الأساليب الحديثة في تدقيق ومراجعة نظم المعلومات

الباحثة سندس نوري شكر
كلية التربية بنات- جامعة تكريت

المستخلص

اتسعت دائرة استخدام نظم المعلومات بشكل كبير بحيث دخلت كل مفاصل حياة الانسان المختلفة مما جعل فرص انتهاك واختراق تلك الانظمة امراً لامناص منه. لذلك فان الحاجة تستدعي ايجاد وسائل تقنية واطر جوهرية للتصدي لظاهرة حدوث أي خلل في نظم المعلومات من خلال مراجعة وتدقيق دورة حياة النظام.

يتطرق البحث الى جملة ادوات واساليب تقنية تساعد المدققين والمراجعين من تحديد الخلل وطبيعته وايجاد حل له . كما توفر للمراجعين والمدققين فرصاً اكثر في متابعة تنفيذ الرقابة الداخلية على مكونات برامج نظم المعلومات .

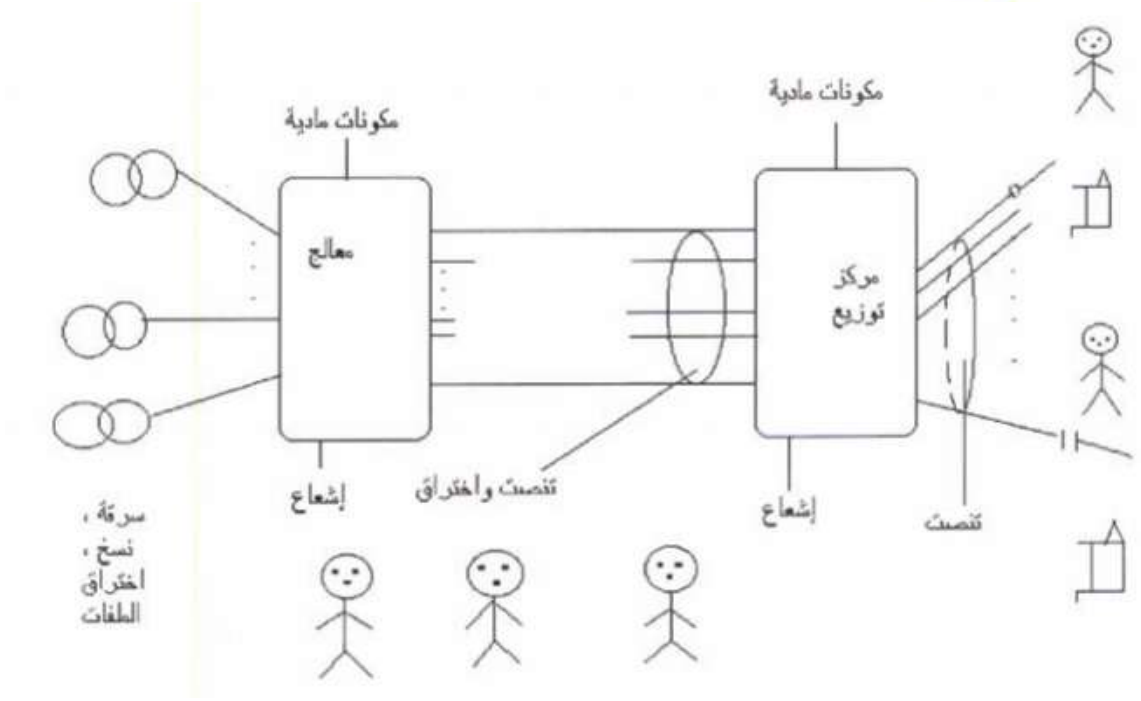
تمهيد

يشهد العالم تطوراً واسعاً في انظمة المعلومات وفي مجال الاتصالات وشبكات الانترنت مما جعل حياة الناس تعتمد بصورة مباشرة او غير مباشرة على صلاحية ومتانة الانظمة. وبالوقت نفسه تتعرض انظمة المعلومات وشبكات الانترنت الى اختراقات متنوعة الاغراض ومن مصادر مختلفة منها الفردية ومنها الحكومية ومن هنا فإن الواجب يحتم على مطوري ومستخدمي نظم المعلومات من التاكد من سلامة تلك الانظمة والمحافظة على خصوصيتها من كل عبث متعمد او غير متعمد .

وسنطلق على العبث الذي يهدف الى انتهاك حرمة نظم المعلومات بالمخاطر . ومن هنا نحتاج ان نتعرف على طبيعة تلك المخاطر وطرق تقديرها . ومما يجدر ذكره ان الوسائل المستخدمة لذلك تسمى وسائل المراجعة والتدقيق ولغرض تحقيق هدف البحث المتمثل في بيان الأساليب الحديثة في تدقيق ومراجعة نظم المعلومات سيتم التطرق إلى الآتي:

أولاً : تعريف المخاطر وما صدرها

تقوم الإدارة بتقدير المخاطر بوصفها جزءاً من تصميم وتشغيل نظام الرقابة الداخلية وذلك لتقليل الأخطاء والمخالفات، إذ إن جميع الوحدات الاقتصادية تواجه مخاطر عديدة سواء داخلية أو خارجية إثناء قيامها بأنشطتها وعملياتها. إذ يعد تقدير المخاطر من الأساليب المهمة في مراجعة نظم المعلومات وتعرف المخاطر بأنها التهديد الذي يستغل نقاط الضعف في مورد أو مجموعة موارد من اجل إحداث فساد أو خسارة للمورد. شكل (1) أدناه يبين بعض الأخطار المحدقة بنظم المعلومات .



شكل (1) : سلسلة من الاخطار

ويمكن تعريف نوع المخاطر بمقدار احتمال اختراق خصوصية نظام المعلومات وامكانية وفاء نظام المعلومات بمهامه عند الحاجة اليه وسلامة بياناته . ومن هذا المنطق فإن عملية تقييم المخاطر تبدا بتحديد مكونات نظام المعلومات وتحديد الانظمة التي تتعامل مع نظام المعلومات وتنتهي بتحديد وتقييم وسائل الضبط والامان المتوقع اعتمادها . وهذه الاجراءات والادوات تهدف الى استبعاد احتمال وقوع الخطر وتهدف كذلك الى سرعة اكتشافه وتقليل اثره او تحويل مجرى الخطر الى مكان اخر . ويمكن العناية بذلك من خلال (3) :

1. **تحديد وسائل الامان المستخدمة في تقليل المخاطر .**
2. **تحديد وتقييم وسائل الامان الجديدة او الاضافية خلال عمليات تحليل المخاطر .**
3. **ترتيب المخاطر حسب درجة الخطورة وتحديد وسائل الامان المعتمدة والتي تؤدي الى وقاية نظام المعلومات بدرجة مقبولة .**

