اللقاء العلمي حول موضوع

"الطرق الحديثة للرقابة على الأنظمة المعلوماتية"

خلال الفترة من 7 إلى 11 يوليو 2024

مكان انعقاد اللقاء:

جمهورية مصر العربية – القاهرة – الجهاز المركزي للمحاسبات

تقديم :

يعقد اللقاء العلمي حول موضوع " الطرق الحديثة للرقابة على الأنظمة المعلوماتية " خلال الفترة من 7 إلى 11 يوليو 2024 .

ويسر الجهاز المركزي للمحاسبات أن يضع بين أيدي الأخوة المهتمين باللقاء والمشاركين والأجهزة العليا للرقابة المالية والمحاسبة الأعضاء بالمنظمة العربية هذا الدليل الذي يتناول الجوانب الإدارية والفنية والتنظيمية للقاء والمعلومات التي تهم كل من يشارك فيه.

أهداف اللقاء:

- **تمكين المشاركين من فهم المعايير المهنية والممارسات الدولية على الأنظمة المعلوماتية .**
- **اكتشاف المخاطر الإلكترونية.**
- **الاطلاع على الطرق الحديثة للرقابة عل الأنظمة المعلوماتية.**
- **التحديات والحلول**
- **استخلاص توصيات وذلك لاستفادة الأجهزة المشاركة منها .**

العناصر التفصيلية للقاء:

- **مراحل عملية المراجعة.**
- **إجراءات مراجعة نظم المعلومات مع حالات عملية.**
- **حوكمة نظم المعلومات مع حالات عملية.**
- **المخاطر التي تواجه الجهات الخاضعة للتدقيق مع حالات عملية.**
- **استخدام تحليل البيانات في مراجعة نظم المعلومات مع حالات عملية.**
- **خطة استمرارية العمل وخطة استعادة الأوضاع بعد الكوارث مع حالات عملية.**
- **إصدار توصيات للقاء العلمي لعرضها على الأجهزة المشاركة.**

مدير اللقاء:

م	مدير اللقاء	الصفة والمؤهلات والخبرات السابقة
1	محاسب/ وائل مروان البكري	مستشار الإدارة المركزية لنظم المعلومات والتحول الرقمي.

الطاقم التدريبي:

م	المدربين	الصفة والمؤهلات والخبرات السابقة
1	**محاسب/ أشرف جلال أمين عمر**	• وكيل وزارة بالجهاز المركزي للمحاسبات – بكالوريوس تجارة شعبة محاسبة • دبلوم دراسات عليا للحاسبات الآلية . • حاصل على شهادة مراجع نظم معلومات معتمد (CISA). • مدرب معتمد وفقًا لمنهجية مبادرة الإنتوساي للتنمية (IDI).
2	**محاسب/ مصطفى معروف عبد الحليم**	• رئيس مجموعة مراجعة بالجهاز المركزي للمحاسبات – بكالوريوس تجارة شعبة محاسبة • عضو جمعية المحاسبين والمراجعين المصرية. • حاصل على شهادة مراجع نظم معلومات معتمد (CISA). • حاصل علي شهادة مراجع داخلي معتمد (CIA). • حاصل علي شهادة فاحص احتيال معتمد (CFE). • حاصل على شهادة في معايير المحاسبة الدولية للقطاع العام (IPSAS) • مدرب معتمد وفقًا لمنهجية مبادرة الإنتوساي للتنمية (IDI).

البرنامج الزمني للقاء العلمي حول "الطرق الحديثة للرقابة على الأنظمة المعلوماتية"
خلال الفترة من 7 إلى 11 يوليو 2024

اليوم	التاريخ	المحاضرة الأولى	المحاضرة الثانية
		11.30 : 9.30	2.30 : 12.30
الأحد	2024/7/7	التسجيل – افتتاح اللقاء صورة تذكارية	مراحل عملية المراجعة
	المحاضر	وائل البكري	مصطفى معروف
الاثنين	2024/7/8	إجراءات مراجعة نظم المعلومات مع حالات عملية	المخاطر التي تواجه الجهة الخاضعة للتدقيق
	المحاضر	أشرف جلال	مصطفى معروف
الثلاثاء	2024/7/9	حوكمة نظم المعلومات	استخدام تحليل البيانات في مراجعة نظم المعلومات
	المحاضر	أشرف جلال	مصطفى معروف
الأربعاء	2024/7/10	خطة استمرارية العمل وخطة استعادة الأوضاع بعد الكوارث	تجارب المشاركين
	المحاضر	أشرف جلال	مصطفى معروف
الخميس	2024/7/11	تجارب المشاركين	الاتفاق حول الصياغة النهائية للتوصيات وإبلاغها للمشاركين – تقييم اللقاء- توزيع الشهادات
	المحاضر	أشرف جلال	وائل البكري

البرنامج الزمني للقاء التدريبي حول "الطرق الحديثة للرقابة علي الأنظمة المعلوماتية "
خلال الفترة من 7 الي 11يولية 2024

اليوم	التاريخ	المحاضرة الأولى	المحاضرة الثانية
		11.30 : 9.30	2.30 : 12.30
الأحد	2024/7/7	التسجيل – افتتاح اللقاء صورة تذكارية - التقييم القبلي	مراحل عملية المراجعة
	المحاضر	وائل البكري	مصطفي معروف
الاثنين	2024/7/8	اجراءات مراجعة نظم المعلومات مع حالات عملية	المخاطر التي تواجه الجهة الخاضعة للتدقيق
	المحاضر	اشرف جلال	مصطفي معروف
الثلاثاء	2024/7/9	حوكمة نظم المعلومات	استخدام تحليل البيانات في مراجعه نظم المعلومات
	المحاضر	اشرف جلال	مصطفي معروف
الأربعاء	2024/7/10	خطة استمرارية العمل وخطة استعادة الأوضاع بعد الكوارث	تجارب المشاركين
	المحاضر	اشرف جلال	مصطفي معروف
الخميس	2024/7/11	تجارب المشاركين	التقييم البعدي – توزيع الشهادات ختام البرنامج
	المحاضر	أشرف جلال	وائل البكري

جمهورية مصر العربية
الجهاز المركزي للمحاسبات

عملية تدقيق نظم المعلومات

هدف الجلسة

سيتمكن المشاركون في نهاية الجلسة من:

- التخطيط لعملية التدقيق لتحديد ما إذا كانت نظم المعلومات محمية.
- تنفيذ عملية التدقيق بما يتفق مع معايير تدقيق نظم المعلومات.
- توصيل الملاحظات والنتائج والتوصيات إلى أصحاب المصلحة.
- المتابعة لتقييم ما إذا كانت المخاطر التي تم الإبلاغ عنها قد تم التعامل معها.

المحتويات

مقـــــــدمـــــة

- تغير البيئة الاقتصادية العالمية وظهور تكنولوجيا المعلومات وانتشارها في مختلف المجالات ومن بينها مجال المحاسبة والتدقيق؛ حيث أظهرت مسئوليات وتحديات جديدة أمام المحاسبين والمدققين الذين وجدوا أنفسهم أمام ضرورة التكيف مع هذه التغيرات والتطورات التي أثرت بشكل واضح على مختلف إجراءات مهمة التدقيق.
- أصبحت عملية تدقيق نظم المعلومات أحد الموضوعات الرئيسية لعمليات التدقيق التي تجريها الأجهزة العليا للرقابة في جميع أنحاء العالم.

تدقيق نظم المعلومات

أنواع التدقيق التي تقوم بها الأجهزة العليا للرقابة المالية والمحاسبة:

- تدقيق الأداء.
- التدقيق المالي.
- تدقيق الالتزام.
- تدقيق نظم المعلومات.
- التدقيق المتكامل.

تدقيق نظم المعلومات

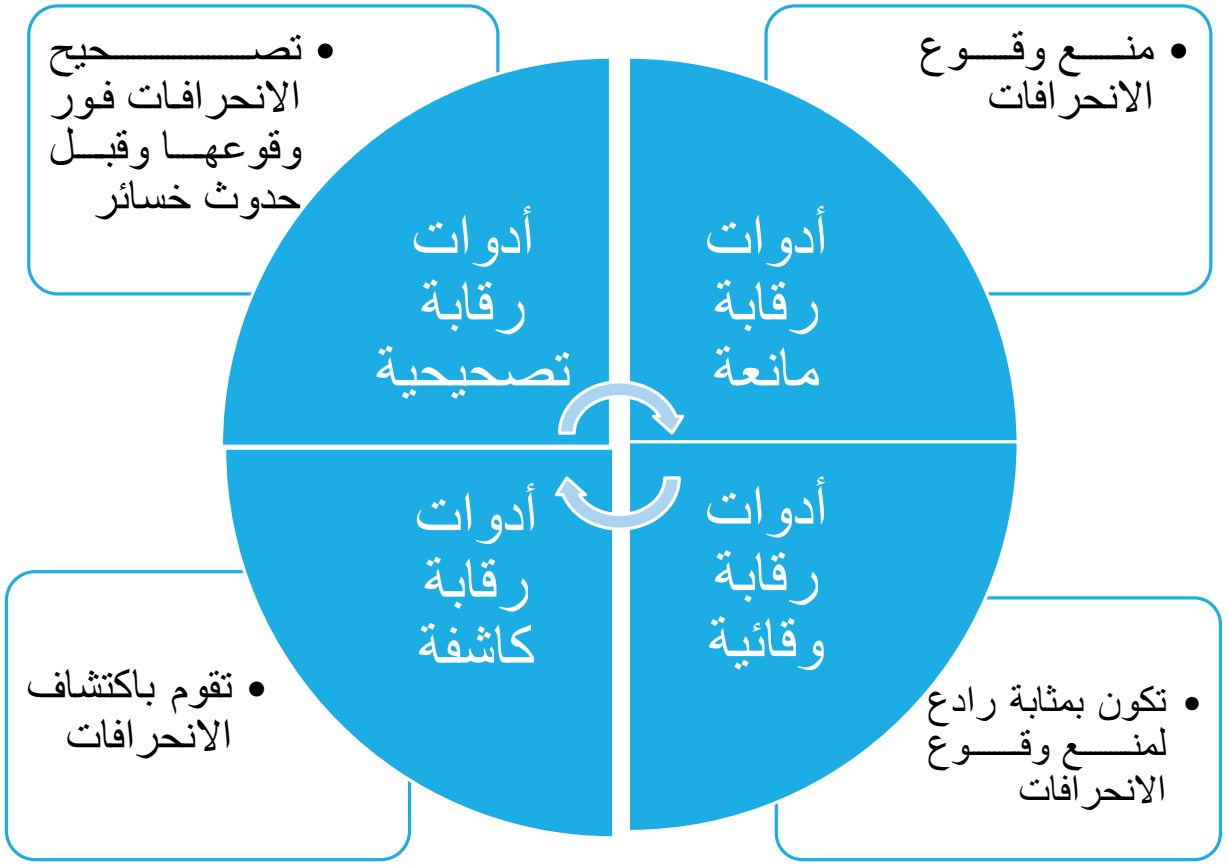
ما الفرق بين نظم المعلومات وتكنولوجيا المعلومات:

- نظم المعلومات.
- تكنولوجيا المعلومات.

تدقيق نظم المعلومات

- **نظم المعلومات :** تعرف بأنها مجموعة من الأنشطة الاستراتيجية والإدارية والتشغيلية والعمليات ذات الصلة المشتركة في جمع ومعالجة وتخزين وتوزيع واستخدام المعلومات وتقنياتها ذات الصلة. تعتبر نظم المعلومات متميزة عن تكنولوجيا المعلومات في أن نظم المعلومات تتضمن تكنولوجيا المعلومات التي تتفاعل مع باقي المكونات.
- **تكنولوجيا المعلومات :** تعرف بأنها الأجهزة والبرمجيات والاتصالات والمرافق الأخرى المستخدمة لإدخال البيانات وتخزينها ومعالجتها ونقلها وإخراجها بأي شكل من الأشكال.

أنواع أدوات الرقابة



أنواع أدوات الرقابة

أدوات الرقابة المانعة

تُصمم أدوات الرقابة المانعة بطريقة تمنع حدوث تهديد محتمل وبالتالي تتجنب أي تأثير محتمل لذلك الحدث التهديدي.

- استخدام الأفراد المؤهلين.
- تقسيم الواجبات.
- استخدام إجراءات التشغيل القياسية لمنع الأخطاء.
- إجراءات تفويض المعاملات.
- إجراءات التحكم في الوصول.
- جدران الحماية Firewalls.
- الحواجز المادية.

أنواع أدوات الرقابة

أدوات الرقابة الكاشفة

تُصمم الضوابط الكشفية لاكتشاف حدث تهديد بمجرد حدوثه. تهدف الضوابط الكشفية إلى تقليل تأثير مثل هذه الأحداث.

- المدققات الداخلية وأنواع التدقيق الأخرى.
- تدقيق السجلات Audit Trails.
- رسائل الخطأ على ملصقات الشريط.
- تحليل الاختلافات.
- ضمان الجودة.

أنواع أدوات الرقابة

أدوات الرقابة التصحيحية

تُصمم أدوات الرقابة التصحيحية لتقليل تأثير حدث تهديد بمجرد حدوثه وتساعد في استعادة الأعمال إلى العمليات الطبيعية.

- التخطيط لاستمرارية الأعمال.
- التخطيط لاستعادة الكوارث.
- التخطيط للاستجابة للحوادث.
- إجراءات النسخ الاحتياطي.

أنواع أدوات الرقابة

أدوات الرقابة الوقائية

تصمم أدوات الرقابة الوقائية بهدف إعطاء إشارة تحذيرية لردع أي تهديد محتمل.

- كاميرات المراقبة أو علامات "تحت المراقبة".
- علامات التحذير.

أنواع أدوات الرقابة

الفرق بين الضوابط المانعة والضوابط الرادعة

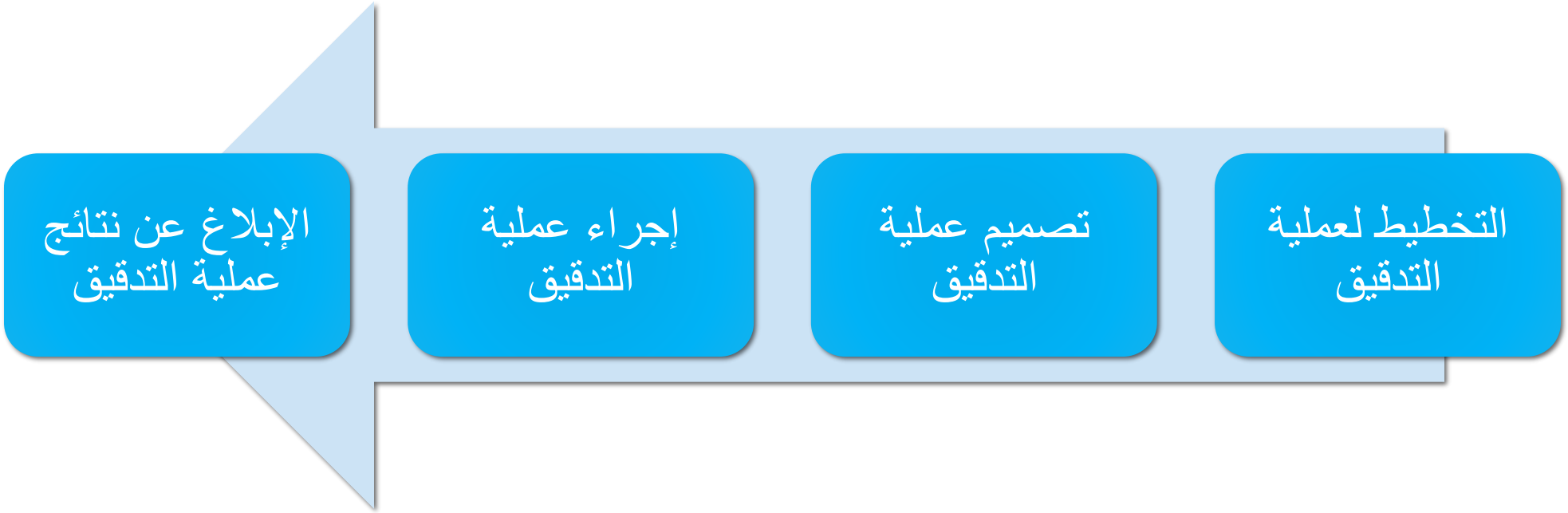
عند تنفيذ أداة رقابة مانعة، يمنع المتسلل من أداء فعل، ولا يكون له حرية الاختيار بين أداء الفعل غير المرغوب أو تركه.

عند تنفيذ ضابط رادع، يُعطى المتسلل تحذيرًا وهنا يكون للمتسلل خيار إما أن يتصرف وفقًا للتحذير أو يتجاهل التحذير.

وعلى سبيل المثال باب مغلق يوصل إلي غرفة هو ضابط مانع، لا يمكن للمتسللين الدخول من الباب. من ناحية أخرى، فقط علامة تحذير تقول "ممنوع الدخول" هي ضابط رادع. يمكن للمتسللين تجاهل التحذير ودخول الغرفة.

