير. ○ يجب أن يتناسب طلب الوصول إلى المعلومات مع المهام والأدوار الوظيفية والفصل المطلوب بين المهام.

موضوع التدقيق الثامن عشر: إدارة صلاحيات الدخول هل عملية منح ورفض صلاحية التحكم بالدخول للموظفين والمقاولين آمنة وفعالة؟	
المعايير: أن تقوم وظيفة أمن المعلومات بمراقبة عمليات إدارة حساب المستخدم في حينها وتسجل مدى كفاءة وفعالية العمل.	
المعلومات المطلوبة	**وسائل التحليل**
• إجراءات الرقابة على الدخول. • عينة من عمليات نقل وإنهاء خدمات الموظفين.	• التحقق من الإجراءات لتحديد مدى قيام الجهة بمراجعة مختلف صلاحيات وامتيازات الدخول الممنوحة للموظفين أو المستخدمين في الجهة. • التحقق من كيفية التأكيد على الصلاحية التي تمنح للموظف (مثل الاستفسار من المشرف، مدير المنطقة، المجموعة، إلخ). • مقابلة عينة من المستخدمين والتحقق من الإرشادات للتأكد من طريقة ابلاغ المستخدمين حول مسئولياتهم في حماية المعلومات أو الأصول الحساسة عند منح صلاحية الدخول لهم. • التأكد من أن الممارسات الأمنية في الجهة تتطلب ان يكون كل مستخدم وعملية من عمليات النظام معرف على حدة وأن يتم اعداد النظام لإجبار التصريح بالدخول قبل السماح به، وأن تستخدم آليات الرقابة للتحكم في الدخول المنطقي بالنسبة لجميع المستخدمين، وعمليات النظام وموارد تكنولوجيا المعلومات. • تحليل صلاحيات الدخول التي تختلف عن صلاحية الدخول من خلال كلمة المرور، مثل الدخول من موقع آمن وباستخدام الأجهزة الأمنية أو قارئ بصمات الأصابع، إلخ). • ***اختبار للتحقق من الصحة الأول:*** فاعلية عمليات نقل وانهاء خدمات الموظفين المعمول بها: ○ الحصول من إدارة الموارد البشرية على عينة من سجل نقل الموظفين وإنهاء خدماتهم ومن خلال مراجعة ملفات حساب النظام أو أدوات وتقنيات التدقيق باستخدام الحاسوب CAATs (مثل ACL، IDEA) يتم التأكد من تعديل او سحب صلاحيات الدخول في الوقت المناسب.

	• ***اختبار للتحقق من الصحة الثاني***: إدارة كلمات المرور: ○ التحقق من أن متطلبات الجودة لكلمات المرور معرفة ومفروضة من قبل نظام إدارة الشبكة وأنظمة التشغيل التي تستند إلى الاحتياجات المحلية أو سياسة الجهة أو أفضل الممارسات.
نتائج التدقيق	

حيازة وتطوير وصيانة نظم تكنولوجيا المعلومات في الملحق الثالث

إدارة استمرارية الأعمال في الملحق السادس

الملحق الثامن

المصفوفة المقترحة للتدقيق على ضوابط التطبيقات

<table>
<tr><th colspan="2">المدخلات</th></tr>
<tr><td colspan="2">هدف التدقيق: التأكد من أن البيانات المدخلة في التطبيق صحيحة ويتم إدخالها من قبل موظف مخول.</td></tr>
<tr><td colspan="2">موضوع التدقيق الأول: التأكد من صحة المدخلات
هل لدى التطبيق ضوابط كافية للتحقق من صحة المدخلات؟</td></tr>
<tr><td colspan="2">المعايير:
توفر العديد من الممارسات الجيدة أساسا لمعايير ضوابط التحقق من صحة المدخلات والمخرجات، على سبيل المثال.