تتوفر مجموعة من السبل والبرامج التي تهدف الى حماية نظام المعلومات من الانتهاك. ويعتمد اختيار البرامج على مجموعة من الاسس منها :

1. **تكلفة برنامج الامان مقارنة بالفوائد الناجمة عن تقليل اثر الخطر .**
2. **مستوى المخاطر الذي يمكن لنظام المعلومات تحمله .**
3. **تحديد مفهوم تقليل الخطر فهل يعني ازالة الخطر نهائياً، تقليل احتمال وقوعه، ام تقليل مفعوله السلبي .**

عناصر المخاطر

تنضوي تحت هذا البند مجموعة من العناصر التي تفيد في تحديد وتقدير المخاطر . ومن هذه العناصر:

1. **<u>الموارد</u> : تعتمد كثير من طرق تحليل المخاطر على تحديد وتصنيف موارد المؤسسة التي تحتاج الى برامج حماية والتي يعتقد إنها معرضة للانتهاك . ويمكن تصنيف الموارد حسب اهميتها او قيمتها الدفترية . ومن هذه الموارد ذات العلاقة بنظم المعلومات ما يلي :**
   1. **البيانات والمعلومات .**
   2. **المكونات المادية والبرمجية**
   3. **الخدمات التي تقدمها المؤسسة .**
   4. **الوثائق .**
   5. **الافراد .**

ويعتقد بوجود موارد اخرى يمكن اخذها بعين الاعتبار ومنها اساليب الاحتفاظ بموارد المؤسسة مثل المخزون والحفاظ على رغبة الزبائن في التعامل مع المؤسسة وسمعة المؤسسة .

2. **<u>مصادر الخطر</u> : وهناك عدد كبير من الاخطار التي تؤثر على مسيرة المؤسسة ومنها :**
   1. **الاخطاء .**
   2. **التخريب المتعمد .**
   3. **الاحتيال والتزوير .**
   4. **السرقات .**
   5. **الخلل في المعدات والبرامجيات .**

يقدر احتمال انتهاك الموارد من خلال حساب عدد تكرارات وقوع الانتهاك ضمن فترة زمنية محددة أو من خلال التقديرات التي تعتمدها ادارة المؤسسة .

3. **<u>نقاط الضعف</u> : أن تحليل مصادر الخطر تفيد في تحديد مجموعة نقاط ضعف ومنها :**
   1. **ضعف في التدريب .**
   2. **ضعف في اجراءات الحماية والامان .**
   3. **اختيار كلمات سر غير مجربة .**
   4. **اعتماد تقنية غير مجربة .**
   5. **البث عبرخطوط غير محمية .**

4. **الاضرار : قد يسبب الانتهاك خسائر متفاوتة في موارد المؤسسة وقد تتعرض بعضها او كلها الى اضرار ومنها :**

1. **فقدان الاموال بصورة مباشرة او غير مباشرة .**
2. **انتهاك القوانين .**
3. **فقدان الرغبة والسمعة .**
4. **تعريض حياة الموظفين والزبائن الى الخطر .**
5. **ضياع الفرص الاستثمارية وانعدام الثقة .**
6. **انخفاض درجة كفاءة واداء موارد المؤسسة .**
7. **توقف النشاط التجاري بصورة مؤقتة او دائمة .**

ويمكن تعريف نقاط الضعف بانها مقدار الفترة الزمنية التي خلالها يحتمل وقوع الانتهاك. وقد يكون الوقت المتيسر امام عملية الانتهاك ضئيلاً نسبياً . وقد يبقى مفتوحاً لفترة لاتتجاوز ثوان او دقائق معدودة، او فترة زمنية قد تطول لساعة او اكثر او لعدة مرات يوميا ، او يبقى مفتوحاً على مدار اليوم .

ونقاط الضعف هذه تساعد من تسول له نفسه ارتكاب الانتهاك ثم الاستمرار في الانتهاكات كلما سنحت الفرصة او تبين ان نقطة الضعف مواتية . وفي الحوادث البسيطة قد لايتخدم سوى منفذ واحد ولمرة واحدة، وفي الحوادث المعقدة تستخدم منافذ عديدة وبصورة متكررة على مدى فترة زمنية طويلة . ويبين الجدول (1) ادناه مصفوفة المخاطر .

جدول (1) : مصفوفة المخاطر

المخاطر		السرقة	التزوير	المصادرة	الحريق	العواصف	الانفجارات	التقدير الكلي
المصادر	القيمة							
النقد	600	0.01د	.005 خ	.006 خ		.009 خ	.0008 د	14,88
الخزين	1000	0.01 خ		.006 خ	.005 خ	.009 خ	.0008 خ	30,8
المنشات	5000	خ	.005 خ	.006 د		.009 خ	.0008 د	104
المباني	8000	0.01خ	.005 خ	.006 خ	.005 خ	.009 خ	.0008 خ	107,4
البيانات	4000	خ	.005 خ		.005 خ	.009 د	.0008 خ	79,2
المنتسبين	1000				.005 خ	.009 خ	.0008 خ	14,8
الانظمة	800	0.01 د	.005 خ	.006 خ	.005 خ	.009 خ	.0008 خ	28,64
الرغبة في العمل	700				.005 د	.009 خ	.0008 د	10,36
	16100	54	67	44,4	47,5	144,9	12,88	390,08

ثانياً : الوسائل التقنية في اتخاذ القرار

تعد عملية مراجعة نظم المعلومات وضبطها من المهام المعقدة والتي تتطلب معرفة شاملة بأسس المراجعة لأنظمة المعلومات واسس التدقيق وادوات الضبط والمراقبة على نظم المعلومات من اجل:

1. **متابعة الانعكاسات السلبية نتيجة فقدان الموجودات المتعلقة بالبيانات .**
2. **معرفة اسلوب التخصيص للموارد بسبب اتخاذ قرار غير سليم .**
3. **معرفة احتمال اختراق نظام المعلومات .**
4. **معرفة التكاليف الباهظة لمكونات نظام المعلومات من مكونات مادية وبرمجية وأيدي عاملة .**
5. **معرفة التكاليف الباهظة بسبب الاخطاء الناجمة عن استخدام نظام المعلومات .**
6. **معرفة مقدار الحاجة الى صيانة الخصوصية الفردية للزبائن والمنتسبين .**
7. **معرفة مقدار الإلمام في التقدم المستمر في مجال تقنية المعلومات .**

ومن التدقيق بصورة أكثر كفاءة في سلامة نظم المعلومات فإن الواجب يحتم إيجاد مجموعة من الادوات والوسائل المساندة في تصويب القرار . ومن هذه الوسائل ما يلي :