تدقيق نظم المعلومات

مراحل عملية تدقيق نظم المعلومات

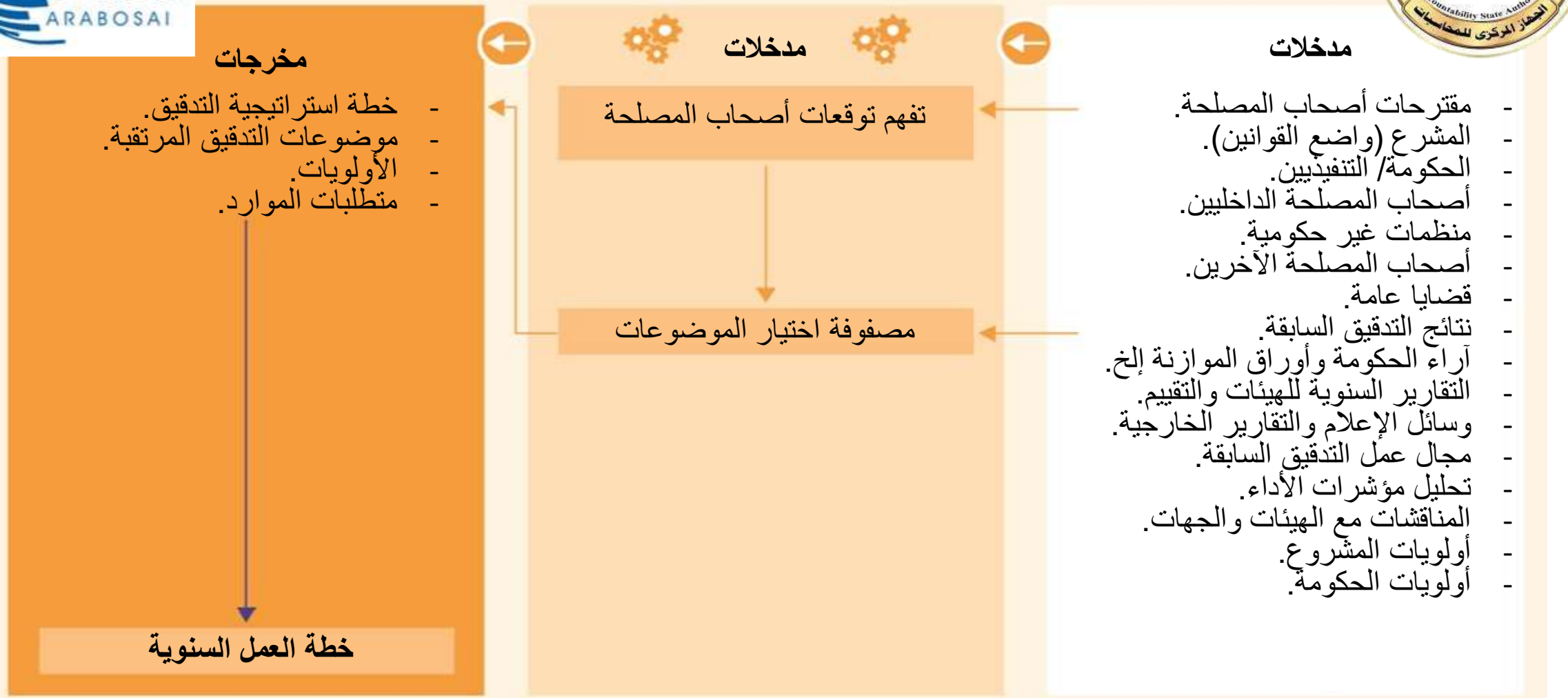


اختيار موضوع التدقيق

التخطيط الاستراتيجي لمراجعة نظم المعلومات

- التخطيط الاستراتيجي هو عملية تحديد الأهداف طويلة المدى للجهاز الأعلى للرقابة وتحديد أفضل النهج الممكنة لتحقيقها.
- يقوم الجهاز الأعلى للرقابة بتحليل هذه الموضوعات لتحديد أي عمليات رقابة لنظم المعلومات تحظى بأكثر اهتمام بالنسبة للجمهور والحكومة والمشرع؛ وأي منها يمكن أن يضيف قيمة أكثر.
- وتختلف عملية التخطيط الاستراتيجي المستخدمة بين الأجهزة العليا للرقابة. وعادة ما تغطي الخطط عدة سنوات وتوجه الأجهزة العليا للرقابة في اختيار موضوعات رقابة نظم المعلومات. الخطة الاستراتيجية عادة ما ينتج عنها خطة تدقيق تشغيلية ذات مستوى منخفض، تحدد الموضوعات التي سيتم تناولها في السنة القادمة أو سنوات أكثر.

اختيار موضوع التدقيق



اختيار موضوع التدقيق

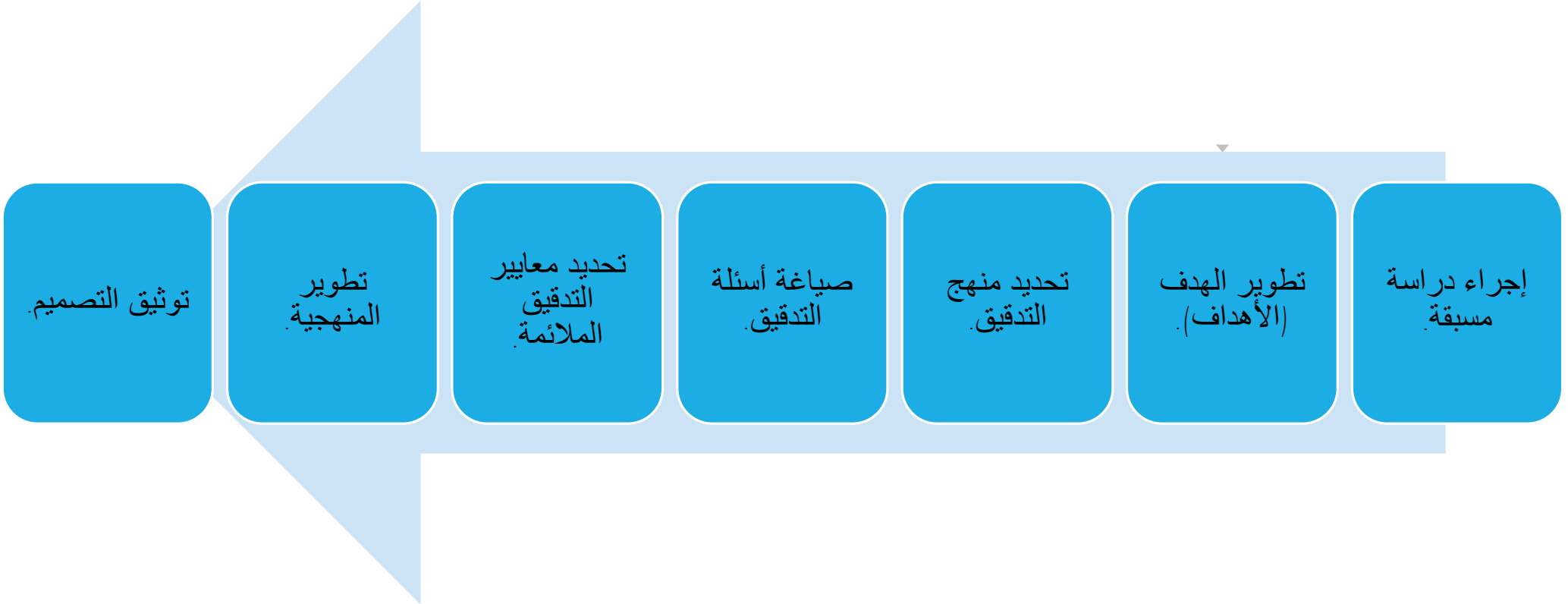
قائمة معايير الاختيار لموضوعات التدقيق

- المادية.
- قابلية التدقيق.
- التأثير المحتمل.
- المخاطر التي يتعرض لها الجهاز الأعلى للرقابة.
- المشرع أو المصلحة العامة.
- الصلة.
- دقة التوقيت.
- أعمال التدقيق السابقة .
- الأعمال الرئيسية الأخرى المخطط لها أو قيد التنفيذ.
- طلب تدقيق نظم المعلومات.

اختيار موضوع التدقيق

المعيار	الأوزان	موضوعات التدقيق البديلة التي تم تحديدها							
		موضوع 1		موضوع 2		موضوع 3		موضوع 4	
		نقاط	الوزن النسبي	نقاط	الوزن النسبي	نقاط	الوزن النسبي	نقاط	الوزن النسبي
الأهمية النسبية	15	3	45	3	45	2	30	2	30
القابلية للمراجعة	15	3	45	1	15	2	30	2	30
التأثير المتوقع	15	3	45	2	30	2	30	2	30
المخاطر تجاه الجهاز الأعلى للرقابة	10	3	30	1	10	3	30	3	30
المشرع أو المصلحة العامة	10	3	30	3	30	0	0	3	30
الصلة	10	3	30	3	30	2	20	3	30
دقة التوقيت	5	3	15	3	15	1	5	2	10
أعمال التدقيق السابقة	5	2	10	3	15	2	10	2	10
الأعمال الرئيسية الأخرى المخطط لها أو قيد التنفيذ	5	2	10	1	5	1	5	1	5
طلب تدقيق نظم المعلومات	10	3	30	0	0	3	30	2	20
مجموع الوزن النسبي	100		290		195		190		225
التصنيف			1		3		4		2

تصميم عملية التدقيق



تصميم عملية التدقيق

- الدراسة المسبقة لموضوع التدقيق

وللتأكد من أن التخطيط لعملية التدقيق تم بشكل صحيح، يحتاج المدقق إلى الحصول على المعرفة الكافية بالبرنامج الذي تتم مراجعته أو أعمال الجهة الخاضعة للتدقيق قبل بدء عملية التدقيق. لذلك، قبل البدء في التدقيق، من الضروري عمومًا إجراء أعمال بحثية لبناء المعرفة واختبار تصميمات التدقيق المختلفة والتحقق من توافر البيانات اللازمة. يمكن تسمية هذا العمل الأولي بالدراسة المسبقة.

تصميم عملية التدقيق

أهداف التدقيق

يجب على المدقق أن يضع هدفاً (أهدافاً) محددة بوضوح للتدقيق.

أسئلة التدقيق

تكون أسئلة التدقيق إما وصفية (بمعنى أنها تصف حالة ما) أو تقييمية (بمعنى أنها تقيم الحالة طبقاً لمعيار ويمكن أن تكون معيارية أو تحليلية). يمكن أن تتخذ أسئلة التدقيق الوصفية أشكالًا متعددة. بعضها يمكن الرد عليه بسهولة، في حين أن البعض الآخر أكثر صعوبة.

تصميم عملية التدقيق

تحليل المشكلة بين السبب والنتيجة

المستوى الأول هدف التدقيق	تقييم فعالية إجراءات إدارة حسابات المستخدمين في الدومين- Active Directory
المستوى الثاني أسئلة التدقيق	هل تتم إنشاء حسابات المستخدمين وتعديلها وإلغاؤها وفقًا لسياسات وإجراءات المؤسسة؟
	هل هناك وثائق توضح عملية توفير الحسابات وإلغاء توفيرها للمستخدمين؟

تحديد نطاق التدقيق

يحدد نطاق التدقيق الحدود ويتناول موضوعات مثل أسئلة محددة التي ينوي طرحها ونوع الدراسة التي سيتم اكتمالها . وعلى وجه الخصوص، يحدد نطاق التدقيق الموضوع الذي سيقوم المدقق بتقييمه وإعداد تقرير عنه، والمستندات أو السجلات التي سيتم فحصها، وفترة التدقيق، ونطاق الفحص التي سيتم تضمينها.

تصميم عملية التدقيق

مثال على نطاق عملية تدقيق نظم المعلومات

النطاق: يشمل التدقيق تقييمًا شاملاً لتنفيذ إطار حوكمة تكنولوجيا المعلومات في شركة ABC، بهدف ضمان التوافق مع الأهداف التنظيمية وتحسين الاستثمارات التكنولوجية وتعزيز عمليات اتخاذ القرار. سيشمل التدقيق جميع جوانب حوكمة تكنولوجيا المعلومات، بما في ذلك هياكل الحوكمة والسياسات والعمليات والضوابط، عبر مختلف الإدارات ووحدات الأعمال داخل المؤسسة. وسيتم إجراء التقييم على مدار فترة تستمر أربعة أسابيع، من خلال المقابلات مع أصحاب المصلحة الرئيسيين، ومراجعة الوثائق ذات الصلة مثل السياسات والإجراءات التكنولوجية، وتقييم فعالية الآليات الحالية لحوكمة تكنولوجيا المعلومات. سيتعاون فريق التدقيق، المؤلف من مدققي تكنولوجيا المعلومات المعتمدين، مع ممثلين من قسم تكنولوجيا المعلومات في شركة ABC، والإدارة التنفيذية، وأصحاب المصلحة الآخرين لجمع الرؤى والتوصيات لتعزيز ممارسات حوكمة تكنولوجيا المعلومات وذلك لتحسين الأداء التنظيمي الشامل وإدارة المخاطر.

تصميم عملية التدقيق

طرق جمع المعلومات:

- المقابلة.
- جمع الوثائق.
- الملاحظات والتفتيش المباشر.
- الدراسات الاستقصائية.
- الزيارات الميدانية.
- تدقيق الملفات وملاحظات المنظمة.
- أساليب المجموعات الصغيرة.
- البيانات الثانوية.
- دراسات الحالة.

تصميم عملية التدقيق

إدارة المخاطر أثناء تصميم التدقيق

يجب على المدقق إدارة مخاطر التدقيق بشكل فعال لتجنب ظهور نتائج واستنتاجات وتوصيات غير صحيحة أو غير كاملة، أو تقديم معلومات غير متوازنة أو الفشل في إضافة قيمة.

مخاطر التدقيق هي احتمال أن تكون نتائج المدققين أو استنتاجاتهم أو توصياتهم غير صحيحة أو غير كاملة بسبب عوامل مثل عمليات التدقيق غير الكافية، أو غير المناسبة،أو عدم كفاية الأدلة، أو القيود المفروضة على الموارد أو البيانات، أو الإغفال المتعمد أو المعلومات المضللة بسبب التحريف أو الاحتيال.

تصميم عملية التدقيق

تحديد وتقييم المخاطر

- هل يمتلك فريق التدقيق المهارات والمعرفة الكافية؟
- هل الأطر الزمنية والموارد اللازمة لإجراء التدقيق متاحة ومجدية؟
- هل موضوع التدقيق حساس أو واضح للغاية أو مثير للجدل؟
- هل التدقيق وموضوعه معقد للغاية، أم أنه يشمل مجالات معرضة تقليديًا للمخاطر؟
- هل هناك تهديدات حقيقية أو محسوسة متعلقة باستقلالية المدققين المكلفين بالتدقيق؟
- هل هناك مخاطر تتعلق بنزاهة الإدارة أو العلاقات مع الجهات الخاضعة للتدقيق؟
- هل تتوفر بيانات كافية وهل البيانات ذات جودة؟

تصميم عملية التدقيق

تخفيف مخاطر التدقيق

- زيادة أو تقليص نطاق العمل.
- إضافة متخصصين (على سبيل المثال، علماء المنهج) أو مراجعين أو كبار الموظفين الإضافيين.
- زيادة الموارد.
- مراقبة أو تتبع التقدم المحرز بانتظام مقابل المعالم المؤقتة من خلال تحديث خطط التدقيق أو عقد الاجتماعات أو إنتاج تقارير الحالة.
- تخصيص وقت إضافي، إن أمكن، للمهام الخطرة بشكل خاص.
- تغيير الطريقة للحصول على أدلة إضافية أو أدلة عالية الجودة أو أشكال بديلة من الأدلة المؤيدة.
- مواءمة النتائج والاستنتاجات لتعكس الأدلة التي تم الحصول عليها.
- زيادة التدقيق الإشرافي أو الإداري.

تصميم عملية التدقيق

تحديد الأطر الزمنية والموارد اللازمة:

- تحديد أطر زمنية واقعية للتدقيق والمهام الفردية التي يجب إكمالها.
- تحديد ومواءمة عدد كافٍ من المدققين والمشرفين وأصحاب المصلحة الداخليين والخارجيين مع مهام محددة لتلبية الأطر الزمنية المتوقعة لإنجاز العمل.
- تحديد التكاليف المرتبطة بالسفر والتدريب والمعدات والخبراء الخارجيين، والتكاليف الإضافية الأخرى.

إجراءات عملية التدقيق

تحديد مدى كفاية وملاءمة الأدلة

يجب على المدقق الحصول على أدلة كافية ومناسبة من أجل تحديد نتائج التدقيق، والتوصل إلى استنتاجات استجابة لهدف (أهداف) التدقيق وأسئلة التدقيق وإصدار التوصيات عندما يكون ذلك مناسبًا ومسموحًا به بموجب تفويض من الجهاز الأعلى للرقابة.

إجراءات عملية التدقيق

كفاية الأدلة

الكفاية هي مقياس لكمية الأدلة التي تستخدمها لدعم النتائج والاستنتاجات المتعلقة بهدف (أهداف) التدقيق الخاص بك وأسئلتك.

هل حصلت على أدلة كافية لإقناع شخص مضطلع بالأمر بأن النتائج معقولة؟

إجراءات عملية التدقيق

مدى ملاءمة الأدلة

- الأدلة ذات الصلة لها علاقة منطقية مع القضية التي يتم تناولها وأهميتها.
- الأدلة الصحيحة مبنية على تفكير سليم أو معلومات دقيقة.
- الأدلة الموثوقة : تعني أن النتائج ينبغي أن تكون متسقة عندما يتم قياس المعلومات أو اختبارها كما ينبغي أن تكون قابلة للتحقق.