تكون قواعد التحقق من الصحة شاملة وموثقة وتنفذ في واجهات الإدخال في التطبيق، وتوثيق أساليب مختلفة وواجهات لإدخال البيانات، ورفض التطبيق بشكل ملائم إدخال أي بيانات غير صحيحة، ويتم تحديث معايير التحقق من الصحة باستمرار بالوقت والتصريح المناسب، ووجود رقابة تعويضية مثل السجلات (Logs) وقواعد الحصول على التصاريح في حالة إمكانية حدوث تجاوزات في الرقابة على المدخلات؛ ووجود ضوابط سليمة، ووثائق خاصة بواجهات التطبيق.</td></tr>
<tr><td>المعلومات المطلوبة</td><td>وسائل التحليل</td></tr>
<tr><td>• متطلبات وقواعد العمل.
• أنواع مدخلات البيانات.</td><td>• تحليل قواعد ومتطلبات العمل ووثائق التطبيق والاستفسار من أصحاب الأعمال لتحديد قواعد التحقق التي يجب تأكيد صحتها في العملية التي يجري تقييمها. والتأكد أن قواعد التحقق من الصحة قد صممت ووثقت بشكل مناسب. والتأكد مما إذا كانت ضوابط التحقق من صحة عمليات إدخال البيانات مفروضة على التطبيق فعليا: ومراقبة مستخدمي التطبيق خلال العمل الفعلي، وتشغيل التطبيق في بيئة الاختبار واختبار واجهات مختلفة لإدخال البيانات؛ وتحليل البيانات</td></tr>
</table>

• متطلبات الالتزام القانوني والخارجي. • هيكل واجهة البيانات مع التطبيقات الأخرى. • رسومات تخطيطية لتدفق النظام. • دليل المستخدم. • قواعد التحقق من الصحة.	المخزنة في قاعدة البيانات من خلال استخدام أدوات وتقنيات التدقيق باستخدام الحاسوب CAATs. • الحصول على وصف وظيفي لكل فئة من فئات المدخلات والتصاميم الخاصة بالمعلومات حول إدخال بيانات العمليات. والتحقق من الوظيفة والتصميم لوجود الفحوصات المنتظمة والمتكاملة لرسائل التنبيه بالأخطاء. وإن أمكن، مراقبة إدخال بيانات المعاملات. • التأكد أن معايير ومؤشرات التحقق من صحة بيانات المدخلات تتناسب مع قواعد العمل وأنها تجبر رفض أي نوع من أنواع المدخلات غير الملائمة. وفي حال نظام المعالجة على الانترنت، يجب التحقق من رفض أو تعديل البيانات المدخلة غير الصحيحة واختبار المعالجة المنطقية او الحسابات التي تم تنفيذها. الرموز التشغيلية لقواعد البيانات (مثلا، *، =، أو select)، يجب عدم السماح بإدخالها حيث يمكن استخدامها لتعطيل أو استرجاع المعلومات من قاعدة البيانات. • الاستفسار من المديرين حول ما إذا كانت معايير ومؤشرات التحقق من الصحة في إدخال البيانات تتم مراجعتها وتأكيدها وتحديثها بشكل دوري، في الوقت المناسب وبشكل قانوني. ويمكن الحصول على ضمانات من خلال مراجعة الوثائق، وتحليل التعليمات البرمجية أو المقابلات. • التحقق من الوثائق من أجل التأكد من إمكانية تجاوز عمليات التحقق من صحة إدخال البيانات والضوابط. والتأكد من أن تسجيل التجاوزات ومراجعة ملاءمتها يتم بشكل صحيح. والتحقق مما إذا كانت صلاحية التجاوز تقتصر على الإشرافيين فقط وعلى عدد محدود من الحالات. ومراجعة عمليات تصحيح الأخطاء والتجاوزات في الدخول والوثائق الأخرى للتحقق من أنه يتم اتباع الإجراءات. • تحديد الواجهات التي تتواجد مع التطبيق. يمكن أن تكون هذه الواجهات في شكل إرسال البيانات بطريقة لحظية أو بشكل دوري لملفات البيانات دفعة واحدة (Batch Processing). ومراجعة الرسومات التخطيطية لتدفق النظام ورموز برمجته، وإجراء مقابلات مع مطوري التطبيقات أو المسؤولين عن تشغيل النظام

	للحصول على المعلومات حول الواجهات والرقابة عليها. مثلاً: الضوابط على مجاميع واجهة الإرسال. مثل HASH[58].