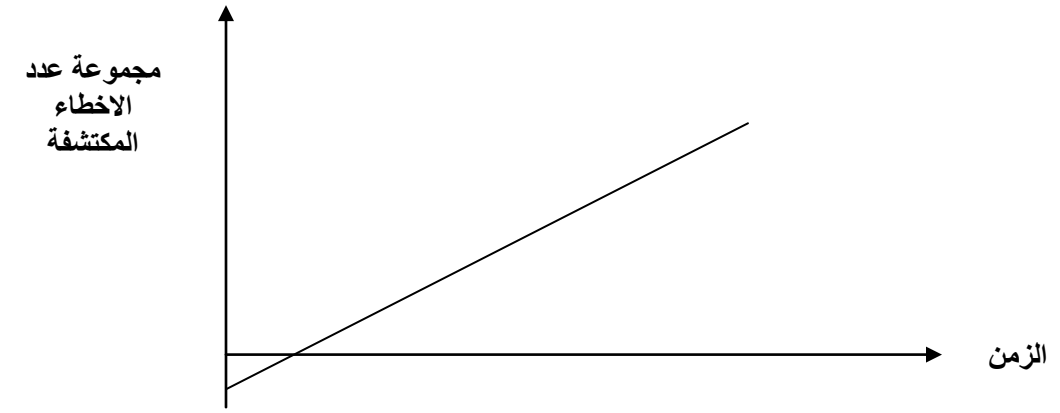
مصفوفة الرقابة

وتعد هذه الوسيلة من اقدم الوسائل المستخدمة في مساعدة مراجعي نظم المعلومات ويمكن تنظيمها بأشكال مختلفة . ويمكن تنظيم المصفوفة على شكل جداول أعمدتها تمثل أسباب الانتهاك وصفوفها تمثل ادوات الضبط والرقابة المستخدمة لتقليل اثر الانتهاك او تقدير احتمال وقوعه بالمقام الاول .

ومن اجل تقييم القرارللمعلومات التي تتضمنها المصفوفة فيصار الى تفحص اعمدة المصفوفة وتحديد مقدار احتمال تقليل الخطر لكل وسيلة أمان ولكل عنصر من العناصر التي تؤدي الى الانتهاك وحساب المستوى المتوقع من الخسارة الناجمة عن الانتهاك وتقدير المستوى الذي يبقى مرشحاً للانتهاك ومدى قبول ذلك من قبل الادارة في المؤسسة وحساب التكلفة المتوقعة ومقانتها بتكاليف وسائل الرقابة والامان المعتمدة .

نماذج قياس متانة وقوة البرمجيات

من اجل قياس قوة البرامجيات وتمكنها من اداء وظائفها بصورة صحيحة فان هناك مجموعة من الاساليب الاحصائية التي تستخدم لتقدير مقدار القصور الذي يمكن ان يقع ضمن فترة زمنية استناداً الى التصور السابق عن مقدار القصور في نظام البرامجيات . ويعتمد مفهوم البرامجيات على مجموعة معطيات منها الاخطاء (القصور) المتراكمة خلال فترة زمنية وكما في الشكل (2) :



شكل (2) : الاخطاء ونمطها العام في البرامجيات

ومن الطبيعي ان عدد الاخطاء غير المكتشفة في بداية استخدام نظام البرامجيات يكون اكبر من عددها في فترات زمنية لاحقة بسبب التحديث والتعديل المستمرين، أي ان النظام يصل الى نوع الاستقرار، ومن هنا يمكن الحصول على معادلة رياضية تربط احتمالات وقوع الاخطاء على عمر النظام ومن الجدير بالذكر ان قوة البرامجيات ومتانتها تندرج تحت ثلاث مسميات :

1. **الفترة الزمنية بين العطلات : ويعتمد هذا المفهوم على اساس ان الفترة الزمنية بين عطل واخر تكون اطول في المرات الاحقة لأنه الاخطاء يتم تصحيحها أولاً بأول . ويمكن قياس الفترة الزمنية بين عطل واخر بأعتماد التوزيعات الاحصائية لذلك .**
2. **عدد مرات العطل : ويعتمد هذا المفهوم على حساب عدد مرات العطل الذي يقع ضمن فترة زمنية محددة . وبعد تصحيح الاخطاء فإن عددها المتوقع في الفترة اللاحقة سيكون اقل مما سبق .**
3. **الاخطاء العارضة والمتأصلة : تحسب نسبة الخطاء العارضة الى نسبة الاخطاء التأصلة في نظام المعلومات من اجل ايجاد معادلة رياضية لحساب الاخطاء من كلا النوعين للفترات الزمنية المقبلة .**

تعد طرق حساب قوة ومتانة البرامجيات من الادوات الاساسية التي يستخدمها المدققون في حساب درجة صلاحية نظام البرامجيات. ويعتمد تقدير دقة عدد الاخطاء المتبقية على كمية البيانات والمعلومات المتاحة عن نظام البرامجيات المستخدم .

ثالثاً : دور المراجعون والمدققون

ان اي نظام للمعلومات يجب ان يحتوي على مجموعة من ادوات الرقابة وادوات الامان التي تساعد في منع الخلل او اكتشاف حال او قبل وقوعه . ان المدققين لايعتمدون على تقدير قوة الضوابط وضعفها وانما على قوة النموذج الرياضي المستخدم وقوة مقدرته على تحديد الاخطاء وبيان الوقت المتوقع لحدوثها من اجل اتخاذ الاحتياطات اللازمة . وقد يستخدم المدققون النماذج الرياضية كأدوات تحليلية لمعرفة مقدار الاخطاء . فإن كان عدد الاخطاء المتوقعة كبيراً فيستوجب الامر اختبار النظام بصورة شاملة ومتكررة لإستخراج تلك الاخطاء الكامنة والمتأصلة وتصحيحها. وأما اذا تبين ان عدد الاخطاء المتوقعة قليلة فيمكن للمدقق الاعتماد على الضوابط الداخلية في منع او اكتشاف الخلل دون الاعتماد على اختبارات كبيرة وشاملة لأن الاختبارات الشاملة تصاحبها تكاليف باهظة قد لاتتحملها المؤسسات .

إن الرقابة الداخلية تنقسم إلى قسمين في ظل استخدام الأسلوب اليدوي لمعالجة البيانات وهما:

1- **الرقابة الإدارية**
2- **الرقابة المحاسبية**

أما في ظل استعمال تقنيات المعلومات والاتصالات داخل الوحدة الاقتصادية وتحول نظام المعلومات المحاسبي اليدوي إلى نظام معلومات محاسبي مؤتمت فان الرقابة الإدارية لا تختلف أساليبها ، إذ سيتم تنفيذ هذه الأساليب من خلال الهيكل التنظيمي للاختصاصات ولوائح الإجراءات وتوصيف الوظائف والسياسات التنظيمية في الوحدة الاقتصادية ،أما في ما يتعلق بالرقابة المحاسبية فإنها ستختلف في حالة وجود نظام معلومات محاسبي مؤتمت داخل الوحدة الاقتصادية (توماس هنكي ، 443:1998).