إجراءات عملية التدقيق

مدى ملاءمة الأدلة

- غالبًا ما تكون الأدلة الوثائقية أكثر موثوقية من أدلة الشهادة.
- تعتبر أدلة الشهادة المدعمة كتابيًا أكثر موثوقية من الأدلة الشفهية وحدها.
- تعتبر الأدلة التي يتم الحصول عليها من طرف ثالث موثوق وغير متحيز أكثر صحة وموثوقية من الأدلة التي يتم الحصول عليها من إدارة الجهة الخاضعة للتدقيق.
- يمكن أن تؤثر الضوابط الداخلية الضعيفة على موثوقية الأدلة واتساقها عبر المؤسسة.
- تعتبر الأدلة التي يتم الحصول عليها من خلال الملاحظة والعمليات الحسابية والتفتيش المباشر للمدقق أكثر موثوقية من الأدلة التي يتم الحصول عليها بشكل غير مباشر.
- تعتبر المستندات الأصلية أكثر موثوقية من المستندات المنسوخة.

إجراءات عملية التدقيق

الجهات الخاضعة للتدقيق

بالنسبة لمعظم عمليات التدقيق، تعد الجهات الخاضعة للتدقيق هي المصدر الرئيسي للأدلة الوثائقية ذات الصلة.

حيث ينبغي أن تتأكد من أن تطلب من الجهات الخاضعة للتدقيق المستندات التي توفر أدلة للإجابة على أسئلة التدقيق الخاصة بك. يمكن أن تكون هذه المستندات نوعية أو كمية. الأمثلة تشمل:

- السياسات والتوجيهات والمخططات التنظيمية.
- العقود والفواتير والمعلومات المحاسبية وبيانات الميزانية.
- بيانات كمية عن الموضوع الذي يتم مراجعته.
- البحوث أو الدراسات المتعلقة بموضوع التدقيق.

إجراءات عملية التدقيق

ما هي الإجراءات التي ستتخذها إذا قامت إحدى الجهات الخاضعة للتدقيق بعرقلة أو إعاقة وصولك إلى المعلومات ذات الصلة بأسئلة التدقيق الخاصة بك؟

إجراءات عملية التدقيق

التغلب على التحديات في الوصول إلى المعلومات أثناء عمليات التدقيق

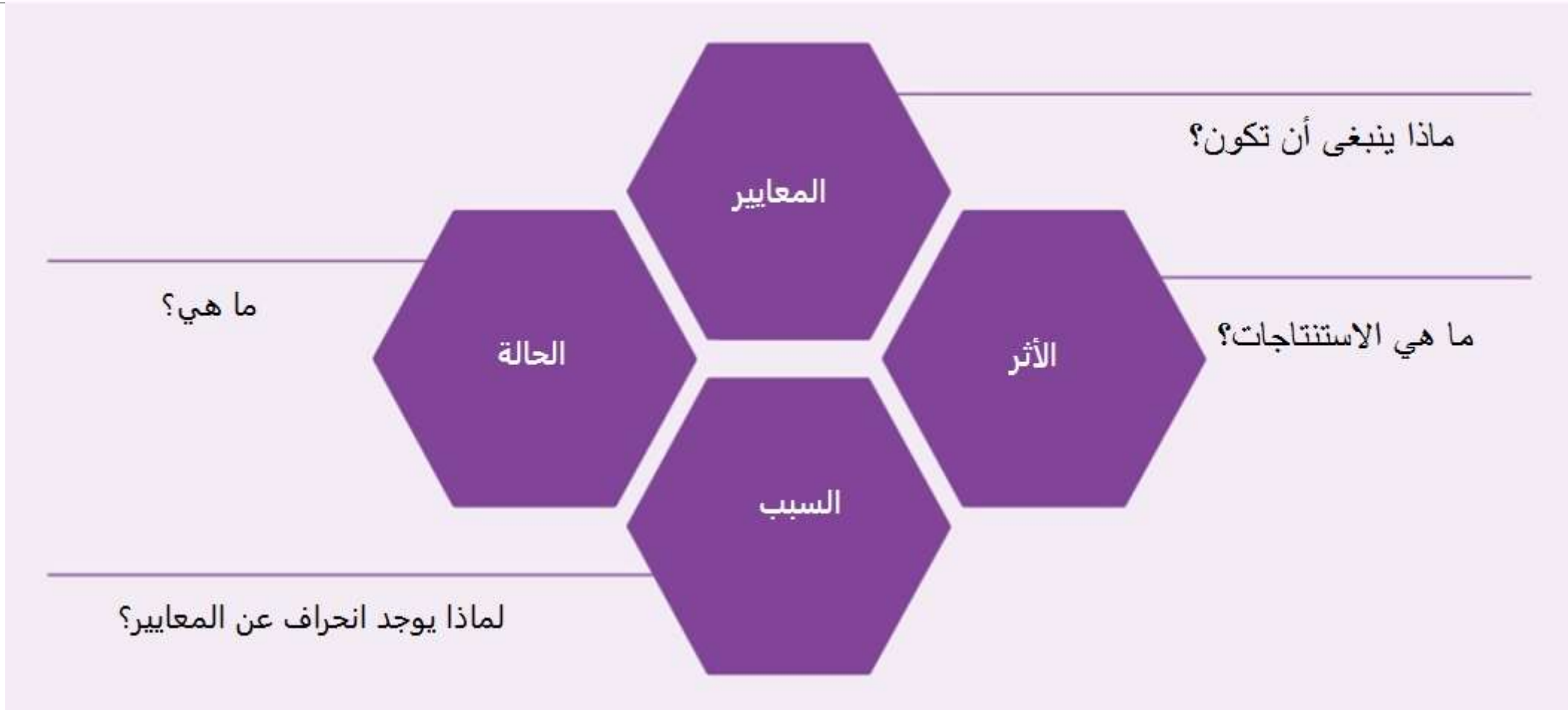
- استشر خبيرًا قانونيًا داخل الجهاز الأعلى للرقابة الخاص بك.
- التأكد من أن طلبك للحصول على معلومات له علاقة مباشرة بأسئلة مراجعة محددة.
- اشرح طبيعة الطلب إلى الجهة الخاضعة للتدقيق على وجه التحديد قدر الإمكان واربطه بسؤال (أسئلة) التدقيق المحدد الخاص بك.
- تحديد مواعيد محددة لتلقي المعلومات المطلوبة.
- إذا كانت المعلومات المطلوبة حساسة من الناحية القانونية، فاعمل مع إدارة الجهاز الأعلى للرقابة والجهة الخاضعة للتدقيق لتحديد ما إذا كان هناك مصدر بديل للمعلومات من شأنه أن يلبي احتياجات التدقيق.
- قم بتوثيق المحاولات التي قمت بها للحصول على المعلومات والاحتفاظ بسجل لطلباتك.

تطوير النتائج والاستنتاجات والتوصيات

- يجب على المدقق تحليل المعلومات المجمعة والتأكد من وضع نتائج عملية التدقيق في منظورها والرد على أهداف وأسئلة التدقيق التي تعيد صياغة أهداف وأسئلة التدقيق حسب الحاجة.
- بمجرد القيام بجمع وتحليل الأدلة الخاصة بك، من المهم تحويل انتباهك إلى تقييم الأدلة لتطوير نتائج التدقيق، ونتائج عملية التدقيق هي "ما هو موجود" مقارنة بـ "ما ينبغي أن يكون".

تطوير النتائج والاستنتاجات والتوصيات

عناصر النتيجة



تطوير النتائج والاستنتاجات والتوصيات

خطوات تطوير نتائج التدقيق

- قارن معايير التدقيق بالحالة.
- تحديد السبب والنتيجة.
- تقييم الأدلة.
- تطوير النتائج.
- تطوير الاستنتاجات.
- تطوير التوصيات (إن وجدت).

تطوير النتائج والاستنتاجات والتوصيات

تحديد السبب والتأثير

السبب: يشير السبب إلى الدواعي أو العوامل الأساسية التي أدت إلى الحالة المرصودة. ويوضح وجود انحراف بين الوضع الفعلي والمعيار (المعايير) المتوقع.

التأثير: التأثير هو نتيجة أو تأثير السبب المحدد على أداء الجهة الخاضعة للتدقيق. فهو يساعد المدققين على فهم آثار السبب على النتائج الإجمالية أو النتائج التي حققتها الجهة الخاضعة للتدقيق .

تطوير النتائج والاستنتاجات والتوصيات

مثال على نتيجة تدقيق نظم المعلومات:

الحالة: عدم وجود برامج مكافحة الفيروسات على بعض الأجهزة المهمة، على عكس المتطلبات المذكورة في سياسة أمن المعلومات للشركة.

المعايير: سياسة أمن المعلومات للشركة، وتحديدًا الفقرة 3.1 التي تنص علي وجوب وجود برامج مكافحة الفيروسات على جميع أجهزة الشركة.

السبب: عدم فعالية تطبيق سياسة أمن المعلومات للشركة، وعدم الوعي بين المستخدمين بأهمية تحديثات برامج مكافحة الفيروسات.

الأثر: زيادة عرضة الأجهزة لهجمات البرامج الضارة، والمخاطر المحتملة لانتهاكات البيانات، واضطراب العمليات التجارية الحاسمة.

تطوير النتائج والاستنتاجات والتوصيات

التحقق من أن الاستنتاج:

- يوضح درجة الاقتصاد والكفاءة و/أو الفعالية.
- واضح وموجز.
- يعكس معايير التدقيق.
- الكمية حيثما كان ذلك ممكنا
- يعكس التغيرات مع مرور الوقت.
- متوازن في اللهجة.
- يوفر رابطًا واضحًا للتوصيات.

تطوير النتائج والاستنتاجات والتوصيات

التوصيات البناءة هي

- تهدف إلى إصلاح الأسباب الكامنة وراء المشاكل التي تم العثور عليها.
- يجب أن تكون عملية وقابلة للتنفيذ.
- إضافة قيمة حقيقية إلى الموقف.
- يجب أن تستند إلى أدلة قوية وأن تكون منطقية مع النتائج.
- استخدام صياغة مختلفة، وتجنب أن تكون واضحة بشكل زائد.
- ليست مفصلة بشكل مفرط.

كتابة التقرير

السمات الرئيسية لتقرير تدقيق نظم المعلومات

يجب أن يسعى المدققون جاهدين لتقديم تقارير تدقيق شاملة ومقنعة وفي الوقت المناسب وسهلة القراءة ومتوازنة.

- شامل
- في الوقت المناسب
- مقنع
- سهل القراءة
- متوازن

متابعة نتائج عملية التدقيق

أهمية المتابعة

- تقييم التنفيذ.
- قياس التأثير.
- توجيه عمليات التدقيق المستقبلية.
- تعزيز أداء الجهاز الأعلى للرقابة.
- إعلام صناع القرار.

متابعة نتائج عملية التدقيق

طرق المتابعة المختلفة:

- اجتماعات المشاركة.
- الردود الكتابية.
- الزيارات الميدانية والمكالمات.
- رصد ردود الفعل.
- الاستفادة من عمليات التدقيق الأخرى.
- النظر في عمليات التدقيق الجديدة.

كتابة التقرير

الهيكل المنطقي للتقرير

- عنوان
- جدول المحتويات
- ملخص تنفيذي
- مقدمة
- أهداف التدقيق والأسئلة
- نطاق ومنهجية التدقيق
- معايير ومصادر التدقيق
- نتائج التدقيق
- خاتمة
- التوصيات
- الاختصارات

شكراً لكم

جمهورية مصر العربية
الجهاز المركزي للمحاسبات

إجراءات تدقيق نظم المعلومات

هدف الجلسة

سيتمكن المشاركون في نهاية الجلسة من:

- مراجعة الضوابط العامة لتكنولوجيا المعلومات.
- مراجعة ضوابط التطبيق.
- إجراء عمليات تشغيل البيانات.

المحتويات

مقـــــــدمـــــة

- في عالم اليوم حيث تعتبر المعلومات أحد أهم الأصول لأي منظمة، أصبح تأمين هذه المعلومات من التحديات الأساسية التي تواجه القطاعات الإدارية والتكنولوجية.
- الضوابط العامة لتكنولوجيا المعلومات وضوابط التطبيقات تلعب دورًا حاسمًا في حماية المعلومات وتوفير ضمان للأداء الأمثل للأنظمة التكنولوجية. هذه الضوابط ليست فقط ضرورية لحماية البيانات من الفقدان أو التلف، بل أيضًا لضمان تكامل البيانات وموثوقيتها وتوافرها في جميع الأوقات.

الضوابط العامة (General Control)

تعريف الضوابط العامة

الضوابط العامة، المعروفة أيضًا باسم ضوابط تقنية المعلومات العامة ITGC،هي الضوابط الأساسية التي تنطبق على جميع الأنظمة والعمليات والبيانات داخل بيئة تقنية المعلومات لمؤسسة ما، هذه الضوابط تكون أساسية لإنشاء بنية تحتية تقنية آمنة وموثوقة.

وتشتمل على :

- الوصول إلى البيانات والبرامج (Access to programs and Data)
- تطوير البرامج (Programs Development)
- تغيير البرامج (Programs Change)
- عمليات الحاسب (Computer Operations)

الضوابط العامة

الوصول إلى البرامج والبيانات (Access to programs and Data) وتتضمن ما يلى :

1- إدارة الوصول للمستخدمين :

إدارة الوصول للمستخدمين هي العمليات والتقنيات المستخدمة لإدارة ومراقبة وصول المستخدمين إلى المعلومات الحرجة داخل المنظمة؛ وتهدف إلي ضمان حصول الأفراد المناسبين على إمكانية الوصول إلى الموارد في الأوقات المناسبة للأسباب الصحيحة.

الضوابط العامة

1- إدارة الوصول للمستخدمين :

الجوانب الرئيسية لإدارة الوصول للمستخدمين تشمل:

- **التحقق من الهوية:** التأكد من هوية الأفراد الذين يدعون أن لديهم الحق في الوصول إلى الموارد.
- **التصـــريح:** تعيـــين وفـــرض حقـــوق وأذونـــات المســـتخدم بنـــاءً علـــى الأدوار والمسؤوليات والاحتياجات التجارية.
- **المصادقة:** استخدام طرق آمنة (كلمات مرور، البيومترية، التحقق بخطوتين) لتأكيد هوية الفرد.
- **التحكم في الوصول:** تقييد وصول المستخدمين إلى الموارد المتصلة بالشبكة وفقًا للسياسات التنظيمية ومتطلبات اللوائح الخارجية.
- **التـدقيق والامتثـال:** مراقبـة وتسـجيل الوصـول لضـمان الامتثـال للسياسـات الداخلية واللوائح الخارجية..

الضوابط العامة

2- الوصول المادي إلى موارد تقنية المعلومات:

الوصول المادي إلى موارد تقنية المعلومات هو جانب حيوي من الوضع الأمني الشامل للمؤسسة، حيث يشمل حماية الأجهزة والبرمجيات والشبكات والبيانات من الأفعال والأحداث الفعلية التي يمكن أن تسبب خسائر جسيمة أو تلف؛ ويكون دور مدقق نظم المعلومات أساسي في ضمان وجود تدابير أمنية فعلية فعّالة وأنها تعمل كما ينبغي.

الضوابط العامة

الوصول المادي إلى موارد تقنية المعلومات:

الجوانب الرئيسية للتحكم في الوصول الفعلي تشمل:

- **أمان المنشأة:** تأمين الحدود مع حواجز، وحراس أمن، وكاميرات المراقبة؛ وينبغي التحكم في نقاط الوصول من خلال أقفال آمنة وأنظمة بيومترية.
- **قيود الوصول:** الحد من الوصول إلى المناطق الحساسة للأشخاص الذين يحتاجون إلى ذلك لأداء وظائفهم. تنفيذ نظم تتبع الدخول باستخدام بطاقات أو إشارات.
- **التحكم في الزيارات:** إنشاء إجراءات لتحديد هوية الزائرين، وتسجيلهم، ومرافقتهم داخل المناطق الآمنة.
- **الضوابط البيئية:** حماية الموارد التقنية من المخاطر البيئية مثل الحرائق، والفيضانات، والحرارة الشديدة باستخدام أنظمة كشف وإخماد مناسبة.

الضوابط العامة

3- الفصل بين المهام المتعارضة:

الفصل بين الواجبات SoD هو آلية رقابة حاسمة في بيئات تقنية المعلومات، تهدف إلى منع الاحتيال والأخطاء من خلال التأكد من أن لا يكون لفرد واحد السيطرة على جميع جوانب المعاملة أو العملية الحساسة

ويُطبق هذا المبدأ في توزيع المسؤوليات بين الكوادر التقنية وفي آليات التفويض داخل تطبيقات المستخدمين.

كما يتمثل دور مدققي تقنية المعلومات في التحقق من كفاية وفعالية تنفيذ تدابير SoD لتقليل المخاطر.