موضوع التدقيق الثاني: هل تعتبر طريقة إدارة الوثائق الأصلية وجمع البيانات وإدخالها ملائمة؟	
المعايير: أن تكون إجراءات إعداد البيانات موثقة ومفهومة من قبل المستخدمين؛ ووجود تسجيل وسجلات صحيحة للوثائق الأصلية الواردة حتى مرحلة التخلص منها، ووجود أرقام متسلسلة وغير مكررة لكل معاملة الكترونية، ويتم الاحتفاظ بالمستندات الأصلية للفترة الزمنية المحددة من قبل المعايير القانونية أو السياسات.	
المعلومات المطلوبة	**وسائل التحليل**
• تصنيفات الوثائق الأصلية. • معيار الجهة لتوقيت واكتمال ودقة الوثائق الأصلية. • إجراءات إعداد البيانات. • واجهات البيانات مع التطبيقات الأخرى.	• يقوم المدقق بفحص ومراقبة عملية إنشاء وتوثيق إجراءات إعداد البيانات، والاستفسار عما إذا كانت الإجراءات مفهومة وتستخدم وسائط المصدر الصحيحة. • التأكد أن مجموعة معالجة البيانات (DP) أو ما يعادلها من مجموعات العمل تحتفظ بسجل بالوثائق الأصلية لجميع إدارات المستخدم الواردة وحتى التخلص منها نهائياً. والتحقق من وجود نظام تسوية للسجلات مع مجموعات إدارة المستخدمين. • التأكد أن جميع الوثائق الأصلية تشتمل على المحتويات القياسية بتوثيق ملائم (مثل التوقيت، ورموز الإدخال المحددة مسبقا، والقيم الافتراضية) وأنها مصرح بها من قبل الإدارة. • التحقق أن الوثائق الأصلية الهامة قد تم ترقيمها مسبقا وكيف يتم التعرف على الأرقام الخارجة عن التسلسل وأخذها بعين الاعتبار. تحديد ومراجعة الأرقام

[58] PC Magazine Encyclopedia from http://www.pcmag.com/encyclopedia/term/44130/hash-total:

طريقة لضمان دقة البيانات المعالجة. الـ Hash عبارة عن مجموع عدة خانات من البيانات في الملف، شاملا حتى الخانات التي لا تستخدم في الحسابات، مثل رقم الحساب. في المراحل المختلفة أثناء المعالجة، يتم إعادة احتساب مجموع Hash ومقارنته بالأصلي. إذا فقدت أي من البيانات أو تغيرت، تظهر إشارة لعدم التطابق في القيمة.

• سياسات الاحتفاظ بالوثائق. • الرسوم التخطيطية لسير عمل النظام.	غير المتسلسلة والفجوات والتكرارات في تسلسل الأرقام باستخدام الأدوات الآلية مثل أدوات وتقنيات التدقيق باستخدام الحاسوب CAATs. والتحقق من وجود أرقام محددة ومتسلسلة لكل معاملة لمنع الازدواجية. • الاستفسار من الموظف المسئول حول سياسات الاحتفاظ بالبيانات والتأكد كيف يتم ضمان تنفيذ هذه السياسات، ويمكن أخذ عينة من سجلات النظام لفحصها ومقارنتها مع الوثائق الأصلية.

موضوع التدقيق الثالث:

هل يتضمن التطبيق إجراءات كافية للتعامل مع الأخطاء؟

المعايير:

وجود نظام واضح لرسائل التنبيه عن الأخطاء لتوصيل المشاكل حتى يمكن اتخاذ إجراءات تصحيحية فورية لكل نوع من أنواع الخطأ. ويتم تصحيح الأخطاء أو تجاوزها على نحو ملائم قبل عملية المعالجة. ويتم مراجعة السجلات الإلكترونية بشكل دوري، واتخاذ الإجراءات التصحيحية اللازمة.