ووفقا لمعيار التدقيق الدولي رقم 1008/الفقرة الخامسة منه والمعنون بـ (تقدير المخاطر والرقابة الداخلية خواص واعتبارات نظم المعلومات المحوسبة) فان الرقابة الداخلية تنقسم الى :

أ- الرقابة العامة *General Control*

ب- الرقابة التطبيقية *Application Control*

وهناك عدد من الباحثين من يضيف نوعاً ثالثاً من أساليب الرقابة الداخلية هو رقابة المستخدم، وقد ورد في المعيار الدولي للتدقيق رقم (315) المعاد صياغته والنافذ المفعول في 2008/12/15 في الفقرة (أ91) الى ان استعمال تقنيات المعلومات يؤثر على طريقة تنفيذ أنشطة الرقابة ، ومن منظور مراقب الحسابات تكون الرقابة على أنظمة تقنية المعلومات فعالة عندما تحافظ على نزاهة المعلومات وامن البيانات التي تعالجها هذه الأنظمة وتشمل الرقابة نوعين : رقابة عامة على تقنيات المعلومات ورقابة على التطبيقات (الاتحاد الدولي للمحاسبين ،2007: 1170) .

أ- الرقابة العامة *General Control*

وتشمل الرقابة العامة عموم الأنشطة الخاصة بنظام المعلومات المؤتمت، وهي عبارة عن مظلة على كل نظم المعلومات داخل الوحدة الاقتصادية وهي تهدف للتأكد من كل مما يأتي: (Laudon & Laudon/1998/466)

وتتضمن الرقابة العامة الرقابة الإدارية والتنظيمية، وتطوير النظم ورقابة الصيانة ورقابة تشغيل الحاسوب ورقابة برامج النظم (ديوان الرقابة المالية المغربي ،2007 : 20)

وتهتم الرقابة العامة بحماية النظام ككل وهي تضم عدة أنواع من الرقابات منها: (Turban et.al/1999/668) إذ تتضمن الرقابة على الأجهزة المادية عملية حماية هذه الأجهزة وملحقاتها ومركز البيانات والبرامج، أما رقابة الوصول فيقصد بها رقابة لمنع وصول أشخاص غير مصرح لهم بالدخول واستخدام النظام إذ من الضروري أن يكون الدخول للأشخاص مخولين رسميا ومصرح لهم ويكون الوصول على ثلاثة أنواع:- (وصول إلى الأجهزة المادية وملحقاتها، وصول الى البيانات والبرامج والعمليات، وصول إلى النظام ككل)

ومن ابرز أساليب الرقابة العامة ما يأتي : (توماس هنكي ،1989 : 446) (لطفي ، 2005 : 60)

1- أسلوب الرقابة التنظيمية
2- إجراءات توثيق واختبار واعتماد النظم وأي تعديلات عليها
3- أسلوب الرقابة على الأجهزة وملحقاتها
4- أسلوب رقابة إمكانية التوصل إلى النظام

ب- الرقابة التطبيقية *Application Control* :

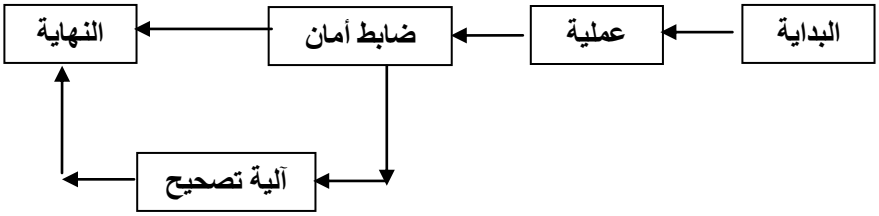
تهتم الرقابة العامة بحماية وامن الأجهزة المادية والبرامج والبيانات والملفات والاتصالات ولكنها لا تحمي محتويات التطبيقات الخاصة ، لذا وجدت الرقابة التطبيقية لحماية التطبيقات التي هي جزء من البرامج، ووفقا لمعيار التدقيق الدولي 315 المعاد صياغته في الفقرة أ93 إن عناصر الرقابة التطبيقية تطبق على معالجة التطبيقات المفردة ، وهي مصممة لضمان نزاهة السجلات المحاسبية فهي تتعلق بالإجراءات المستخدمة لإدخال وتسجيل ومعالجة وإعداد التقارير حول المعاملات أو البيانات المالية الأخرى ، وهي بذلك تقسم إلى ثلاث أنواع رئيسة وهي: (ديوان الرقابة السعودي،2007: 23)،(Laudon & Laudon . 1998 : 468)

1- الرقابة على المدخلات :
   أ- الرقابه على المدخلات المعتمدة على المستندات
   ب- الرقابة على المدخلات من دون مستندات
2- الرقابة على العمليات
3- الرقابة على المخرجات

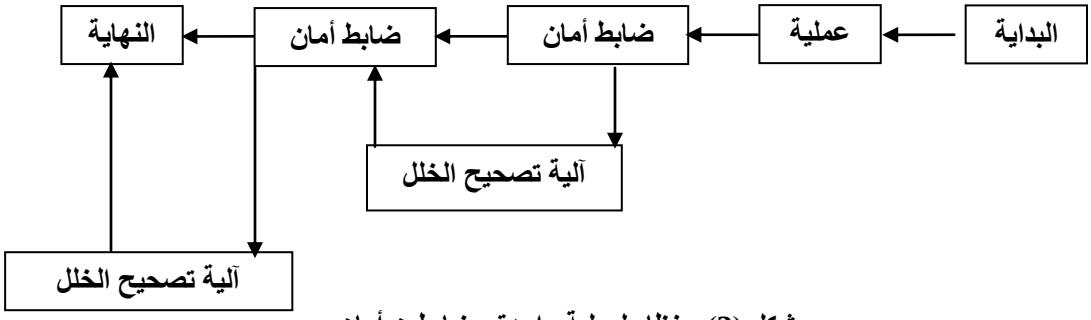
رابعاً : النماذج الهندسية لقياس المتانة

تعتمد هذه النماذج في حساب متانة النظام على اساس متانة وقوة الوحدات المكونة للنظام بصورة انفرادية ودرجة قوة الضوابط الداخلية لكل وحدة من مكونات النظام . ومن هذا المنطلق فإن المدقق سيحصل على صورة عن قوة ومتانة نظام الضوابط المستخدم وبذلك يتمكن المدقق من الحصول على صورة واضحة من اجل تقييم نظام الضوابط المعتمدة .