الضوابط العامة

تقسيم الواجبات بين موظفي إدارة تكنولوجيا المعلومات:

يتضمن تقسيم الواجبات بين الكوادر التقنية تقسيم الأدوار والمسؤوليات لمنع أي فرد من تنفيذ عملية كاملة قد تؤدي إلى أخطاء متعمدة أو غير متعمدة. إليك بعض الاعتبارات الرئيسية:

- **تطوير وصيانة النظام:** يجب أن يدير أفراد أو مجموعات مختلفة تطوير النظام، والإنتاج، والتحكم في الوصول لتجنب التعارض والاختراقات المحتملة.
- **إدارة الشبكة والنظام:** يجب أن تكون مسؤوليات إدارة الشبكة والنظام مفصولة لتقليل خطر الوصول أو التغييرات غير المصرح بها.
- **معالجة وأمان البيانات:** يجب أن تكون الأدوار المتعلقة بإدخال البيانات، ومعالجة البيانات، وتدقيق البيانات مفصولة بوضوح لضمان سلامة وسرية البيانات.

الضوابط العامة

صلاحيات مستخدمي التطبيقات:

في تطبيقات المستخدمين، يضمن تقسيم الواجبات أن عملية طلب الوصول، والموافقة عليه، وتنفيذه يتم توزيعها بين عدة أفراد لمنع الاستغلال أو الأخطاء؛ وتشمل الجوانب الرئيسية ما يلي:

- **طلب الوصول والموافقة عليه:** يجب أن يكون أفراد مختلفون مسؤولين عن طلب الوصول إلى التطبيقات والموافقة على هذه الطلبات. حيث أن ذلك سوف يقلل من احتمالية منح الوصول غير المصرح به.
- **مراجعة وصول المستخدم:** يجب إجراء مراجعات دورية لوصول المستخدمين يقوم بها أفراد مختلفون عن الذين يمنحون أو يديرون الوصول لضمان فحص مستقل لحقوق الوصول.
- **إدارة التغييرات:** يجب تطبيق إدارة التغييرات على حقوق الوصول للتطبيق من خلال عملية رسمية تتضمن موافقات متعددة لضمان ضرورة وتفويض هذه التغييرات.

الضوابط العامة

تطوير البرمجيات (Program Development):

تطوير البرامج هو جزء حيوي من عمليات تقنية المعلومات، ويشمل التخطيط، والبرمجة، والاختبار، ونشر تطبيقات البرمجيات. يلعب مدققي تقنية المعلومات دورًا رئيسيًا في ضمان أن تكون هذه العملية آمنة وفعالة ومتوافقة مع المعايير التنظيمية. يساعد تطورهم المنظمات على التخفيف من المخاطر المرتبطة بتطوير البرمجيات، مثل خروقات البيانات، والاضطرابات التشغيلية، وعدم الامتثال للمعايير.

الضوابط العامة

تطوير البرامج:

يتبع تطوير البرامج عادةً دورة حياة منظمة، تشمل عدة مراحل:

- **جمع المتطلبات:** تحديد ما يجب بناؤه استنادًا إلى متطلبات المستخدمين وأهداف الأعمال.
- **التصميم:** تحديد هيكل النظام وإنشاء مستندات التصميم التفصيلية.
- **البرمجة:** كتابة الكود الفعلي بناءً على مواصفات التصميم.
- **الاختبار:** التحقق من أن البرمجيات تعمل كما هو مقصود من خلال أشكال مختلفة من الاختبار مثل الاختبار الوحدوي، واختبار الاندماج، واختبار النظام.
- **النشر:** إصدار البرمجيات التي تم اختبارها بالكامل في بيئة حية أو إنتاجية.
- **الصيانة والتحديثات:** تحديث وصيانة البرمجيات بشكل مستمر لمعالجة الاحتياجات الجديدة والتهديدات الأمنية.

الضوابط العامة

تغيير البرامج (Program Change) :

إدارة تغيير البرامج هي جانب حاسم من حوكمة تقنية المعلومات يضمن تنفيذ التغييرات على البرمجيات والأنظمة بفعالية وأمان، مع تقليل الانقطاعات في العمليات والحفاظ على التوافق مع الأهداف الاستراتيجية. يلعب مدققو تقنية المعلومات دورًا حاسمًا في الإشراف على هذه العملية، مما يضمن عدم إدخال تغييرات تشكل مخاطر جديدة أو تضعف الضوابط القائمة.

الضوابط العامة

إدارة تغيير البرامج :

تشمل إدارة تغيير البرامج نهجًا منظمًا لبدء التغييرات والموافقة عليها وتنفيذها في بيئة تقنية المعلومات. تتضمن هذه العملية عادةً:

- **بدء التغيير:** تحديد الحاجة إلى تغيير، والتي قد تنشأ عن متطلبات تجارية جديدة، أو مشاكل تم تحديدها أثناء العمليات، أو التقدم التكنولوجي.
- **تقييم الأثر:** تقييم الآثار المحتملة للتغيير المقترح على العمليات الحالية ومتطلبات الأمان والامتثال.
- **تخطيط التغيير:** وضع خطة مفصلة توضح الخطوات المطلوبة لتنفيذ التغيير، بما في ذلك الجداول الزمنية والموارد وإجراءات الاختبار.

الضوابط العامة

إدارة تغيير البرامج :

- **الموافقة على التغيير:** التدقيق والموافقة على خطة التغيير من قبل أصحاب المصلحة ذوي الصلة، بما في ذلك الإدارة وطاقم تقنية المعلومات وضباط الأمان.
- **التنفيذ:** تنفيذ التغيير وفقًا للخطة الموافق عليها، مع وجود ضوابط مناسبة لإدارة المخاطر.
- **مراجعة ما بعد التنفيذ:** تقييم نجاح تنفيذ التغيير، وتقييم ما إذا كان التغيير قد حقق الأهداف المقصودة، وتحديد أي مشكلات تحتاج إلى معالجة.

الضوابط العامة

إدارة عمليات الحاسب (Computer Operations):

تشمل إدارة عمليات الحاسب مجموعة واسعة من الأنشطة التي تهدف إلى ضمان الأداء الفعال والآمن لأنظمة الحاسب داخل المنظمة. ويشمل ذلك إدارة تدابير مكافحة الفيروسات، إجراءات النسخ الاحتياطي، وعمليات إدارة الحوادث؛ ويلعب مدققو تقنية المعلومات دورًا حيويًا في ضمان إدارة هذه العمليات بفعالية، والامتثال للمعايير، وتقليل المخاطر.

الضوابط العامة

إدارة مكافحة الفيروسات:

تشمل إدارة مكافحة الفيروسات نشر وتحديث ومراقبة برامج مكافحة الفيروسات عبر المنظمة للحماية من التهديدات مثل الفيروسات والديدان وأحصنة طروادة، المهام الرئيسية تشمل:

- **النشر:** التأكد من تثبيت برامج مكافحة الفيروسات على جميع الأجهزة ذات الصلة.
- **التحديثات المنتظمة:** الحفاظ على تحديث برامج مكافحة الفيروسات وتعريفات الفيروسات للحماية من التهديدات الأخيرة.
- **المراقبة والاستجابة:** المراقبة المستمرة للكشف عن البرمجيات الخبيثة والاستجابة لها.

الضوابط العامة

إجراءات النسخ الاحتياطي:

تعتبر إجراءات النسخ الاحتياطي حاسمة لضمان سلامة البيانات وتوافرها؛ وتشمل عملية إنشاء نسخ من البيانات بانتظام والتي يمكن استعادتها في حالة فقدان البيانات أو تلفها، الجوانب الرئيسية لإجراءات النسخ الاحتياطي تشمل:

- **الجدولة المنتظمة:** تنفيذ جدول منتظم للنسخ الاحتياطية لضمان تأمين البيانات بشكل متكرر.
- **التخزين والأمان:** استخدام حلول تخزين آمنة وموثوقة لتخزين نسخ النسخ الاحتياطية، وضمان حماية هذه النسخ من الوصول غير المصرح به والتهديدات المحتملة.
- **اختبار النسخ الاحتياطية:** اختبار النسخ الاحتياطية بانتظام لضمان إمكانية استعادتها بنجاح.

الضوابط العامة

إدارة الحوادث:

تشمل إدارة الحوادث تحديد وإدارة وحل الحوادث التقنية التي قد تؤثر على عمليات وأمان المنظمة، العمليات الرئيسية تشمل:

- **الكشف عن الحوادث والتبليغ عنها:** إنشاء أنظمة للكشف عن الحوادث والتبليغ عنها عند حدوثها.
- **تحليل الحوادث:** تحليل الحوادث لتحديد سببها وتأثيرها على العمليات.
- **الحل والاسترداد:** تنفيذ خطوات لحل الحوادث واستعادة أي أنظمة أو بيانات متأثرة.
- **مراجعة ما بعد الحادث:** مراجعة وتوثيق الحادث والاستجابة له لتحسين ممارسات إدارة الحوادث في المستقبل.

ضوابط التطبيقات (Application Controls)

ضوابط التطبيقات:

تعتبر ضوابط التطبيقات محددة للأنظمة والبرمجيات التي تعالج المعاملات والبيانات داخل المنظمة. تصمم هذه الضوابط لضمان سلامة، دقة، وسرية البيانات التي تتم معالجتها بواسطة التطبيقات. يلعب مدققو تقنية المعلومات دورًا حاسمًا في تقييم هذه الضوابط للتأكد من فعاليتها وامتثالها للسياسات الداخلية والمعايير التنظيمية.

ضوابط التطبيقات

ضوابط التطبيقات:

يمكن تصنيف ضوابط التطبيقات إلى ضوابط إدخال، معالجة، وإخراج:

- **ضوابط الإدخال:** تضمن هذه الضوابط أن البيانات المدخلة في أنظمة التطبيقات دقيقة وكاملة ومصرح بها؛ وتشمل الأمثلة التحقق من صحة النماذج، التحقق من التصاريح، والتحقق من الإدخال.
- **ضوابط المعالجة:** توجد هذه الضوابط لضمان إجراء عمليات التعامل مع البيانات داخل التطبيقات وتشمل مطابقة البيانات، تنفيذ سير العمل، وضوابط المعاملات التي تضمن سلامة البيانات خلال مرحلة المعالجة.
- **ضوابط الإخراج:** تضمن هذه الضوابط أن البيانات الصادرة من التطبيقات دقيقة وموزعة بشكل مناسب ؛ وتشمل مراجعة التقارير، التحقق من صحة البيانات، وتدابير السرية لحماية البيانات من الوصول غير المصرح به عند الإخراج.

ضوابط تشغيل البيانات (Data Processing)

ضوابط تشغيل البيانات:

أصبح تحليل البيانات أداة أساسية لمدققي تقنية المعلومات، مما يعزز قدرتهم على تقييم فعالية أنظمة المعلومات في المنظمات، والامتثال للوائح، والنزاهة التشغيلية العامة. من خلال استخدام تقنيات تحليل البيانات المختلفة، ويمكن لمدققي تقنية المعلومات الكشف عن التناقضات، وتحديد مناطق المخاطر، وتقديم رؤى عملية تساعد المنظمات على تحسين حوكمتها لتقنية المعلومات وأطر الرقابة الخاصة بها.

شكراً لكم

جمهورية مصر العربية
الجهاز المركزي للمحاسبات

المخاطر التي تواجه الجهات الخاضعة للتدقيق

هدف الجلسة

سيتمكن المشاركون في نهاية الجلسة من:

- التعرف على مخاطر نظم المعلومات التي تواجه الجهات الخاضعة للتدقيق.
- التفرقة بين أمن المعلومات والأمن السيبراني.
- التعرف على الأركان الثلاثة لأمن المعلومات.
- التحقق من مدى كفاية التدابير التي تتخذها الجهة الخاضعة للتدقيق في مواجهة التحديات.

المحتويات

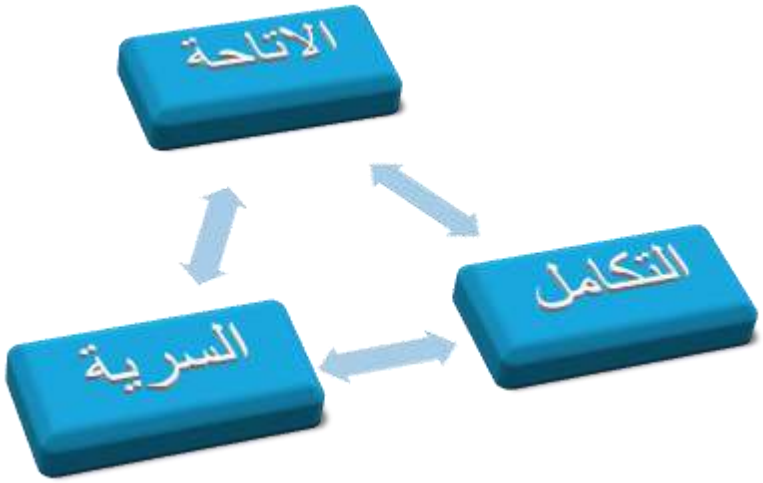
مقـــــــدمـــــة

- أمن المعلومات يعد عنصراً حيوياً لأي منظمة في العصر الرقمي الحديث، حيث تعتمد الشركات والمؤسسات بشكل متزايد على التكنولوجيا وتبادل البيانات الإلكترونية لتحقيق أهدافها.
- يساهم أمن المعلومات في حماية البيانات الحساسة والمعلومات السرية من التسريب أو الاختراق، مما يحافظ على استمرارية المؤسسات وثقة العملاء وحماية الأصول والبيانات التجارية.
- يساعد أمن المعلومات في الحفاظ على سلامة الأنظمة والشبكات، وتجنب الاختراقات والهجما ال، من هنا يُعَدُّ ته أمرًا حاسمًا.

أهمية أمن المعلومات

- حماية البيانات والمعلومات الهامة والحساسة.
- الحفاظ على استمرارية الأعمال.
- الالتزام بالمتطلبات القانونية والتنظيمية.
- حماية الملكية الفكرية.
- بناء الثقة مع العملاء وأصحاب المصلحة.
- منع سرقة الهوية واستخدام البيانات التي تم الاستيلاء عليها في الأعمال الاحتيالية.
- ضمان إتاحة وتكامل الأنظمة.

الأركان الثلاثة لأمن المعلومات



- تضمن **السرية** أن يكون الوصول إلى البيانات مقتصرًا فقط على الأفراد أو الأنظمة المصرح لها.
- يضمن **التكامل** بقاء البيانات دقيقة وكاملة وغير متغيرة أثناء التخزين والنقل والمعالجة.
- تضمن **الإتاحة** توافر المعلومات والموارد للمستخدمين المصرح لهم كلما احتاجوا إليها.

أمن المعلومات والأمن السيبراني

ما الفرق بين أمن المعلومات والأمن السيبراني:

- أمن المعلومات.
- الأمن السيبراني.

أمن المعلومات والأمن السيبراني

ما الفرق بين أمن المعلومات والأمن السيبراني:

- أمن المعلومات : يشير إلى ممارسة حماية المعلومات من الوصول غير المصرح به، أو الاستخدام، أو الكشف، أو التعطيل، أو التعديل، أو الإتلاف؛ ويشمل تنفيذ مجموعة متنوعة من التدابير والسياسات والإجراءات لحماية البيانات الحساسة وضمان السرية والنزاهة وتوفرها؛ كما يشمل أمن المعلومات مجموعة واسعة من التقنيات الهادفة إلى التخفيف من المخاطر والضعف المرتبط بتخزين ونقل ومعالجة المعلومات داخل منظمة ما.
- الأمن السيبراني: هو جزء فرعي من أمن المعلومات ويركز بشكل خاص على حماية الأصول الرقمية والأنظمة والشبكات من التهديدات السيبرانية؛ كما يتضمن الدفاع ضد الأنشطة الخبيثة التي تُجرَى عبر الإنترنت أو غيرها من القنوات الرقمية، بما في ذلك الهجمات السيبرانية، وانتهاكات البيانات، والإصابات بالبرمجيات الخبيثة، وعمليات الصيد الاحتيالي، وغير ذلك من أشكال الجريمة السيبرانية.

أمن المعلومات والأمن السيبراني

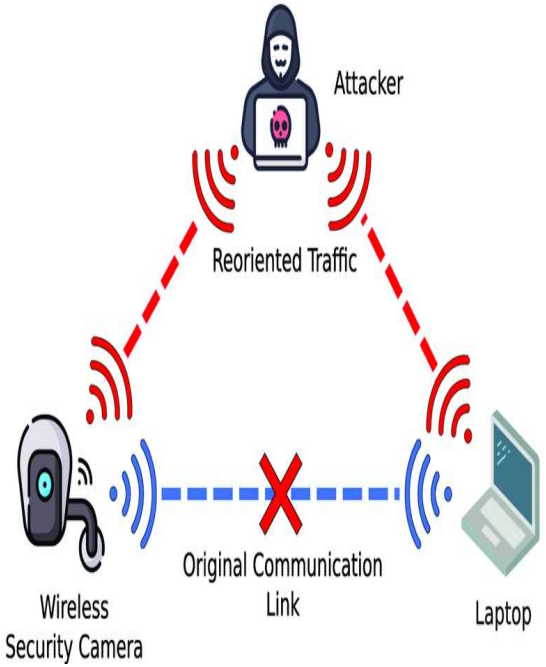
من حيث طبيعة التهديدات :

- يتعامل أمن المعلومات مع مجموعة أوسع من التهديدات، بما في ذلك السرقة المادية، والوصول غير المصرح به، والخطأ البشري، والكوارث الطبيعية، بالإضافة إلى التهديدات السيبرانية.
- يتعامل الأمن السيبراني بشكل أساسي مع التهديدات السيبرانية مثل البرامج الضارة، والاختراقات، وعمليات الصيد الاحتيالي، وبرامج الفدية، وهجمات حجب الخدمة، التي تستغل الثغرات في الأنظمة الرقمية والشبكات.