المعلومات المطلوبة	وسائل التحليل
• أنواع الأخطاء ورسائل التنبيه. • إجراءات مراجعة السجل. • سياسات وإجراءات التعامل مع البيانات المرفوضة. • إجراءات مراجعة الملفات المعلقة او الموقوفة.	• يقوم المدقق بمناقشة الأخطاء بالنظام والتعامل مع الاستثناءات مع مطور النظام و/أو المدير، والاستفسار والتأكد من وجود الإجراءات والسياسات للتعامل مع المعاملات التي لم تجتاز اختبارات التعديل والصحة. • التحقق مما إذا كان النظام يحتوي على رسائل الأخطاء لكل نوع من الأخطاء (على مستوى الحقول أو على مستوى المعاملات) التي لا تتوافق مع متطلبات ضوابط صحة تعديل البيانات. • التحقق من كيفية تعامل التطبيق إذا تم رفض البيانات من قبل ضوابط المدخلات. والتحقق ما إذا كانت هذه البيانات يتم تسجيلها أو تكتب تلقائيا في الملف المعلق. والتحقق مما إذا كان الملف المعلق الآلي يشمل رموز تشير إلى نوع الخطأ، وتاريخ ووقت الدخول وتحديد الشخص الذي قام بإدخال البيانات. تقييم إذا كانت هناك إجراءات لمراجعة وتصحيح البيانات في الملف المعلق قبل معالجته مرة أخرى. والتأكد من وجود إجراءات لتصعيد الخطأ عندما تكون معدلات الخطأ مرتفعة جداً وتم اتخاذ إجراءات تصحيحية.

	• الاستفسار من المدراء عن وجود إجراءات للمراجعة الدورية للسجل. والتحقق مما إذا كانت الإجراءات تشمل البدء في اتخاذ تدابير تصحيحية. والحصول على أدلة – مادية كانت أو رقمية – أن مراجعة السجل تتم بشكل دوري.

موضوع التدقيق الرابع:

كيف تتم إدارة منح صلاحية إدخال البيانات في التطبيق؟

المعايير:

وجود مستويات صلاحية للقيام بالمعاملات ويتم فرضها من خلال استخدام ضوابط ملائمة، وهناك فصل مناسب للمهام الخاصة بإدخال البيانات ووجود ضوابط تعويضية للحالات التي لا يمكن معها فصل المهام.

المعلومات المطلوبة	وسائل التحليل
• متطلبات الالتزام القانونية والخارجية. • متطلبات وقواعد العمل. • أدلة المستخدم.	• يقوم المدقق بالاستفسار والتأكد أن تصميم النظام يتيح وجود قوائم للصلاحيات المعتمدة مسبقا. والتحقق من خلال البحث في قوائم الصلاحيات، أن مستويات الصلاحية محددة بشكل ملائم لكل مجموعة من المعاملات. والتأكد من أن قواعد منح الصلاحيات لإدخال البيانات وتحريرها وقبولها ورفضها وتجاوزها في المعاملات الرئيسية مصممة وموثقة بشكل جيد. • يقوم المدقق بالتأكد أن مستويات منح الصلاحيات يتم تطبيقها بشكل صحيح من خلال تشغيل التطبيق في بيئة الاختبار. والتحقق، من خلال استخدام أدوات وتقنيات التدقيق باستخدام الحاسوب CAATs أو وحدات التدقيق المضمنة، أن صلاحيات السجلات الموجودة في قاعدة البيانات متوافقة مع قواعد منح الصلاحيات المحددة. • التأكد من وجود جدول للفصل بين الواجبات، ومراجعته لتحقق من وجود الفصل الملائم بين الواجبات والوظائف الرئيسية والمعاملات المعتمدة، ثم الاطلاع على قائمة المستخدمين وامتيازات الدخول الخاصة بالمستخدم. وتقييم ما إذا كان الفصل بين الواجبات يضمن أن الشخص المسئول عن اقفال البيانات غير مسؤول أيضا عن التحقق من صحة الوثائق. والتحقق من اعتماد الضوابط التعويضية في الحالات التي لا يفيد معها الفصل بين الواجبات.