ومن اجل توضيح هذا النوع من النماذج تفترض وجود نظام معلومات بسيط يتكون من عملية حسابية واحدة وضابط امان واحد والية تصحيح اخطاء واحدة. ونفترض تواجد نوع واحد من انواع الانتهاك او الخلل وكما يبين ذلك الشكل (3) .



نظام لعملية واحدة وضابط أمان واحد



شكل (3) : نظام لعملية واحدة وضابطين أمان

تحسب قوة ومتانة النظام وذلك بحساب احتمال عدم ظهور خلل بعد إكمال تنفيذ نظام المعلومات وعل النحو :

$$R = p + (1-p) \times P(e) \times P(c)$$

حيث :

R : قوة ومتانة النظام

p : احتمال ان العملية تنفذ بصورة صحيحة بدون خلل

$P(e)$: احتمال اكتشاف الخلل إن كان موجوداً بواسطة ضابط الأمان

$P(c)$: احتمال تصحيح الخلل بواسطة ضابط الأمان ان كان موجوداً

تشير المعادلة السابقة الى ان قوة ومتانة النظام تساوي حاصل جمع احتمال تنفيذ العملية بصورة صحيحة واحتمال عدم تنفيذها بصورة صحيحة وان ضابط الامان الموجود يمكنه اكتشاف الخلل وصيانته. ومن اجل توضيح ذلك اليك نظام حريق واطفاء، فالنظام المطلوب مراجعته هواكتشاف حريق ومحاولة اخماده. لنفترض احتمال نشوب الحريق يساوي 0.005 وهو يساوي $(p - 1)$ وان احتمال تنفيذ العملية بصورة صحيحة– دون نشوب حريق– هو p ويساوي 0.995 ونفترض احتمال اكتشاف الحريق يساوي 0.95 ويساوي $P(e)$. ونفترض احتمال صلاحية نظام الاطفاء واداء مهمته بصورة صحيحة يساوي $P(c)$ ويساوي 0.9 . لذا فإن فعالية النظام تحسب على النحو:

$$R = 0.995 + (0.005) \times (0.95) \times (0.9)$$
$$= 0.999275$$
$$(1-R) = 0.000725$$
$$(R-P) = 0.004275$$

ومن الممكن تطبيق قاعدة عملية واحدة الى عدة عمليات . فالعملية رقم i يمكن حساب فعاليتها على النحو:

$$R_i = p_i + (1-p_i) \times P(e_i) \times P(c_i)$$

ويمكن حساب فعالية النظام لجميع انواع الخلل الذي يصيب نظام المعلومات على النحو :

$$R = \prod R_i$$

قد لا تكون المعادلة اعلاه ذات مغزى ذو فائدة كبيرة للمدققين، فهم يودون معرفة المغزى الاقتصادي وكمية الاخطاء المتوقعة اوالبيانات الخاطئة. فمثلا ، اذا رغب المدققون تدقيق صحة البيانات بدلالة اقتصادية او مالية فان تأثير الخطأ رقم i يمكن حسابه :

$$A_i = Ne_{ir} \times Ve_i \times T_r$$

حيث :

A_i : حجم الخطأ الناجم

Ne_{ir} : متوسط عدد الأخطاء من نوع i غير المكتشفة بعد مرور النظام بعدد من ضوابط الامان تساوي r

Ve_i : متوسط حجم الاخطاء غير المكتشفة من نوع i

T_r : عدد مرات تنفيذ r من ضوابط الامان

ويمكن حساب حجم الاخطاء الكلي المتوقع على النحو :

$$A = \sum A_i$$

وبإمكان المدقق حساب عدد البيانات الخاطئة باستخدام المعادلة :

$$H = \sum H_i$$

حيث H_i تساوي $Ne_{ir} \times T_r$ ، علماً إن كل من A و H قيم توقعية وعلى المدققين تقدير التوزيعات الاحتمالية لهما باعتبارهما دوال رياضية لكل من التوزيعات الرياضية Ve_i ، Ne_{ir} على الترتيب .

نماذج بيزيان

توفر هذه النماذج للمراجعين والمدققين طريقة اساسية لمراجعة التقديرات السابقة لفعالية الضوابط الداخلية استناداً الى المعلومات الجديدة التي يمكن تجميعها خلال عمليات المراجعة والتدقيق.

وقد اثبتت الدراسات فعالية هذه النماذج في اتخاذ القرارات سواء في الانظمة اليدوية او انظمة المعلومات الحاسوبية . فعندما يتطلب الامر من المدققين اتخاذ قرار او عدمه بخصوص صلاحية نظام الرقابة او الضوابط الداخلية ، كما في الجدول (2) .

جدول (2) : متانة الرقابة الداخلية على نظام المعلومات

	فعال	غير فعال
مقبول	قرار صائب	قرار غير صائب
مرفوض	قرار غير صائب	قرار صائب

ومن اجل بيان طبيعة أسلوب بيزيان في اتخاذ القرار فإن نظام الرقابة الداخلية كما يشير جدول (2) إما أن يكون فعالاً أو غير فعال ويتطلب الأمر من المدقق اتخاذ قرار بقبول نظام الرقابة أو رفضه .

فمن الطبيعي بدون توفر المعلومات الكافية عن نظام الرقابة، قد يصار الى اتخاذ قرار خاطىء. وقد يصاحب القرار الخاطىء تكلفة عالية ممايؤدي الى افلاس وخسارة المؤسسة .

<u>مثال</u>. يعتقد مدققون النظم في أحد نظم المعلومات ان احتمال نجاح نظام الرقابة الداخلي يساوي *0.9* وقد تم تحديد هذه الاحتمالات من الخبرة السابقة ومن كمية المعلومات المتاحة حول نظام المعلومات ونظام الرقابة الداخلي. فإذا افترضنا صلاحية نظام الرقابة الداخلي وتبين فيما بعد أنه غير دقيق فيصاحب ذلك تكلفة مقدارها مليون نتيجة دعاوى قانونية بسبب عدم كفاءة النظام وأن تكلفة الخطأ في عدم قبول نظام الرقابة الداخلي وتبين أنه فعال يساوي خمسون الفاً. ماهو القرار الذي تعتقد أكثر صواباً ؟

في غياب المعلومات الإضافية التي تساعدنا في اتخاذ القرار الصحيح فسيقوم المدقق بحساب التكلفة المتوقعة في الحالتين :

1. **في حالة الموافقة على نظام الرقابة الداخلي، فإن التكلفة المتوقعة ستكون :**

$$0.9 \times 0 + 0.1 \times 1{,}000{,}000 = 100{,}000$$

2. **في حالة عدم الموافقة على نظام الرقابة الداخلي، فإن التكلفة المتوقعة ستكون :**

$$0.9 \times 50.000 + 0.1 \times 0 = 45.000$$

وإستناداً الى النتائج اعلاه سيتم اعتماد الخيار الثاني والقاضي بعدم صلاحية نظام الرقابة الموجود .