من حيث الحلول التكنولوجية :

- يستخدم أمن المعلومات مجموعة متنوعة من الضوابط التقنية والإدارية والمادية لحماية أصول المعلومات، بما في ذلك التشفير، وضوابط الوصول، وآليات المصادقة، والسياسات الأمنية، وتدريب الموظفين.
- يعتمد الأمن السيبراني بشكل كبير على الحلول التكنولوجية مثل جدران الحماية، وأنظمة اكتشاف الاختراق، وبرامج مكافحة الفيروسات، وبروتوكولات التشفير، وبنية الشبكة الأمنة لاكتشاف ومنع وتخفيف التهديدات السيبرانية.

هجمات الأمن السيبراني الشائعة



- **اختراق البيانات: البرمجيات الخبيثة (Malware):** تشمل أنواع البرمجيات الخبيثة الفيروسات، والديدان، وحصان طروادة، وبرمجيات الفدية، أي برمجيات ضارة مصممة لإلحاق الضرر أو استغلال أي جهاز، أو خدمة، أو شبكة.
- **الصيد الاحتيالي Phishing:** هذا النوع من الهجمات يتضمن خداع الضحية لتقديم معلومات حساسة مثل كلمات المرور، أرقام بطاقات الائتمان، أو معلومات شخصية أخرى من خلال التظاهر على أنها طلب شرعي أو كيان موثوق في الاتصالات الإلكترونية.
- **هجمة الرجل في المنتصف MitM Attack:** حيث يعترض المهاجمون الاتصال بين طرفين يعتقدان أنهما يتواصلان مباشرة مع بعضهما البعض.
- **هجمات الحرمان من الخدمة DoS والحرمان الموزع من الخدمة DDoS:** تهدف هذه الهجمات إلى إغلاق جهاز أو شبكة، مما يجعلها غير متاحة لمستخدميها حيث تغمر هجمات الحرمان من الخدمة و الأنظمة، والخوادم، أو الشبكات بحركات مروريه لاستنزاف الموارد والنطاق الترددي.

هجمات الأمن السيبراني الشائعة

- **الحقن SQL (SQL Injection):** تتضمن هذه الهجمات إدخال أوامر SQL ضارة في حقل إدخال البيانات ، للتلاعب بقاعدة البيانات للوصول إلى معلومات لم يقصد عرضها، بما في ذلك بيانات الشركة.

- **استغلال اليوم الصفر Zero-Day Exploit:** حيث يستغل المهاجمون نقطة ضعف أمنية خطيرة محتملة في البرمجيات قد لا يكون البائع أو المطور على علم بها؛ وتحدث الهجمة في "اليوم الصفر"، أي أن المشكلة لم تُعرف بعد، لذا لا توجد تصحيحات أو إصلاحات متاحة.
- **برمجيات الفدية Ransomware:** هي نوع من البرمجيات الضارة المصممة لحظر الوصول إلى نظام كمبيوتر أو البيانات او المعلومات حتى يتم دفع مبلغ من المال.
- **البرمجة النصية (Script) عبر المواقع XSS:** تحدث عندما يحقن المهاجمون سكربتات ضارة في مواقع ويب حميدة وموثوقة. تحدث هجمات XSS عندما يستخدم المهاجم تطبيق ويب لإرسال رمز ضار، عادةً على شكل سكربت جانبي للمتصفح، إلى مستخدم نهائي مختلف.

الآثار المترتبة على اختراق الأمن السيبراني

- **الخسائر المالية:** التكاليف المرتبطة بإصلاح الاختراق، والرسوم القانونية، والغرامات التنظيمية، وفقدان الإيرادات بسبب التوقف أو التأثير على السمعة.
- **العواقب القانونية والتنظيمية:** عدم الامتثال لقوانين حماية البيانات واللوائح يمكن أن يؤدي إلى غرامات مالية كبيرة، ودعاوى قانونية، وضرر لسمعة الشركة.
- **فقدان ثقة العملاء:** قد يختار العملاء توجيه أعمالهم في مكان آخر إذا شعروا بأن معلوماتهم الحساسة لم تتم حمايتها بشكل كاف، مما يؤدي إلى فقدان الإيرادات وحصة السوق.

إطارات الأمان السيبراني

- **نظرة عامة على الإطارات الشائعة:** توفر إطارات الأمن السيبراني مثل NIST و ISO/IEC 27001 إرشادات وممارسات جيدة لإدارة مخاطر الأمن السيبراني.
- **أهمية تنفيذ الإطارات لإدارة المخاطر:** من خلال إتباع الإطارات المعتمدة، يمكن للشركات تحديد وتقييم وتخفيف مخاطر الأمن السيبراني بطريقة منظمة ومنهجية، مما يقلل من احتمالية الاختراقات وتأثيرها على المؤسسة.

إدارة الثغرات

- **تحديد وتقييم الثغرات:** تساعد التقييمات الدورية للثغرات واختبار الاختراق في تحديد نقاط الضعف في الأنظمة والتطبيقات التي يمكن استغلالها من قبل المهاجمين.
- **إدارة التصحيحات:** يعد تطبيق التصحيحات والتحديثات على البرامج والأنظمة في الوقت المناسب أمرًا أساسيًا للتعامل مع الثغرات المعروفة وتقليل مخاطر الاستغلال.
- **أهمية المسح الدوري للثغرات:** يساعد المسح المستمر والمسح للأنظمة عن الثغرات في ضمان أن تظل التدابير الأمنية فعالة ضد التهديدات المتطورة.

تدريب الموظفين وزيادة الوعي

- **أهمية تدريب الموظفين في مجال الأمن السيبراني:** غالبًا ما يكون الموظفون الحلقة الأضعف في بنية الأمان للمؤسسة.
- **توفير تدريب دوري:** حول ممارسات الأمان السيبرانية يساعد في زيادة الوعي وتمكين الموظفين من التعرف على التهديدات والاستجابة الأمنية لها.
- **الممارسات المثلى للتدريب على زيادة الوعي الأمني:** يجب أن تغطي برامج التدريب مواضيع هامة ، مثل التوعية من الصيد الاحتيالي، ومعايير كلمات المرور، ومعالجة البيانات بشكل آمن، والإبلاغ عن الأنشطة المشبوهة.
- **خلق ثقافة توعية بالأمن:** تعزيز ثقافة الأمان حيث أن فهم الموظفون لأهمية حماية المعلومات الحساسة وشعورهم بالراحة عند الإبلاغ عن حوادث الاختراق أمر حاسم للتخفيف من تهديدات الداخل وتقليل مخاطر الاختراق.

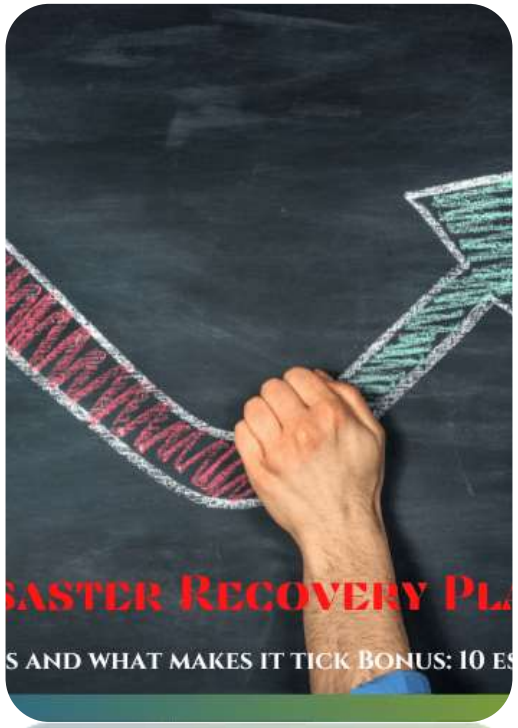
التحكم في الوصول والمصادقة

- **التحكم في الوصول بناءً على الأدوار:** تقييد الوصول إلى الأنظمة والبيانات بناءً على أدوار ومسؤوليات المستخدمين يساعد في تقليل مخاطر الوصول غير المصرح به وتسرب البيانات.
- **المصادقة المتعددة العوامل:** إضافة طبقة إضافية من المصادقة بعد كلمات المرور، مثل التعرف على الوجه أو رموز المرور مرة واحدة، يعزز الأمان عن طريق تقليل مخاطر سرقة بيانات الاعتماد والوصول غير المصرح به.
- **مبدأ الامتياز الأقل:** منح المستخدمين أدنى مستوى من الوصول المطلوب لأداء وظائفهم يساعد في تقليل الأثر المحتمل للتهديدات الداخلية والوصول غير المصرح به.

تشفير البيانات

- **أهمية تشفير البيانات:** تشفير البيانات الحساسة في التخزين وأثناء النقل يساعد في حمايتها من الوصول غير المصرح به، مما يضمن السرية والتكامل.
- **أنواع التشفير:** يستخدم التشفير التماثلي نفس المفتاح للتشفير وفك التشفير، بينما يستخدم التشفير غير التماثلي مفاتيح عامة وخاصة منفصلة.
- **تنفيذ مزيج من أساليب التشفير:** استنادًا إلى حساسية البيانات والحالة الخاصة مما يعزز الأمان.
- **تنفيذ التشفير في جميع أنحاء المؤسسة:** تشفير البيانات عبر جميع الأنظمة والتطبيقات وقنوات الاتصال يساعد في الحفاظ على مستوى ثابت من الحماية ويقلل من مخاطر اختراق البيانات.

الاستجابة للحوادث واستعادة الوضع بعد الكوارث



- **وضع خطة استجابة للحوادث:** وجود خطة موثقة للاستجابة لحوادث الأمان يساعد في تقليل تأثير الاختراقات وضمان استجابة منسقة وفعالة.
- **إنشاء خطة استعادة الوضع من الكوارث:** التخطيط للانقطاعات المحتملة، مثل الهجمات السيبرانية، والكوارث الطبيعية، أو فشل المعدات، يضمن استمرارية الأعمال ويمكن من استعادة الأنظمة والبيانات الحيوية في الوقت المناسب.
- **أهمية الاختبار والتحديث الدوري:** اختبار وتحديث الخطط للاستجابة للحوادث واستعادة الوضع بعد الكوارث بانتظام يساعد في تحديد ومعالجة الفجوات في التأهب، مما يضمن قدرة المؤسسة على الاستجابة والاسترداد بفعالية من حوادث الأمان.

الامتثال والمتطلبات التنظيمية والقانونية

- **نظرة عامة على التشريعات الخاصة بالصناعة:** اعتمادًا على الصناعة والموقع الجغرافي، قد تكون الشركات خاضعة لقوانين حماية البيانات واللوائح المختلفة، مثل GDPR، HIPAA، أو PCI DSS.
- **أهمية الامتثال لتجنب الغرامات والعقوبات:** يمكن أن يؤدي عدم الامتثال لمتطلبات التنظيم إلى غرامات مالية كبيرة، ومسؤوليات قانونية، وضرر لسمعة الشركة؛ وتنفيذ برامج الامتثال القوية يساعد في تقليل هذه المخاطر ويظهر الالتزام بحماية بيانات وخصوصية العملاء.

شكراً لكم

جمهورية مصر العربية
الجهاز المركزي للمحاسبات

مقدمة عن حوكمة نظم المعلومات

هدف الجلسة

سيتمكن المشاركون في نهاية الجلسة من:

- ❑ التعرف على مفهوم حوكمة نظم المعلومات
- ❑ التعرف على مبادئ وأطر عمل حوكمة نظم المعلومات
- ❑ التعرف على مكونات حوكمة نظم المعلومات
- ❑ التعرف على التحديات التي تواجه حوكمة نظم المعلومات

المحتويات

- مقدمة
- مبادئ حوكمة نظم المعلومات
- اطر عمل حوكمة نظم المعلومات
- ممارسات تطبيق حوكمة نظم المعلومات وأمثلة عليها
- مكونات حوكمة نظم المعلومات
- تحسين وتطوير حوكمة نظم المعلومات
- تحديات تطبيق حوكمة نظم المعلومات وطرق مواجهتها
- الاتجاهات المستقبلية لحوكمة نظم المعلومات

مقدمة

- تعريف حوكمة نظم المعلومات
- أهداف حوكمة نظم المعلومات
- مخاطر عدم تطبيق حوكمة نظم المعلومات

تعريف حوكمة نظم المعلومات

هي عبارة عن عملية تهدف إلى ضمان أن أنظمة المعلومات داخل المؤسسات تعمل بكفاءة وفعالية وتتوافق مع معايير الأمان والخصوصية.

أهداف حوكمة نظم المعلومات

وتتمثل هذه الأهداف في :

- **الاستخدام الفعال لنظم المعلومات:** تهدف حوكمة نظم المعلومات إلى ضمان استخدام نظم المعلومات لتحقيق أهداف المنظمة.
- **الإدارة الفعالة لنظم المعلومات:** تهدف حوكمة نظم المعلومات إلى ضمان إدارة نظم المعلومات بشكل فعال وكفء.
- **سلامة البيانات وسرية المعلومات:** تهدف حوكمة نظم المعلومات إلى ضمان سلامة البيانات وسرية المعلومات وعدم الوصول غير المسموح به للبيانات.
- **الاستخدام المسؤول والأخلاقي لنظم المعلومات:** تهدف حوكمة نظم المعلومات إلى ضمان استخدام نظم المعلومات بشكل مسؤول وأخلاقي.

مبادئ حوكمة نظم المعلومات

1. الشفافية والمساءلة.
2. توثيق السياسات والإجراءات.
3. تحديد الأدوار والمسؤوليات.
4. الامتثال للمعايير واللوائح.
5. تقييم المخاطر وإدارة الأمانات.
6. تقارير ومتابعة الأداء.
7. التعلم المستمر والتحسين المستمر.

أطر عمل حوكمة نظم المعلومات

تهدف أطر عمل حوكمة نظم المعلومات إلى تحسين إدارة وتنظيم نظم المعلومات في المؤسسات. كما أنها تعتبر أداة هامة لضمان تحقيق أهداف الحوكمة وضمان توافق النظم مع المعايير الدولية والمحلية. وتساعد هذه الأطر القياسية على تحسين كفاءة وفعالية استخدام تكنولوجيا المعلومات في تحقيق أهداف المؤسسة.

من بين الأطر القياسية الشهيرة :

- إطار عمل COBIT
- إطار عمل ITIL
- إطار عمل ISO/IEC 27001

أطر عمل حوكمة نظم المعلومات

وجه المقارنة	COBIT	ISO 27001	ITIL
التركيز	إطار عمل موجه نحو الأعمال يحكم محاذاة تكنولوجيا المعلومات مع أهداف العمل. يركز على أهداف التحكم لعمليات موارد تكنولوجيا المعلومات.	معيار دولي يحدد أفضل الممارسات لتنفيذ نظام إدارة أمن المعلومات (ISMS) لإدارة مخاطر أمن المعلومات.	مجموعة من أفضل الممارسات لتقديم خدمات تكنولوجيا المعلومات بشكل فعال وكفء. تركز على دورة حياة خدمات تكنولوجيا المعلومات، من التصميم والتطوير إلى التسليم والدعم.
الجمهور المستهدف	يستهدف في المقام الأول متخصصي حوكمة تكنولوجيا المعلومات ومديري الأعمال والمراجعين المهتمين بمواءمة تكنولوجيا المعلومات مع استراتيجيات العمل.	يستهدف المؤسسات من جميع الأحجام التي تسعى إلى إنشاء نظام إدارة أمن معلومات قوي.	موجهة نحو مزودي خدمات تكنولوجيا المعلومات والفرق الداخلية لتكنولوجيا المعلومات التي تسعى إلى تحسين طريقة تقديم خدمات تكنولوجيا المعلومات إلى عملائها أو مستخدميها.

تابع أطر عمل حوكمة نظم المعلومات

وجه المقارنة	COBIT	ISO 27001	ITIL
الجوانب الأساسية	▪ يوفر إطارًا بأهداف تحكم ونماذج نضج العمليات وإرشادات التنفيذ لحوكمة عمليات تكنولوجيا المعلومات وضمان التوافق مع أهداف العمل. ▪ يركز على ممارسات الحوكمة الرشيدة ويساعد على سد الفجوة بين تكنولوجيا المعلومات والأعمال.	▪ يحدد متطلبات إنشاء وتنفيذ وصيانة وتحسين نظام إدارة أمن المعلومات (ISMS) باستمرار. ▪ يساعد المؤسسات على تحديد مخاطر أمن المعلومات، وتنفيذ ضوابط لتخفيف تلك المخاطر، وضمان سرية وسلامة وتوافر أصول المعلومات.	▪ تقدم مجموعة من أفضل الممارسات لإدارة خدمات تكنولوجيا المعلومات، بما في ذلك تصميم الخدمة، وترحيل الخدمة، وتشغيل الخدمة، والتحسين المستمر للخدمة (CSI). ▪ يركز على العملاء وتحسين العمليات وتقديم خدمات تكنولوجيا المعلومات عالية الجودة.
الامتثال مقابل أفضل الممارسات	ليس معيارٌ للالتزام؛ بل يقدم أفضل الممارسات وإرشادات لحوكمة تكنولوجيا المعلومات.	معيار دولي معترف به يمكن للمؤسسات الحصول على شهادة له من خلال إثبات الامتثال لمتطلباته.	مجموعة من أفضل الممارسات؛ يمكن للمؤسسات تبني مبادئ أفضل دون الحاجة إلى اعتماد رسمي.