المعالجة

هدف التدقيق: تقييم أن التطبيق يضمن كمال وصحة وموثوقية البيانات خلال دورة معالجة المعاملات.

موضوع التدقيق الخامس:

هل قوانين ومتطلبات العمل منفذة بشكل صحيح في التطبيق؟

المعلومات المطلوبة	وسائل التحليل
• توثيق التطبيق. • متطلبات وقواعد العمل. • رسومات تخطيطية لتدفق البيانات. • قائمة بالمعاملات ذات الأهمية الكبيرة. • رمز المصدر.	• التعرف على البرامج القابلة للتنفيذ في التطبيق من خلال دراسة مخطط سير البيانات ومطابقته مع قواعد إجراءات العمل المحددة والقائمة. • مراجعة وثائق التطبيق للتحقق من أنها منطبقة ومناسبة للمهمة. وحيثما كان ذلك مناسباً، يتم مراجعة الرموز (Code) للمعاملات الحيوية للتأكد من أن الضوابط الموجودة في الأدوات والتطبيقات تعمل كما يجب. وإعادة معالجة عينة للتحقق من أن الأدوات الآلية تعمل على النحو المنشود. • بالنسبة للمعاملات ذات الأهمية القصوى، يتم إنشاء نظام اختباري يعمل مثل النظام المباشر (live system). ومعالجة المعاملات في النظام الاختباري للتأكد من أن معالجة المعاملات تتم على نحو ملائم وفي الوقت مناسب.

موضوع التدقيق السادس:

هل تضمن ضوابط النظام سلامة المعاملات من العبث واكتمالها؟

المعايير:

يحدد التطبيق بشكل صحيح الأخطاء في المعاملات. ويتم الحفاظ على سلامة البيانات حتى أثناء الانقطاع غير المتوقع لمعالجة المعاملات. وهناك آليه مناسبة للتعامل مع الأخطاء أثناء المعالجة، ومراجعة الملفات المعلقة والمجازة.

المعلومات المطلوبة	وسائل التحليل
• توثيق تصميم التطبيق.	• تقييم ما إذا لدى التطبيق تحقيقات كافية لصحة البيانات وذلك للتأكد من سلامة المعالجة. وفحص الوظائف والتصميمات للتأكد من عدم وجود أخطاء في

• متطلبات وقواعد العمل. • التقارير غير المتوازنة. • التسويات. • إجراءات مراجعة التقارير. • الملفات المعلقة.	التسلسل وعدم حدوث الازدواجية وإجراء تدقيق لرقم المرجع، والتحكم، وإجماليات التجزئة[59] (Hash Totals). • فحص التسويات والوثائق الأخرى للتأكد من أن عدد المدخلات تتوافق مع عدد المخرجات لضمان اكتمال معالجة البيانات. وتتبع المعاملات من خلال العملية للتحقق من أن فعالية التسويات تحدد ما إذا كانت مجاميع الملف متطابقة او يتم الإبلاغ عن الحالات الغير المتوازنة. والاستفسار عما إذا كانت الملفات الرقابية تستخدم لتسجيل المعاملات والقيم النقدية وأن القيم تتم مقارنتها بعد تسجيلها. • التأكد من إعداد التقارير التي يتم فيها تحديد حالات عدم التوازن ومراجعتها واعتمادها وتوزيعها على الموظفين المناسبين. • أخذ عينة من مدخلات المعاملات واستخدام التحليل الآلي المناسب وأدوات البحث لتحديد الحالات التي يحدث فيها الأخطاء بكثرة والحالات التي لا يتم فيها اكتشاف الأخطاء. • الاستفسار والتأكد من استخدام الأدوات، وحيثما كان ملائما، المحافظة تلقائيا على تكامل البيانات خلال حدوث انقطاع غير متوقع في معالجة البيانات. والتحقق من أن مسار التدقيق والوثائق والخطط والسياسات والإجراءات الأخرى التي يتم فيها التحقق من إمكانات النظام وأنها مصممة بفعالية لتحافظ تلقائيا على تكامل البيانات. • فحص الوصف الوظيفي وتصميم المعلومات في إدخال بيانات المعاملات للتحقق مما إذا كان يتم ترحيل المعاملات التي لا تجتاز إجراءات التأكد من صحة المعاملة الى الملف المعلق. والتحقق من أن الملفات المعلقة يتم إنشاؤها بشكل صحيح وثابت، وأن يتم إعلام المستخدمين عما تم ترحيله إلى الحسابات المعلقة. وبالنسبة إلى عينة نظم المعاملات، يجب التحقق من أن الحسابات والملفات المعلقة للمعاملات التي لا تجتاز اجراءات التحقق من صحة المعاملات تحتوي فقط على الأخطاء الحالية. والتأكد أن المعاملات الفاشلة القديمة تمت معالجتها بشكل ملائم.