فإذا افترضنا القيام بتحريات إضافية اخرى من أجل الحصول على معلومات أكثر وذلك بإعتماد سلسلة من الاختبارات على النظام من أجل تحديد فعاليته وبذلك سنحصل عل مجموعة من النتائج . وبما أن الاختبارات بكل حال من الاحوال لن تكون كافية لتحديد صلاحية او فعالية نظام المعلومات والضوابط المعتمدة معه فإن هذه النتائج تفيد تحديد اتجاهات المراجعين والمدققين حول فعالية النظام. ومن هنا فإن نماذج بيزيان تفيد في تقدير احتمال إن :

1. نتائج الاختبارات مناسبة إذا كن النظام فعالاً .
2. نتائج الاختبارات مناسبة ولكن النظام غير فعال .

ويمكن اعتماد مفهوم الاحتمالات المشروطة عل النحو :

Probability (favorable | reliable) = P (F|R) = 0.8
Probability (favorable | unreliable) = P (F|U) = 0.2

حيث F يمثل اتجاه القبول بكفاءة نظام الرقابة الداخلية وأن R يمثل صلاحية أو فعالية نظام الرقابة ، وإن U تمثل عدم فعالية النظام .

وبإستخدام قاعدة بيز فإن احتمال كون النظام فعالاً إذا كانت نتائج الاختبار مناسبة وكون النظام غير فعالاً إذا كانت نتائج الاختبار غير مناسبة على النحو :

$$P(R \mid F) = \frac{P(F \mid R)P(R)}{P(F)}$$

$$= \frac{P(F \mid R)P(R)}{P(F \mid R)P(R) + P(F \mid U)P(U)}$$

$$= \frac{(0.8)(0.9)}{(0.8)(0.9) + (0.2)(0.1)}$$

$$= 0.97$$

$$P(U|F) = 1 - 0.97$$

$$= 0.03$$

وفي ضوء النتائج الجديدة، فإن التكاليف المتوقعة في حالة القبول والرفض وعلى النحو:

1. في حالة القبول كون نظام الضوابط فعالاً فإن التكاليف المتوقعة تساوي :

$$0.97 \times 0 + 0.03 \times 1{,}000{,}000 = 30{,}000$$

2. في حالة الرفض كون نظام الضوابط فعالاً فإن التكاليف المتوقعة تساوي :

$$0.97 \times 50{,}000 + 0.03 \times 0 = 48{,}000$$

القرار : نظام الضوابط فعالاً ويجب اعتماده وهذا يختلف عن القرار السابق الذي تم اعتماده .

نماذج المحاكاة

عندما يصعب اتخاذ قرار بإستخدام النماذج السابقة بسبب كثرة التغيرات أو عدم الحصول على بيانات كافية فإن نماذج المحاكاة تكون الأنسب للمراجعين والمدققين فمثلاً يقوم الحاسب بمحاكاة نظام المعلومات لمعرفة احتمال اختراق ضوابطه او احتمال فشل نظام المراقبة لإكتشاف المخترق او احتمان أن المخترق يتمكن من إستخراج شفرات النظام إن كان مشفراً أو التوصل الى كلمة السر او احتمال اختراق النظام في نهاية المطاف لسرقة بيانات حساسة جداً.

وكذلك اختبار نظام المعلومات وذلك بتحديد سلسلة من المدخلات وتجزئتها الى اجزاء وادخال سلسلة من كل جزء ومعرفة نتائج النظام ومقارنتها بالنتائج المتوقعة ذاتياً.

وتفيد المحاكاة المدققين والمراجعين في تنظيم نتائج المدخلات على شكل توزيع يمكن منه إستخراج مجموعة من المقاييس الإحصائية كالمتوسط الحسابي والانحراف المعياري ودرجات الحرية ودرجة الثقة بالنتائج. وهذه التوزيعات والمقاييس الإحصائية المصاحبة لها بمثابة خلاصة حسابية لقياس فعالية النظام وقوة بنائه.

ومن خلال التوزيع الإحصائي يمكن قياس كثير من خصائص نظام المعلومات، فعلى سبيل المثال، يمكن معرفة الخلل في نظام المعلومات من خلال التوزيع الإحصائي الذي يمثل الخلل. فمن نتائج النظام في وحدة المعالجة المركزية للحاسب لمدة ألف ساعة تحصل على نموذج توزيع بواسون اللوغاتمي والذي يعتمد الشكل التالي :

$$f(t) = (1/p)\ln(l_0 pt + 1)$$

حيث :

دالة الخلل التجميعي المتوقع خلال فترة التنفيذ ***f(t):***

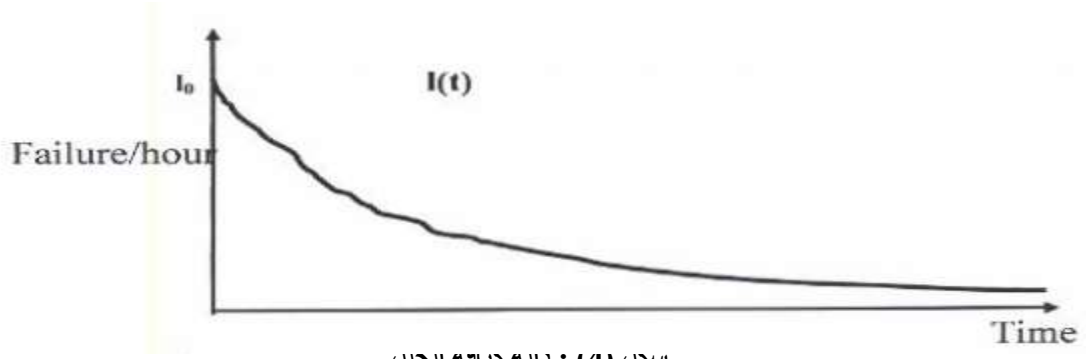
كثافة الخلل في بداية اختبار نظام المعلومات (مقدار الخلل خلال ساعة) ***l_0 :***

نسبة اكتشاف الاخطاء وتصحيحها ***p :***

ويمكن حساب نسبة الاخطاء عند أي فترة زمنية ***l(t)*** **من خلال حساب مشتقة الدالة** ***f(t)*** **وعلى النحو :**

$$l(t) = l_0 / (l_0 pt + 1)$$

وشكل منحني الخلل سيكون بالصورة في الشكل (4)



شكل (4) : دالة كثافة الخلل

ومن هنا يستطيع المرجع والمدقق قياس مقدار الخلل لأي نظام من أنظمة المعلومات والحصول على صورة عن فعالية ومتانة النظام (1).