تابع أطر عمل حوكمة نظم المعلومات

العلاقة بين تلك الأطر

* يمكن أن يكون COBIT وITIL مكملين لبعضهما البعض؛ ويمكن أن يساعد COBIT في ضمان محاذاة خدمات تكنولوجيا المعلومات مع أهداف العمل، بينما يقدم ITIL إرشادات حول كيفية تقديم تلك الخدمات بشكل فعال.

* يمكن دمج ISO 27001 مع كل من COBIT وITIL ؛ ويمكن لنظام إدارة أمن المعلومات المطبق وفقًا لـ ISO 27001 الاستفادة من الضوابط التي يقترحها COBIT،كما يمكن تأمين عمليات إدارة خدمات تكنولوجيا المعلومات المحددة من قبل ITIL باتباع متطلبات ISO 27001.

باختصار

- اختر(COBIT) إذا كنت ترغب في تحسين حوكمة تكنولوجيا المعلومات، وضمان محاذاة تكنولوجيا المعلومات مع أهداف العمل، وسد الفجوة بين تكنولوجيا المعلومات والأعمال.
- اختر(ISO 27001) إذا كنت ترغب في إنشاء نظام إدارة أمن معلومات قوي وتحقيق الامتثال لمعيار معترف به.
- اختر(ITIL) إذا كنت ترغب في تحسين طريقة تقديم خدمات تكنولوجيا المعلومات إلى عملائك أو مستخدمينك.

ممارسات تطبيق حوكمة نظم المعلومات وأمثلة عليها

تطبيق ممارسات الحوكمة في نظم المعلومات يتطلب ما يلي:

- تحديد الأدوار والمسؤوليات الخاصة بإدارة المعلومات داخل المؤسسة.
- يجب تحديد المسارات التنظيمية وتوزيع الصلاحيات بشكل واضح لضمان تنفيذ السياسات والإجراءات بشكل صحيح.
- كما يجب توفير التدريب المناسب للموظفين لضمان فهمهم لأهمية الحوكمة وكيفية تطبيقها بشكل صحيح باعتبارها جزءًا أساسيًا من استراتيجية الأعمال العامة للمؤسسة.

أمثلة على ممارسات تطبيق حوكمة نظم المعلومات

1. تشكيل لجنة توجيهية مكونة من كبار المديرين التنفيذيين من مختلف الإدارات للإشراف على مشاريع واستثمارات تكنولوجيا المعلومات. ستقوم هذه اللجنة بمراجعة المقترحات وتحديد أولويات المبادرات والتأكد من توافق استثمارات تكنولوجيا المعلومات مع أهداف العمل الشاملة.
2. تنفيذ عملية رسمية لتقييم واعتماد مشاريع تكنولوجيا المعلومات، بما في ذلك معايير تقييم المخاطر والتكاليف والفوائد. ستساعد هذه العملية على ضمان تخصيص الموارد للمشاريع التي تتمتع بأعلى إمكانية لإضافة قيمة إلى المنظمة.
3. إنشاء إطار حوكمة يحدد بوضوح الأدوار والمسؤوليات المتعلقة باتخاذ القرار في مجال تكنولوجيا المعلومات، مثل تعيين رئيس قسم المعلومات (CIO) لقيادة استراتيجية تكنولوجيا المعلومات ورئيس قسم التكنولوجيا (CTO) للإشراف على التنفيذ الفني. ويساعد هذا الهيكل على ضمان المساءلة ومنع التضارب حول أولويات تكنولوجيا المعلومات.

تابع أمثلة على ممارسات تطبيق حوكمة نظم المعلومات

4. إنشاء آليات مراقبة وإعداد تقارير منتظمة لتتبع أداء استثمارات ومشاريع تكنولوجيا المعلومات، مثل مؤشرات الأداء الرئيسية (KPIs) المتعلقة بالجداول الزمنية للمشروع، والالتزام بالموازنة، والنتائج. تسمح هذه البيانات للمؤسسات بتصحيح المسار حسب الحاجة واتخاذ قرارات مستنيرة بشأن الاستثمارات المستقبلية في تكنولوجيا المعلومات.

5. إجراء عمليات تدقيق منتظمة لتكنولوجيا المعلومات لتقييم الامتثال لسياسات تكنولوجيا المعلومات واللوائح وأفضل الممارسات. ويساعد ذلك على ضمان استخدام موارد تكنولوجيا المعلومات بطريقة آمنة وفعالة، مما يقلل من مخاطر اختراق البيانات أو الاضطرابات التشغيلية.

مكونات حوكمة نظم المعلومات

تشير حوكمة تكنولوجيا المعلومات إلى الإطار والعمليات المستخدمة لضمان توافق استثمارات ومبادرات تكنولوجيا المعلومات مع أهداف المنظمة واستراتيجياتها. وتتضمن ما يلي:

- السياسات والإجراءات والضوابط لإدارة وضبط استخدام موارد تكنولوجيا المعلومات بشكل فعال داخل المنظمة. وتساعد حوكمة تكنولوجيا المعلومات على ضمان اتخاذ قرارات تكنولوجيا المعلومات بطريقة تدعم الأهداف العامة للمنظمة وتساعد على تخفيف المخاطر المرتبطة بعمليات تكنولوجيا المعلومات.
- إنشاء أدوار ومسؤوليات واضحة داخل المنظمة؛ ويتضمن ذلك تحديد أدوار لجان حوكمة تكنولوجيا المعلومات، مثل اللجنة التوجيهية لتكنولوجيا المعلومات، المسؤولة عن تحديد أولويات تكنولوجيا المعلومات واتخاذ القرارات بشأن استثمارات تكنولوجيا المعلومات.

تابع مكونات حوكمة نظم المعلومات

- تحديد أدوار إدارة تكنولوجيا المعلومات وموظفيها، والتأكد من وجود مسؤولية واضحة عن القرارات والإجراءات المتعلقة بتكنولوجيا المعلومات. ومن خلال تحديد الأدوار والمسؤوليات بوضوح، يمكن للمؤسسات ضمان توافق مبادرات تكنولوجيا المعلومات مع أهداف العمل الشاملة.
- إنشاء آليات فعالة للاتصالات وإعداد التقارير. يتضمن ذلك ضمان وجود اتصالات منتظمة بين تكنولوجيا المعلومات وأصحاب المصلحة في الأعمال، بحيث يتم إعلام كلا المجموعتين بمبادرات تكنولوجيا المعلومات والتقدم والتحديات. كما يتضمن إنشاء آليات إعداد التقارير لرصد وتقييم أداء استثمارات ومشاريع تكنولوجيا المعلومات. من خلال وجود آليات اتصال وإعداد تقارير واضحة، يمكن للمؤسسات ضمان اتخاذ قرارات تكنولوجيا المعلومات بناءً على معلومات دقيقة وفي الوقت المناسب، وأن هناك شفافية في عملية حوكمة تكنولوجيا المعلومات.

تحسين وتطوير حوكمة نظم المعلومات

تقييم أداء حوكمة نظم المعلومات يعتبر جزءًا أساسيًا من عملية تحسين الحوكمة في أي منظمة. وذلك عن طريق :

- تقييم كيفية إدارة وتنظيم البيانات والمعلومات داخل المؤسسة، ومدى فعالية هذه العمليات في تحقيق أهداف المنظمة.
- فحص السياسات والإجراءات المتبعة في إدارة المعلومات وتحليل مدى توافقها مع المعايير الدولية والمتطلبات القانونية .يعتمد تقييم أداء حوكمة نظم المعلومات على عدة مؤشرات وقواعد بيانات لقياس جودة وفعالية الإجراءات المتبعة.
- تحليل استراتيجيات النمو والتطوير لضمان مواكبة التكنولوجيا الحديثة وتحقيق الابتكار والتميز التنافسي بناءً على نتائج تقييم أداء حوكمة نظم المعلومات.

تحسين وتطوير حوكمة نظم المعلومات

- تحليل أداء نظم الحماية والأمان السيبراني لضمان سلامة المعلومات، وكذلك تقييم العمليات المتبعة في إدارة البيانات وضمان سريتها وسلامتها.
- يتم اقتراح تحسينات وتطويرات لتعزيز كفاءة وفعالية إدارة المعلومات داخل المؤسسة. يمكن أن تتضمن هذه التحسينات تطوير نظم التخزين والاسترجاع لتسهيل الوصول إلى المعلومات، وتعزيز سياسات الحماية والأمان للوقاية من الاختراقات السيبرانية، وتطوير استراتيجيات إدارة البيانات لتحقيق أقصى استفادة منها. يعتبر تقييم أداء حوكمة نظم المعلومات عملية مستمرة وضرورية لضمان استمرارية النجاح والتطور في العصر الرقمي الحديث.

تحديات تطبيق حوكمة نظم المعلومات وطرق مواجهتها

يمكن أن تشمل الأمثلة الملموسة للتحديات التي تواجه حوكمة تكنولوجيا المعلومات ما يلي:

1. تكامل التقنيات الجديدة: تقرر إحدى المنظمات تنفيذ خدمات الحوسبة السحابية لتحسين الكفاءة وخفض التكاليف. ومع ذلك، يتطلب هذا التغيير مراجعة وتعديل إطار حوكمة تكنولوجيا المعلومات لضمان دمج التكنولوجيا الجديدة بسلاسة وأمان في الأنظمة الحالية.

2. تهديدات الأمن السيبراني: تتعرض إحدى الشركات لاختراق بيانات بسبب هجوم سيبراني، مما يسلط الضوء على أهمية تقييم وتحديث التدابير الأمنية كجزء من حوكمة تكنولوجيا المعلومات. يجب على المنظمة الاستثمار في بروتوكولات أمنية أقوى ومراقبة نقاط الضعف المحتملة بانتظام.

تحديات تطبيق حوكمة نظم المعلومات وطرق مواجهتها

3. الامتثال للوائح: تم تقديم لائحة جديدة لحماية البيانات، مما يؤثر على كيفية قيام المؤسسة بتخزين بيانات العملاء ومعالجتها. يجب على المتخصصين في حوكمة تكنولوجيا المعلومات التأكد من أن المنظمة تظل متوافقة مع هذه اللوائح، الأمر الذي قد يتضمن مراجعة السياسات والإجراءات لتلبية المتطلبات الجديدة.

4. قرارات الاستثمار في تكنولوجيا المعلومات: يقترح قسم تكنولوجيا المعلومات استثمارًا كبيرًا في نظام برمجي جديد يعد بتبسيط العمليات. يجب على المتخصصين في حوكمة تكنولوجيا المعلومات تقييم الفوائد والمخاطر المحتملة لهذا الاستثمار، ومواءمته مع الأهداف الاستراتيجية للمنظمة والتأكد من أنه يقدم قيمة على المدى الطويل.

تحديات تطبيق حوكمة نظم المعلومات وطرق مواجهتها

للتغلب على هذه التحديات، يمكن للمنظمات:

1. تخصيص الموارد الكافية لبرامج التدريب والتوعية للموظفين بأهمية حوكمة نظم المعلومات وكيفية تنفيذها بالشكل الصحيح.
2. وضع سياسات وإجراءات صارمة لضمان الالتزام بالمعايير الأمنية وحماية المعلومات الحساسة.
3. تعزيز ثقافة الحوكمة داخل المنظمة من خلال دعم القيادة العليا وتعزيز تنفيذ ممارسات الحوكمة على جميع المستويات.

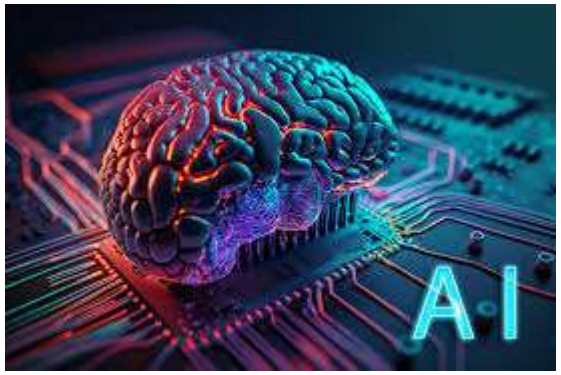
الاتجاهات المستقبلية لحوكمة نظم المعلومات

يُتوقع أن تشهد حوكمة نظم المعلومات العديد من التغييرات في المستقبل، ومن أهم هذه التغييرات:

- الذكاء الاصطناعي .
- التقنيات الناشئة .
- حماية البيانات والأمن السيبراني .
- الاستدامة والأخلاقيات .

تابع الاتجاهات المستقبلية لحوكمة نظم المعلومات

الذكاء الاصطناعى:



- أتمتة المهام الروتينية مثل جمع البيانات وتحليلها.
- اكتشاف المخاطر والتنبؤ بها.
- تحسين كفاءة وفعالية حوكمة نظم المعلومات.

التقنيات الناشئة:

استخدام إنترنت الأشياء لمراقبة الأصول الرقمية والتحكم فيها.

استخدام البلوك تشين لضمان سلامة البيانات وخصوصيتها.

استخدام تقنية الحوسبة السحابية لتوفير خدمات حوكمة نظم المعلومات بشكل أكثر كفاءة.

تابع الاتجاهات المستقبلية لحوكمة نظم المعلومات

حماية البيانات والأمان السيبراني:

- تطوير استراتيجيات متقدمة لحماية البيانات ومكافحة التهديدات السيبرانية المتطورة.
- تنفيذ تقنيات تشفير متقدمة وأساليب اكتشاف التهديدات في الوقت المناسب.

الاستدامة والأخلاقيات

- تكامل مبادئ الاستدامة والأخلاقيات في إطار الحوكمة الخاص بنظم المعلومات.
- توجيه الاستثمارات نحو تطوير حلول تكنولوجية تحترم الخصوصية وتعزز المسؤولية الاجتماعية.

شكراً لكم

جمهورية مصر العربية
الجهاز المركزي للمحاسبات

تحليل البيانات

هدف الجلسة

سيتمكن المشاركون في نهاية الجلسة من:

- تحديد الأهداف والمعايير لعملية التحليل، مثل الاتجاهات المرغوب في فهمها والمعلومات المطلوب استخراجها من البيانات.
- جمع البيانات اللازمة للتحليل من مصادر مختلفة، مثل قواعد البيانات، والملفات النصية، والمصادر الأخرى.
- استخدام أدوات التحليل المناسبة لفهم البيانات وتحويلها إلى معلومات قيمة.
- التعرف على تقنيات التدقيق بمساعدة الحاسب (CAATs).

المحتويات

مقـــــــدمـــــة

- تحليل البيانات هو الطريقة التي يتم من خلالها اختبار البيانات أو المعلومات، ليساعد على فهمها من خلال تحويل البيانات الخام إلى معلومات قابلة للاستخدام وذات معنى.
- تحليل البيانات يلعب دورًا حاسمًا في عملية التدقيق، سواء كان ذلك في مجال التدقيق المالي، والإداري، أو تدقيق نظم المعلومات او أي نوع آخر من أنواع التدقيق.

مراحل عملية تحليل البيانات

مرحلة التخطيط	مرحلة الإعداد	مرحلة الاختبار	مرحلة ما بعد الاختبار
• فهم البيانات. • تحديد أهداف الفحص. • بناء ملف للأخطاء المحتملة. • تحديد ما إذا كان هناك دليل مبدئي.	• تحديد البيانات ذات الصلة. • الحصول على البيانات. • التحقق من صحة البيانات. • تنظيف البيانات وتطبيعها	• تحليل البيانات.	• الاستجابة لنتائج التحليل. • مراقبة البيانات.

الوظائف الأساسية لبرمجيات تحليل البيانات

تنظيم وإدارة البيانات

- **الفرز والفهرسة:** ترتيب البيانات بكفاءة لسهولة الوصول.
- **اختيار السجلات:** تصفية البيانات بناءً على معايير محددة.
- **دمج الملفـــــات:** تجميع البيانات من مصادر مختلفة.
- **المعالجة المتعددة:** إدارة ومعالجة البيانات عبر ملفات متعددة في وقت واحد.