[59] نفس المرجع السابق

المخرجات

هدف التدقيق: التأكد أن النظام يضمن تكامل ودقة المعلومات المخرجة قبل استخدامها والتأكد من حماية المعلومات بشكل مناسب

موضوع التدقيق السابع:

هل لدى التطبيق ضوابط لضمان تكامل ودقة المخرجات؟

المعايير:

تم تصميم الإجراءات لضمان أنه يتم التحقق من اكتمال ودقة مخرجات التطبيق قبل استخدام المخرجات للمعالجة اللاحقة، بما في ذلك الاستخدام في معالجة المستخدم النهائي، وتعقب صحة مخرجات التطبيق مفعلة بشكل ملائم، وأن المخرجات تتم مراجعتها لضمان معقوليتها ودقتها، وأن الرقابة على التكامل والدقة تتم بفاعلية

المعلومات المطلوبة	وسائل التحليل
• الرقابة على التكامل والدقة. • وسائل التوازن والتسوية. • قائمة بالمخرجات / التقارير الإلكترونية. • عينة من المخرجات الإلكترونية.	• الحصول على قائمة بالمخرجات الإلكترونية التي يعاد استخدامها من قبل تطبيقات المستخدم النهائي. والتأكد من انه يتم فحص المخرجات الإلكترونية لضمان اكتمالها ودقتها قبل إعادة استخدام وإعادة معالجة المخرجات. • اختبار توازن وتسوية المخرجات حسب الوسائل الموثقة. • اختيار عينة ممثلة للمخرجات الإلكترونية، وتعقب الوثائق المختارة من خلال المعالجة لضمان أنه تم التحقق من الاكتمال والدقة قبل أداء عمليات أخرى. • إعادة أداء اختبارات التكامل والدقة للتأكد من فعاليتها. • التأكد ما إذا كان كل منتج من المخرجات يحتوي على اسم او رقم برنامج المعالجة، العنوان أو الوصف، وفترة المعالجة المشمولة، اسم ومكان المستخدم، التاريخ والوقت المستغرق في الإعداد، والتصنيف الأمني.

	• اختيار عينة ممثلة لتقارير المخرجات، والتحقق من مدى معقولية ودقة المخرجات. والتأكد من الإبلاغ عن الأخطاء المحتملة وأنها مسجلة مركزيا.

موضوع التدقيق الثامن:

هل مخرجات البيانات محمية بشكل ملائم؟

المعايير:

هل يتم التعامل مع المخرجات وفقاً لتصنيفات السرية المطبقة، وهل عملية توزيع المخرجات / التقارير تتم مراقبتها بشكل مناسب.

المعلومات المطلوبة	وسائل التحليل
• إجراءات التعامل مع المخرجات وحفظها. • سياسات تصنيف المعلومات.	• مراجعة إجراءات التعامل مع المخرجات وحفظها المتعلقة بالخصوصية والأمن. وتقييم ما إذا كان تم تحديد الإجراءات التي تتطلب تسجيل الأخطاء المحتملة وحلها قبل توزيع هذه التقارير. وفحص نظام التسوية مجاميع الرقابة على المخرجات مع مجاميع الرقابة على المدخلات قبل اعتماد التقارير بهدف إنشاء بيانات متكاملة. • التحقق من وجود إجراءات موثقة لتحديد المخرجات الحساسة للتطبيق، وان اقتضت الضرورة، إرسال المخرجات الحساسة إلى أجهزة عليها رقابة خاصة في الدخول إلى المخرجات. ومراجعة وسائل توزيع المعلومات الحساسة والتحقق من سلامة تنفيذ الآليات لحقوق صلاحية الدخول على البيانات التي تم إنشاؤها.