خامساً : الأنظمة الخبيرة

عبارة عن برامج تجمع الخبرة البشرية في نطاق تخصص معين والإستفاذة من تلك الخبرة في ايجاد الحلول للمشاكل التي تظهر في ذلك المجال او التخصص. لأهمية الأنظمة الخبيرة فقد انفقت كثير من شركات التدقيق والمراجعة أموال كثيرة على تطوير نظم الخبرة من اجل تسهيل عملية المراجعة والتدقيق. وقد اثبتت هذه البرامج فعاليتها واعتمادها الكثير من المدققين والمراجعين في تجميع الحقائق وتحليلها.

1. أسباب اعتماد الأنظمة الخبيرة في المراجعة والتدقيق .

يقوم المدققون والمراجعون ببناء وإدامة واستخدام نظم الخبرة لعدة اسباب منها :

أ- يقدم النظام الخبير خلاصة الممارسات التي يتمتع بها خيرة اختصاصيو التدقيق والمراجعة مع النظريات والممارسات المتعارف عليها. إن تجميع خبرة وممارسات اختصاصيو التدقيق وصياغتها في قالب واحد يمكن نقل الخبرة الى بقية العاملين في مجال التدقيق والمراجعة .

ب- وبسبب التطور السريع في تكنولوجيا المعلومات فإنه يصعب على كثير من المدققين والمراجعين مواكبة تلك التطورات مما يستدعي تحديد عدد معين من المراجعين في متابعة التكنولوجيا ونقل تلك الخبرة الى النظام الخبير وجعلها في متناول أيدي بقية المراجعين والمدققين .

ج- يقدم النظام الخبير وسيلة فعالة في ايجاد قاعدة مشتركة وتطابق في التقييم وفي طريقة اتخاذ القرار. إن النظام الخبير يساعد المدققين والمراجعين في إتباع سلسلة من الخطوات المساعدة في توعية المدققين والمراجعين بأهمية المعلومات المتوفرة والتي تؤثر في اتخاذ القرار وإصدار الأحكام، وتوجيههم في حالة القرارات المتناقضة وتحديد عدة حلول وإختيار الأفضل منها والإحتفاظ بالقرارات المناسبة للإستفادة منها مستقبلاً.

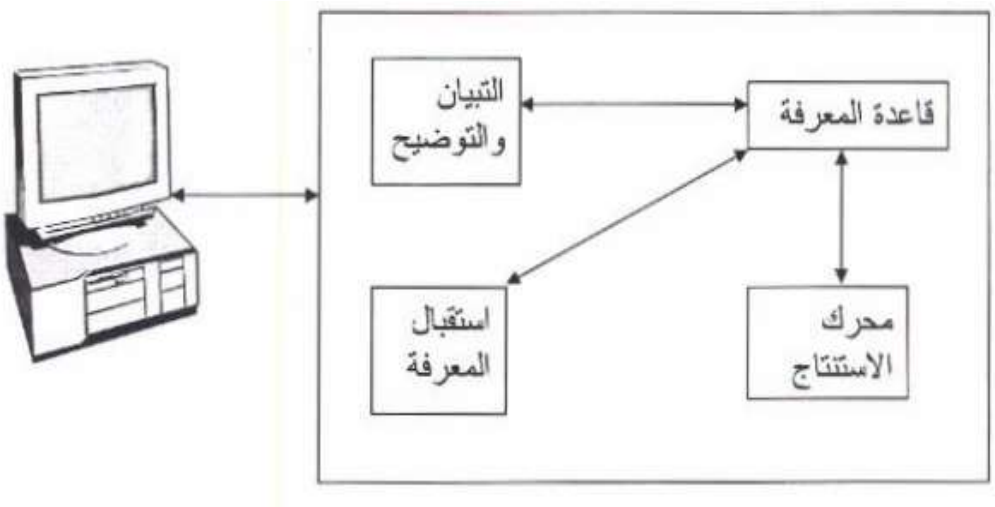
وفي ضوء ماتقدم فإن الأنظمة الخبيرة تؤثر بصورة ايجابية على كفاءة وفعالية عمليات التدقيق. وتشير الابحاث إن التقدم في مجال تقوية فعالية نظم المعلومات سيستمر بصورة متتابعة (2) .

2. مكونات النظام الخبير : يتكون النظام الخبير من مقطعين رئيسين هما :

أ- قاعدة المعرفة ***Knowledge – base*** : وهي عبارة عن هيكل لتجميع الخبرات من ذويها وتخزينها في القاعدة وتكون المعلومات على شكل حقائق وقوانين يستخدمها الخبير من إستخراج حلول المشاكل المتعلقة في قضايا المراجعة والتدقيق.

ب- محرك الإستنتاج ***Inference engine*** : وهو عبارة عن برنامج يعتمد على علم المنطق ويستخدم قاعدة المرفة لإستخراج علاقات بين الحقائق والقوانين من أجل الوصول إلى استنتاج حول المسائل المطلوب إيجاد حلاً لها .

الشكل (5) يبين العلاقة بين مكونات النظام الخبير .



شكل (5) : المكونات الأساسية في النظام الخبير

وكما يشير الشكل (5) أعلاه فهناك مقطعين أخريين هما :

أ- وسائل التبيان والتوضيح: والتي تقوم بعرض المعلومات الى المستخدم مبينة طريقة العرض واسلوب الوصول الى النتائج .

ب- إستقبال المعرفة: وهو عبارة عن برنامج يستقبل الخبرة وإسداء النصح في مجالات التخصص المختلفة من خلال آراء الخبراء ويضيفها الى قاعدة المعرفة.

ومن أجل بيان الطريقة التي يتعامل فيها النظام الخبير مع المراجعين والمدققين من أجل تسهيل مهماتهم فنورد بعض قواعد المعرفة المتعلقة بالمدينين *Account Receivable* .