الوظائف الأساسية لبرمجيات تحليل البيانات

Sample Customer Sales Data

Date	Customer	Invoice	Amount
3/12/20X6	V45892	J54534	$10,000
4/8/20X6	V45892	J54535	$10,000
5/7/20X6	V78293	J70384	$15,698
2/8/20X6	V90132	J37234	$85,365
12/15/20X5	V10345	J12853	$47,952
1/8/20X6	V78343	J26487	$52,978

الوظائف الأساسية لبرمجيات تحليل البيانات

Data Sorted by Invoice Number

Date	Customer	Invoice	Amount
12/15/20X5	V10345	J12853	$47,952
1/8/20X6	V78343	J26487	$52,978
2/8/20X6	V90132	J37234	$85,365
3/12/20X6	V45892	J54534	$10,000
4/8/20X6	V45892	J54535	$10,000
5/7/20X6	V78293	J70384	$15,698

الوظائف الأساسية لبرمجيات تحليل البيانات

Data Sorted by Amount

Date	Customer	Invoice	Amount
3/12/20X6	V45892	J54534	$10,000
4/8/20X6	V45892	J54535	$10,000
5/7/20X6	V78293	J70384	$15,698
12/15/20X5	V10345	J12853	$47,952
1/8/20X6	V78343	J26487	$52,978
2/8/20X6	V90132	J37234	$85,365

الوظائف الأساسية لبرمجيات تحليل البيانات

1. تقنيات تحليل البيانات

- **تحليل الارتباط:** يُحدد العلاقات بين المتغيرات.
- **تحليل الانحدار:** يُحدد تأثير متغير على آخر.
- **التحليل الإحصائي:** يُجري تقييمات إحصائية شاملة.
- **التصنيف:** يقسم البيانات إلى طبقات محددة للتحليل التفصيلي.
- **الجداول المحورية:** تلخص البيانات الواسعة في شكل مضغوط.

الوظائف الأساسية لبرمجيات تحليل البيانات

الجداول المحورية

Sum of Amount	Country				
Salesperson	CAN	MEX	UK	USA	Grand Total
Carson	$978	$24,613			$25,591
Grant	$7,842		$1,248		$9,090
Hughes	$6,777	$1,203			$7,980
Jamison		$8,596		$5,634	$14,230
Jarrison		$9,785	$4,576	$7,854	$22,215
Miller		$452	$552	$9,809	$10,813
Parsons	$9,846		$2,458		$12,304
Grand Total	**$25,443**	**$44,649**	**$8,834**	**$23,297**	**$102,223**

الوظائف الأساسية لبرمجيات تحليل البيانات

التصنيف الطبقي

Invoice Amount	Count	% of Total	Total Amount
Less than $1,000	87	10.5%	$ 66,078.24
$1,001–$5,000	196	23.6%	$ 782,089.00
$5,001–$10,000	359	43.2%	$ 2,515,940.21
$10,001–$20,000	102	12.3%	$ 1,427,527.74
$20,001–$50,000	68	8.2%	$ 2,022,600.16
Over $50,000	19	2.3%	$ 1,298,874.96
Total:	**831**	**100%**	**$ 8,113,110.31**

الوظائف الأساسية لبرمجيات تحليل البيانات

2. التحقق والامتثال

- **التحقق من الامتثال:** تلبية البيانات للمعايير التنظيمية المحددة.
- **البحث عن النسخ المكررة:** العثور على السجلات المكررة وإزالتها.
- **التحقق من الأرقام:** يفحص أنماطًا رقمية محددة.

الوظائف الأساسية لبرمجيات تحليل البيانات

3. أدوات تحليل البيانات المتقدمة

- **التعبيرات والمعادلات:** تأدية حسابات معقدة.
- **معايير الفلترة والعرض:** عروض مخصصة بناءً على الاحتياجات المحددة.
- **تطابق المنطق الضبابي:** استخدام التقريب المنطقي لمطابقة البيانات.
- **اختبارات الفجوة:** تحديد الفجوات في تسلسل البيانات.
- **تحليل قانون بنفورد:** اكتشاف الانحرافات في البيانات العددية.

الوظائف الأساسية لبرمجيات تحليل البيانات

قانون بينفورد

First Digit	Probability
1	30.1%
2	17.6%
3	12.5%
4	9.7%
5	7.9%
6	6.7%
7	5.8%
8	5.1%
9	4.6%
Total	**100.0%**

الوظائف الأساسية لبرمجيات تحليل البيانات

4. التصوير والتقارير

- **الرسم البياني:** لإنشاء تمثيلات بصرية لاتجاهات البيانات.
- **وظائف التاريخ:** إدارة البيانات المتعلقة بالتاريخ.

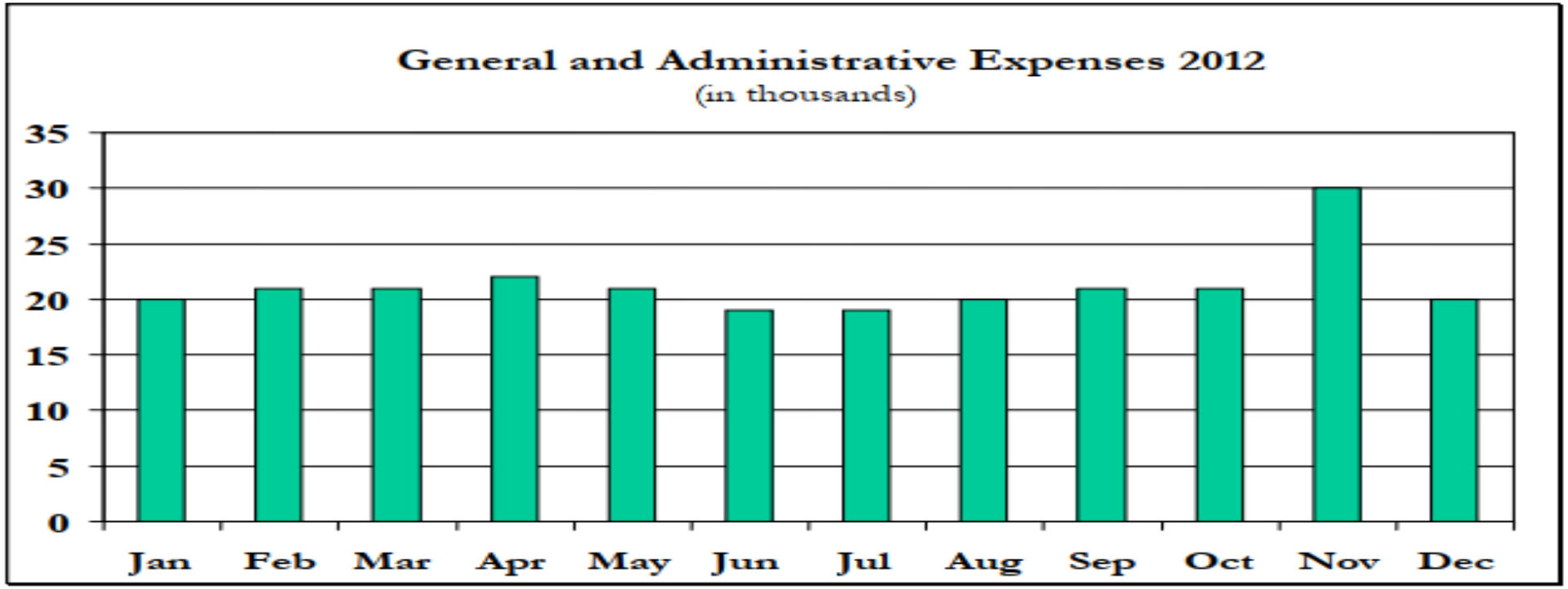
الوظائف الأساسية لبرمجيات تحليل البيانات

وظائف التاريخ

Amounts Outstanding								
Invoice Number	Customer Name	Amount Receivable	Amount Owed	1–30 Days	31–60 Days	61–90 Days	90–120 Days	120+ Days
56987	McClintock Fabrics	$1,250	$250		$250			
45365	ABC Incorporated	$5,250	$650	$650				
78942	Riley's Pest Control	$1,000	$200			$200		
25410	Bob's Lawn Service	$250	$50			$50		
89463	Clean 4 You	$750	$300					$300
97156	XYZ Corporation	$6,250	$1,000				$1,000	

الوظائف الأساسية لبرمجيات تحليل البيانات

الرسومات البيانية



أدوات تحليل البيانات

أدوات تحليل البيانات

- **مايكروسوفت إكسل** هو برنامج جداول بيانات يستخدم على نطاق واسع، ويتميز بقدرته على تنظيم البيانات، وإجراء الحسابات الرياضية، وإنشاء الرسوم البيانية. كما يشمل على دوال متقدمة للتحليل الإحصائي والمالي، ويدعم الجداول المحورية التي تسهل تلخيص البيانات وتحليلها. ويعتبر برنامج Excelمثاليًا للمستخدمين بالمستويات المبتدئة إلى المتوسطة ويعمل بشكل جيد للمشاريع الصغيرة إلى المتوسطة الحجم.

أدوات تحليل البيانات

معايير التطبيق:

- **الوظـائف:** تحليـل بيانـات أساسـي، جـداول محوريـة، دوال إحصـائية ورياضية.
- **سهولة الاستخدام:** يعتبر سهل للمبتدئين.
- **التكامل:** يدمج بسهولة مع برامج Microsoft الأخرى.
- **التحليل:** قدرات محدودة لبيانات كبيرة.
- **التكلفة:** مدرج ضمن حزمة Office.
- **الدعم:** دعم واسع من المجتمع.

أدوات تحليل البيانات

- **مايكروسوفت Power BI** هو أداة تحليل أعمال من مايكروسوفت تتيح تصور البيانات بشكل ديناميكي وإنشاء تقارير تفاعلية. يقدم إمكانيات قوية في دمج البيانات من مصادر مختلفة وتحليلها بطرق متقدمة. يمكن للمستخدمين إنشاء لوحات معلومات تفاعلية تسهل على صانعي القرار الحصول على رؤى عميقة من البيانات. يفضل استخدامه في الشركات التي تحتاج إلى تقارير ديناميكية وتحليلات معمقة.

أدوات تحليل البيانات

معايير التطبيق:

- **الوظائف:** تحليل بيانات متقدم، تصورات ديناميكية، تقارير.
- **سهولة الاستخدام:** واجهة مستخدم جذابة ولكن تحتاج إلى تعلم.
- **التكامل:** ممتاز مع خدمات Azure وOffice.
- **التحليل:** دعم قوي لبيانات كبيرة ومصادر متعددة.
- **التكلفة:** يتطلب اشتراك.
- **الدعم:** دعم قوي ومجتمع نشط.

أدوات تحليل البيانات

- **تـابلو** هـي أداة تصـور بيانـات متقدمـة تُسـتخدم لتحويـل البيانـات الخـام إلـى رؤى سهلة الفهم من خـلال تقـارير ورسـوم بيانيـة تفاعليـة. تـابلو ممتـاز فـي التعامـل مـع كميـات كبيـرة مـن البيانـات ويـوفر مرونـة كبيـرة فـي تصـميم التقـارير والتحلـيلات. يمكنـه الاتصـال بمصـادر بيانـات متعـددة ويـدعم التحليلات البصرية العميقة. يستخدم على نطاق واسع في الشركات الكبيرة والمؤسسات التي تتطلب تحليلات معقدة ومفصلة للبيانات
- يتميز بأنـه من أكثر التطبيقات سهولة للمستخدمين غير المبرمجين الذين يحتاجون إلى إجراء تصوير للبيانات

أدوات تحليل البيانات

معايير التطبيق:

- **الوظائف:** تصورات بيانية متقدمة، تفاعلية عالية.
- **سهولة الاستخدام:** واجهة مستخدم سهلة الاستخدام.
- **التكامل:** جيد مع مصادر بيانات متعددة.
- **التحليل:** قوي في التحليل البصري.
- **التكلفة:** تكلفة عالية نسبيًا.
- **الدعم:** دعم واسع ومجتمع نشط.

أدوات تحليل البيانات

- **لغة R** هي لغة برمجة وبيئة برمجية تستخدم بشكل خاص في التحليل الإحصائي ورسومات البيانات. تتميز R بقدرتها على تنفيذ تحليلات إحصائية معقدة وتوفر مكتبات واسعة لمختلف أنواع التحليل والتعلم الآلي. هي الأداة المفضلة للباحثين والعلماء الذين يحتاجون إلى إجراء تحليلات دقيقة وتطوير نماذج إحصائية.

أدوات تحليل البيانات

معايير التطبيق:

- **الوظائف:** تحليل إحصائي متقدم، موديلات تنبؤية.
- **سهولة الاستخدام:** يتطلب خلفية في البرمجة.
- **التكامل:** جيد مع بيانات وأنظمة متعددة.
- **التحليل:** ممتاز في التحليل الإحصائي والكمي.
- **التكلفة:** مجاني (مفتوح المصدر).
- **الدعم:** مجتمع دعم قوي.

أدوات تحليل البيانات

بايثون

- هي لغة برمجة متعددة الاستخدامات تُستخدم على نطاق واسع في تحليل البيانات، التعلم الآلي، وتطوير التطبيقات.
- تتميز بايثون بمكتباتها القوية ، مثل NumPy، Pandas، و Matplotlib التي تسهل معالجة البيانات، الحسابات الإحصائية، والتصور.
- تُعتبر الخيار الأمثل لمشاريع التحليل التي تتطلب دمج بيانات كبيرة وتطبيقات تعلم آلي متقدمة.

أدوات تحليل البيانات

معايير التطبيق:

- **الوظائف:** تحليل بيانات شامل، معالجة بيانات كبيرة، تعلم آلي.
- **سهولة الاستخدام:** يتطلب بعض المعرفة بالبرمجة.
- **التكامل:** ممتاز مع أدوات وتقنيات متنوعة.
- **التحليل:** متميز في التحليل والتعلم الآلي.
- **التكلفة:** مجاني (مفتوح المصدر).
- **الدعم:** دعم واسع ومجتمع كبير.

أدوات تحليل البيانات

- **Caseware IDEA** هو برنامج متخصص في التدقيق وتحليل البيانات المالية. يوفر أدوات قوية لفحص البيانات واكتشاف التناقضات والأخطاء في السجلات المالية. يُستخدم بشكل خاص من قبل المدققين والمحاسبين لتسهيل تدقيق الحسابات وتحليل الامتثال. يتميز بقدرته على التعامل مع كميات كبيرة من البيانات وتقديم تقارير مفصلة حول النتائج.

أدوات تحليل البيانات

معايير التطبيق:

- **الوظائف:** تحليلات مالية متخصصة، تدقيق.
- **سهولة الاستخدام:** يتطلب خبرة في المجال المالي.
- **التكامل:** جيد مع برامج المحاسبة.
- **التحليل:** قوي في تحليل المعاملات والتدقيق.
- **التكلفة:** مرتفعة نسبيًا.
- **الدعم:** دعم متخصص.

أدوات تحليل البيانات

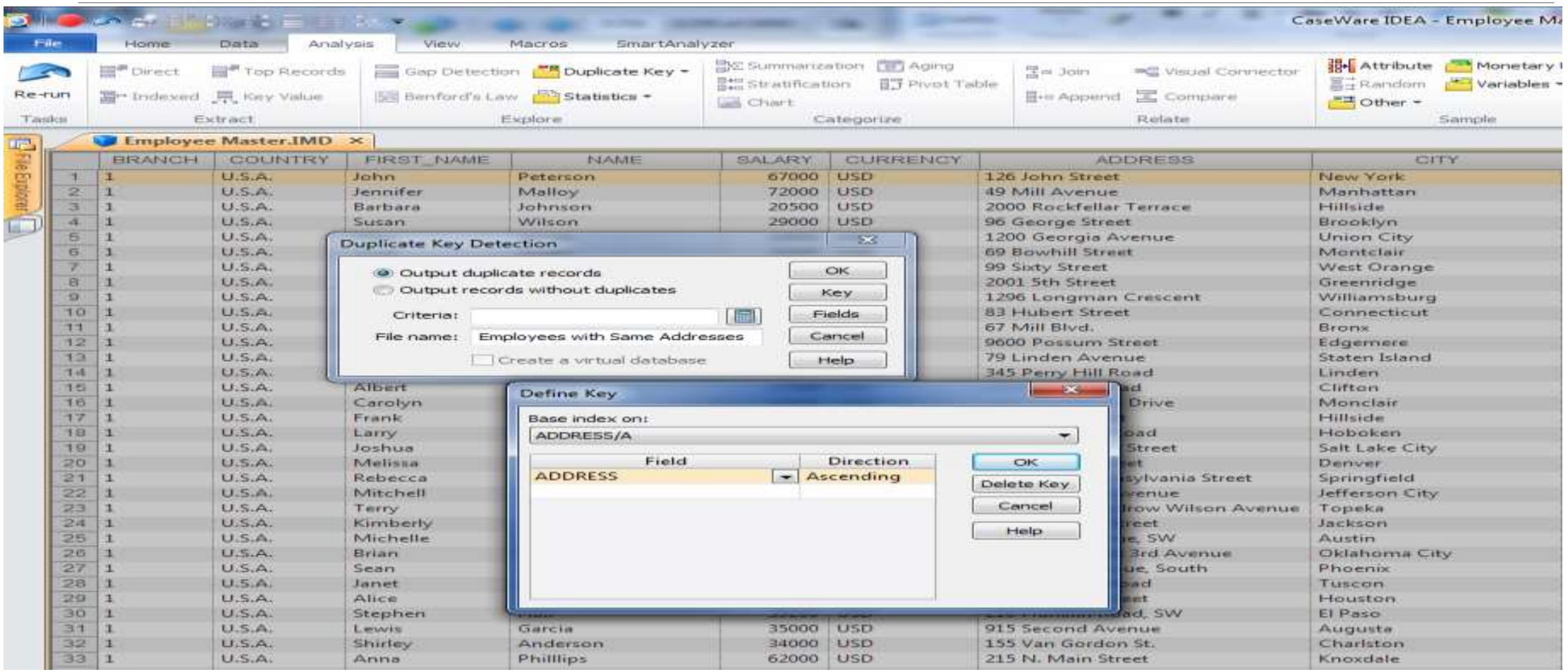
- ACL هو برنامج يستخدم في تحليل المخاطر والتدقيق ومراقبة الامتثال. يوفر أدوات لتحليل البيانات تساعد في الكشف عن الاحتيال وإدارة المخاطر وضمان الامتثال التنظيمي. ACL يدعم الشركات في إنشاء بيئات تدقيق شاملة وفعالة من حيث التكلفة، وهو مثالي للمؤسسات الكبيرة التي تحتاج إلى مراقبة دقيقة لأنشطتها المالية والتشغيلية.