أمن التطبيق

هدف التدقيق: التأكد ما إذا كان يتم تأمين معلومات التطبيق بشكل ملائم ضد سوء الاستغلال

موضوع التدقيق التاسع:

هل آليات تتبع التطبيق كافية للغرض المنشود منها؟

المعايير:

يوجد سجل للتدقيق الإلكتروني (Audit trail) يكشف عن عمليات التحرير والتجاوزات، وصلاحيات الاطلاع على المعاملات الحيوية؛ وتتم مراجعة سجل التدقيق دورياً لمراقبة أي نشاط غير عادي؛ وتتم حماية والمحافظة على سجل التدقيق على نحو كاف؛ ويتم تحديد رقم خاص ومتسلسل أو معرفات لكل معاملة.

المعلومات المطلوبة	وسائل التحليل
• هيكل وتوثيق سجل التدقيق. • سياسات التجاوز. • إجراءات المراجعة. • الرسوم التخطيطية للنظام.	• الحصول على الوثائق وتقييم التصميم والتنفيذ والصلاحيات ومراجعة مسارات التدقيق. فحص هيكل سجل التدقيق والوثائق الأخرى للتحقق أن سجل التدقيق قد تم تصميمه بفعالية. والاستفسار عن الشخص الذي بإمكانه ايقاف أو حذف مسارات التدقيق. • فحص مسار التدقيق، والوثائق الأخرى والخطط والسياسات والإجراءات للتأكد أنه تم تصميم التعديلات والتجاوزات والمعاملات ذات القيمة العالية بفعالية ليتم مراجعتها بالتفصيل. • يتم فحص مسار التدقيق والمعاملات والمراجعات والوثائق الأخرى، وتعقب المعاملات خلال العملية، وعند الامكان، استخدام جمع الأدلة الآلي بما فيها عينة البيانات، ونماذج التدقيق المدمجة أو أدوات وتقنيات التدقيق باستخدام الحاسوب CAATs، وذلك للتأكد أن المراجعة والصيانة الدورية لسجل التدقيق تكشف الأنشطة غير العادية بفاعلية وأن المراجعة التي تتم بواسطة المشرف فعالة. • الاستفسار كيف يتم تقييد الوصول لسجل التدقيق. ودراسة حقوق وسجلات الوصول اليه. والتحقق مما إذا تم الاطلاع على سجل التدقيق من قبل الأفراد المرخص لهم فقط. وتقييم ما إذا كان سجل التدقيق محمي ضد التعديلات ذات الصلاحيات العالية. • في حال تم تخصيص تعريف فريد لكل معاملة. فانه يجب التحقق باستخدام الجمع الآلي للأدلة ، إن أمكن.
موضوع التدقيق العاشر: **هل بيانات التطبيق محمية بشكل مناسب؟**	
للرقابة على الدخول المادي والمنطقي، الرجاء الرجوع للملحق السابع المتعلق بأمن المعلومات. وللتخطيط لاستعادة الأوضاع بعد الكوارث الرجاء الرجوع للملحق السادس المتعلق بالتخطيط لاستمرارية الأعمال وخطة استعادة الأوضاع بعد الكوارث.	

ملاحظات

ملاحظات

INTOSAI Working Group on IT Audit
c/o CAG of India
Pocket-9, DDU Marg,
New Delhi- 110124, India

www.intosaiitaudit.org

INTOSAI Development Initiative (IDI)
c/o Riksrevisjonen
Pilestredet 42
Postboks 8130 Dep.
N-0032 Oslo, Norway
www.idi.no