1. **إن كانت الرقابة غير مبرمجة المدخلات . فإن تعديلات مزورة قد تقع على وصولات الإستلام .**
2. **إن كانت الرقابة مبرمجة على المدخلات وإن الرقابة لم يتم تطبيقها. فإن تعديلات مزورة قد تقع على وصولات الإستلام .**
3. **إن كانت الرقابة مبرمجة على المدخلات وإن الرقابة قيد التطبيق وإن المدخلات لم تدون.**
4. **إذا أمكن تزوير او تعديل في وصولات الإستلام النقدي وكانت عمليات الايداع والسحب غير مراقبة بصورة مستقلة فإن التزوير قد يقع على حسابات مدين.**
5. **إن وقع التزوير على حساب المدينين فسيصاحب ذلك التصريح ديون غير قانونية .**
6. **إذا لم يصاحب اصدار أذونات الدين نظام رقابة مناسب فإن ذلك يعني التصريح بديون غير قانونية.**

يمكن تخزين القواعد اعلاه في قاعدة المعرفة واستخدامها في الوصول الى إستنتاج حول مسألة معينة. وقد لايقتصر الأمر على قواعد المعرفة وإنما تخزين حالات سابقة وحلولها ومن مقارنة الحالات الجديدة بها واستخلاص النتائج.

أنواع برامج التدقيق الخبيرة

تنحصر معظم برامج التدقيق الخبيرة في مجالات اربع وعل النحو:

1. **تحليل المخاطر: يقوم النظام الخبير بتقييم الانتهاك المادي على جميع عناصر نظام المعلومات التي يمكن أن يقع عليها الانتهاك .**
2. **تقييم الضوابط الداخلية: يجب النظام الخبير درجة صلاحية وحدات الرقابة الداخلية ومنها يتم تقدير تعرض الموارد الى انتهاك .**
3. **تخطيط عمليات التدقيق: يقدم النظام الخبير مجموعة من الخطوات الواجب اتباعها في تنفيذ عمليات التدقيق ويقدم تقريراً عن فعالية الضوابط الداخلية .**
4. **إستشارات فنية: يقدم مجموعة من النصائح ذات الطابع الفني والتي يمكن أن تواجه المدققون خلال عمليات التدقيق مثل تحديد فيما إذا كانت القوائم المالية تشيع القواعد العامة المتبعة .**

الإعتبارات الإقتصادية والمادية

من الممكن إيجاد نظام معلومات فعال وذو صلاحية عالية ولكن لقاء تكاليف باهظة. ومن هنا يجب قياس المنافع والتكاليف وفي ضوء ذلك اتخاذ القرار. ومن المنافع والتكاليف المصاحبة لإعتماد الضوابط ما يلي :

- **تكاليف اولية تنجم عن تصميم وتنفيذ نظام الرقابة الداخلي .**
- **تكاليف تصاحب تنفيذ أنظمة الرقابة الداخلية .**
- **تكاليف عملية تحديد الخلل عندما تكتشف نظم الرقابة وجود خلل . وكذلك يصاحب ذلك تكاليف تصحيح الخلل وإعادة نظام المعلومات إلى وضعه الطبيعي .**
- **التكاليف التي تنتج عن عدم تمكن نظام الرقابة من إكتشاف الخلل بالرغم من وجوده وكذلك التكاليف الناجمة عن إكتشاف الخلل لكن لم يتمكن نظام الرقابة من تصويبه بالصورة الصحيحة.**
- **تكاليف الناجمة عن ديمومة صيانة نظام الرقابة الداخلي.**

ومما تجدر الإشارة إليه، إن حساب الموازنة بين التكاليف والفوائد الناجمة عن إعتماد نظام الرقابة قد لا يكون أمراً سهلاً لوجود متغيرات كثيرة وقد يكون الخلل متعدد الوجوه .

سادساً : الخلاصة

تطرقنا في هذا البحث عن الأدوات والوسائل التي يمكن إعتمادها من أجل ضمان صلاحية نظام المعلومات التي أصبحت حياة الناس تعتمد عليه بصورة كبيرة . وقدم البحث تصوراً شاملاً عن المخاطر وأنواعها وطرق معالجتها والفترات الزمنية التي تستغرقها . كذلك بين البحث أنواع الخلل الذي يمكن أن يقع على نظم المعلومات واثر ذلك على موارد المؤسسة التي وقع عليها الانتهاك .

وشمل البحث في عرضه مجموعة من الأدوات التي تساعد المدققين والمراجعين في أداء درهم الريادي في تحديد الخلل والتمكن من اصدياده قبل وقوعه. ومن هذه الأدوات اتي تضمنها البحث هي مصفوفة المخاطر، والأنظمة الخبيرة، وأساليب المحاكاة ونظرية بيز في حساب الاحتمالات المشروطة .

ويوصي البحث القائمين على عمليات صناعة البرامجيات بصياغة نظم رقابة وأمان وإيجاد الضوابط المناسبة لضمان سلامة نظم المعلومات وإعتماد المراجعين والمدققين ذوي المهارات الخاصة في نظم المعلومات من أجل التأكد من صلاحية أنظمة الرقابة الداخلية وإن إعدادها وتصميمها وتنفيذها قد خضع لشروط القياس العالمية .

المصادر

1- توماس، وليم وهنكي، امرسون، المراجعة بين النظرية والتطبيق، تعريب ومراجعة: د. احمد حامد حجاج ود. كمال الدين سعيد، تقديم: د. سلطان المحمد العلي السلطان، دار المريخ للنشر، الرياض، م. ع. س. 1996.

2- الاتحاد الدولي للمحاسبين، "إصدارات المعايير الدولية لممارسة اعمال التدقيق والتأكيد وقواعد أخلاقيات المهنة، ترجمة المجمع العربي للمحاسبين القانونيين، 2008.

3- لطفي، امين السيد احمد (مراجعة وتدقيق نظم المعلومات) الدار الجامعية، الإسكندرية،2005.

3- ديوان المحاسبة السعودي (تقويم نظم الرقابة الداخلية في الجهات الخاضعة للرقابة)، بحث مقدم للمشاركة في اجتماع الجمعية العمومية للمجموعة العربية للأجهزة العليا للرقابة المالية والمحاسبة، بيروت، 1995 .

4- ورقة بحثية مقدمة من (ديوان المحاسبة القطري، السعودي، المغربي، الكويتي) بعنوان (تطوير معايير الرقابة في ضوء نظم المعلومات الالكترونية) بحوث مقدمة في اجتماع الجمعية العمومية للمجموعة العربية للأجهزة العليا للرقابة المالية والمحاسبية، دار صفاء للطباعة والنشر ،2007 .

5. R. S. pressman, *"Software Engineering: A practitioner' approach"*, McGraw Hill, fifth edition 2001.
6. Baldwin-Morgan, Amelia Anette, *"The Impact of Expert Systems Audit Tools and Auditing Firm in the year 2001: A Delphi Investigation"*, Journal of Information Systems (Spring), pp. 16-34, 1993.
7. ISACA, *www.isaca.org,"Standards, Guidelines and Procedures"*, Information Systems Audit and Control Association, 2006.
8. Turban, etall., *"Information Technology for Management "*, 2nd ed., (1999)
9. Laudon ,Keneth c.&Ludon ,Janp.,*"Information System &Internet"*,4th ed.,(1998)