أدوات تحليل البيانات

معايير التطبيق:

- **الوظائف:** تحليل مخاطر، تدقيق، مراقبة الامتثال.
- **سهولة الاستخدام:** متخصص ويحتاج لتدريب.
- **التكامل:** يدمج بشكل جيد مع أنظمة ERP.
- **التحليل:** ممتاز في تحليل الامتثال والمخاطر.
- **التكلفة:** مرتفعة.
- **الدعم:** دعم متخصص ومجتمع نشط.

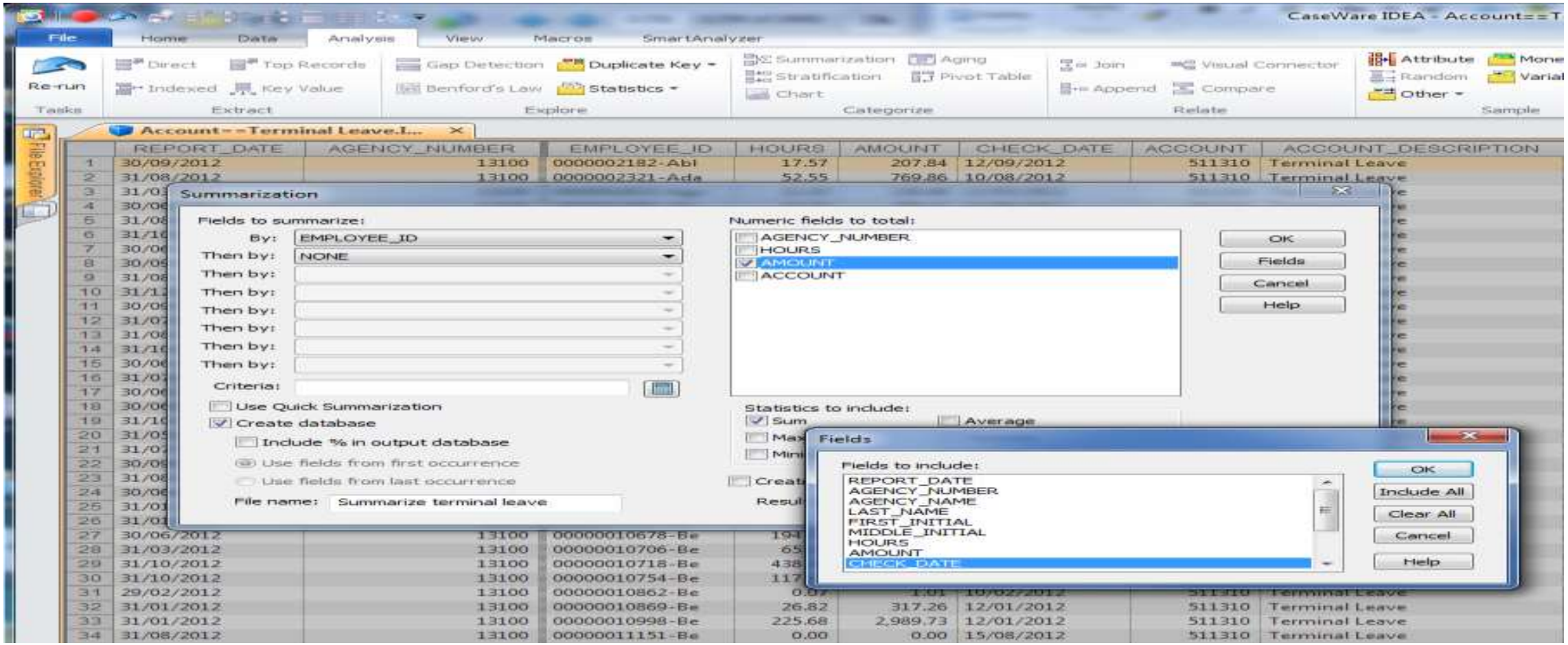
مثال : باستخدام برنامج IDEA



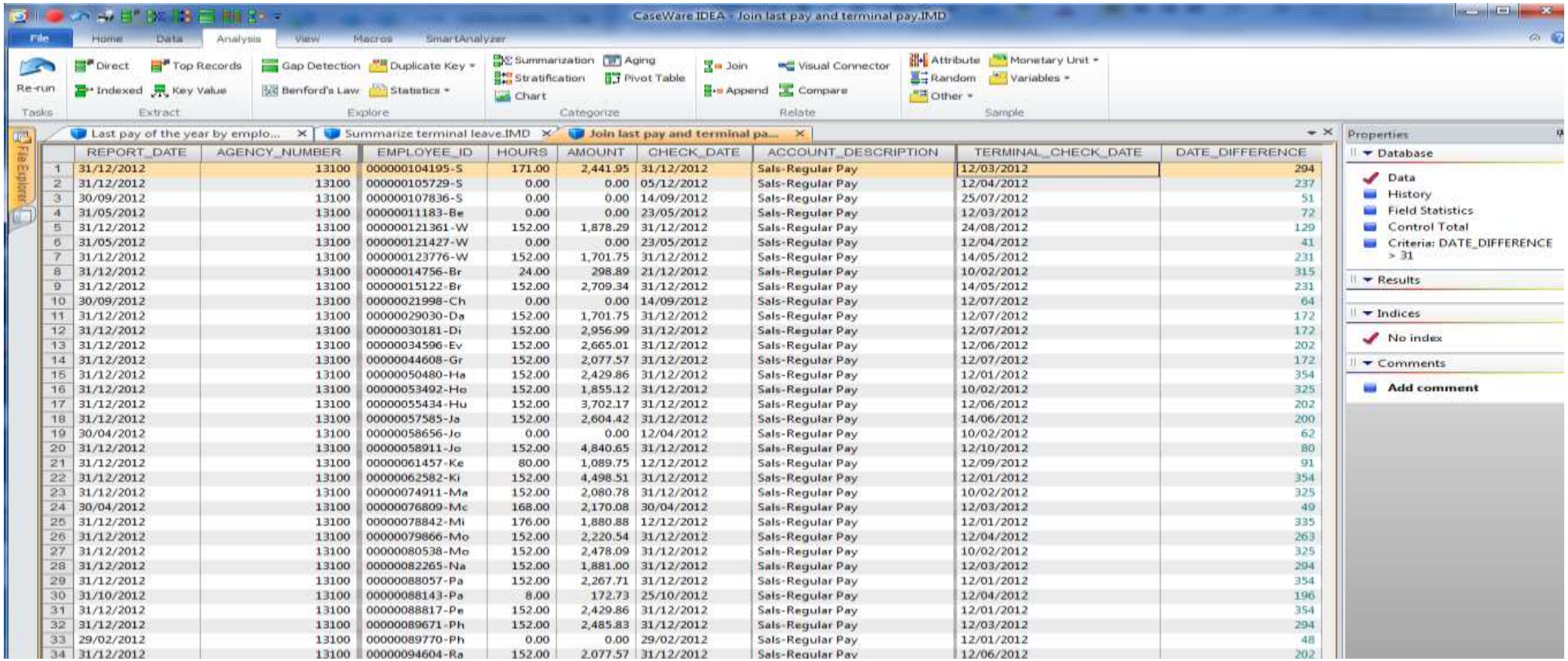
مثال : باستخدام برنامج IDEA

	BRANCH	COUNTRY	FIRST_NAME	NAME	SALARY	CURRENCY	ADDRESS	CITY
1	3	China	Zhang	Chu	360000	CHY	1469 Huaihai Zhonglu	Shanghai
2	3	China	Liu	He	190000	CHY	1469 Huaihai Zhonglu	Shanghai
3	1	U.S.A.	Alice	Saunders	19567	USD	215 N. Main Street	Houston
4	1	U.S.A.	Anna	Phillips	62000	USD	215 N. Main Street	Knoxdale
5	3	China	Yzhi	Le	600000	CHY	313 Mid-Changjiang Road	Hefei
6	3	China	Wu	Niu	240000	CHY	313 Mid-Changjiang Road	Heifei
7	2	Germany	Lea	Wagner	54000	EUR	Im Mühlenbruch 6	Georgsmarienhütte
8	2	Germany	Leon	Newmann	37028	EUR	Im Mühlenbruch 6	Dueren

مثال : باستخدام برنامج IDEA

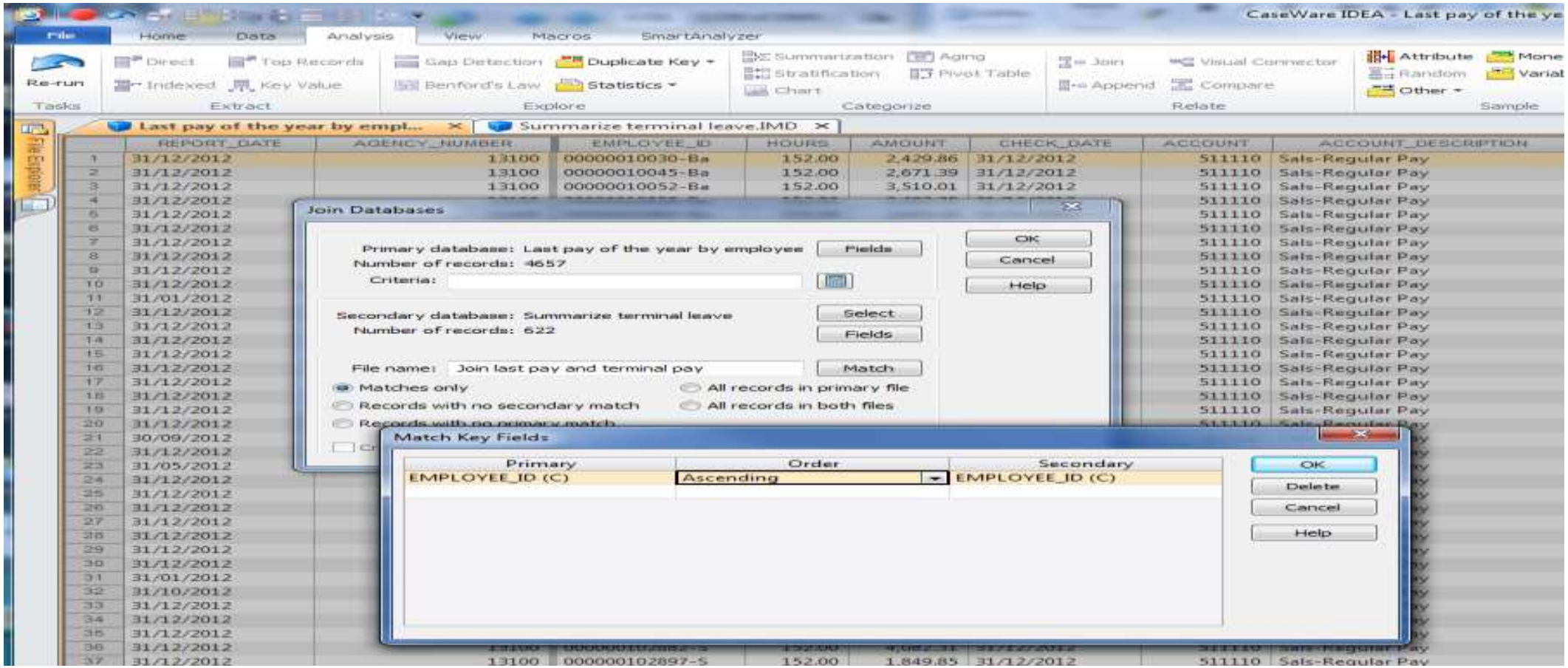


مثال : باستخدام برنامج IDEA



	REPORT_DATE	AGENCY_NUMBER	EMPLOYEE_ID	HOURS	AMOUNT	CHECK_DATE	ACCOUNT_DESCRIPTION	TERMINAL_CHECK_DATE	DATE_DIFFERENCE
1	31/12/2012	13100	000000104195-S	171.00	2,441.95	31/12/2012	Sals-Regular Pay	12/03/2012	294
2	31/12/2012	13100	000000105729-S	0.00	0.00	05/12/2012	Sals-Regular Pay	12/04/2012	237
3	30/09/2012	13100	000000107836-S	0.00	0.00	14/09/2012	Sals-Regular Pay	25/07/2012	51
4	31/05/2012	13100	00000011183-Be	0.00	0.00	23/05/2012	Sals-Regular Pay	12/03/2012	72
5	31/12/2012	13100	000000121361-W	152.00	1,878.29	31/12/2012	Sals-Regular Pay	24/08/2012	129
6	31/05/2012	13100	000000121427-W	0.00	0.00	23/05/2012	Sals-Regular Pay	12/04/2012	41
7	31/12/2012	13100	000000123776-W	152.00	1,701.75	31/12/2012	Sals-Regular Pay	14/05/2012	231
8	31/12/2012	13100	00000014756-Br	24.00	298.89	21/12/2012	Sals-Regular Pay	10/02/2012	315
9	31/12/2012	13100	00000015122-Br	152.00	2,709.34	31/12/2012	Sals-Regular Pay	14/05/2012	231
10	30/09/2012	13100	00000021998-Ch	0.00	0.00	14/09/2012	Sals-Regular Pay	12/07/2012	64
11	31/12/2012	13100	00000029030-Da	152.00	1,701.75	31/12/2012	Sals-Regular Pay	12/07/2012	172
12	31/12/2012	13100	00000030181-Di	152.00	2,956.99	31/12/2012	Sals-Regular Pay	12/07/2012	172
13	31/12/2012	13100	00000034596-Ev	152.00	2,665.01	31/12/2012	Sals-Regular Pay	12/06/2012	202
14	31/12/2012	13100	00000044608-Gr	152.00	2,077.57	31/12/2012	Sals-Regular Pay	12/07/2012	172
15	31/12/2012	13100	00000050480-Ha	152.00	2,429.86	31/12/2012	Sals-Regular Pay	12/01/2012	354
16	31/12/2012	13100	00000053492-Ho	152.00	1,855.12	31/12/2012	Sals-Regular Pay	10/02/2012	325
17	31/12/2012	13100	00000055434-Hu	152.00	3,702.17	31/12/2012	Sals-Regular Pay	12/06/2012	202
18	31/12/2012	13100	00000057585-Ja	152.00	2,604.42	31/12/2012	Sals-Regular Pay	14/06/2012	200
19	30/04/2012	13100	00000058656-Jo	0.00	0.00	12/04/2012	Sals-Regular Pay	10/02/2012	62
20	31/12/2012	13100	00000058911-Jo	152.00	4,840.65	31/12/2012	Sals-Regular Pay	12/10/2012	80
21	31/12/2012	13100	00000061457-Ke	80.00	1,089.75	12/12/2012	Sals-Regular Pay	12/09/2012	91
22	31/12/2012	13100	00000062582-Ki	152.00	4,498.51	31/12/2012	Sals-Regular Pay	12/01/2012	354
23	31/12/2012	13100	00000074911-Ma	152.00	2,080.78	31/12/2012	Sals-Regular Pay	10/02/2012	325
24	30/04/2012	13100	00000076809-Mc	168.00	2,170.08	30/04/2012	Sals-Regular Pay	12/03/2012	49
25	31/12/2012	13100	00000078842-Mi	176.00	1,880.88	12/12/2012	Sals-Regular Pay	12/01/2012	335
26	31/12/2012	13100	00000079866-Mo	152.00	2,220.54	31/12/2012	Sals-Regular Pay	12/04/2012	263
27	31/12/2012	13100	00000080538-Mo	152.00	2,478.09	31/12/2012	Sals-Regular Pay	10/02/2012	325
28	31/12/2012	13100	00000082265-Na	152.00	1,881.00	31/12/2012	Sals-Regular Pay	12/03/2012	294
29	31/12/2012	13100	00000088057-Pa	152.00	2,267.71	31/12/2012	Sals-Regular Pay	12/01/2012	354
30	31/10/2012	13100	00000088143-Pa	8.00	172.73	25/10/2012	Sals-Regular Pay	12/04/2012	196
31	31/12/2012	13100	00000088817-Pe	152.00	2,429.86	31/12/2012	Sals-Regular Pay	12/01/2012	354
32	31/12/2012	13100	00000089671-Ph	152.00	2,485.83	31/12/2012	Sals-Regular Pay	12/03/2012	294
33	29/02/2012	13100	00000089770-Ph	0.00	0.00	29/02/2012	Sals-Regular Pay	12/01/2012	48
34	31/12/2012	13100	00000094604-Ra	152.00	2,077.57	31/12/2012	Sals-Regular Pay	12/06/2012	202

مثال : باستخدام برنامج IDEA



تقنيات التدقيق باستخدام الحاسب CAATs

- تقنيات التدقيق باستخدام الحاسب CAATs مفيدة للغاية لتدقيق نظم المعلومات في جمع وتحليل البيانات الكبيرة والمعقدة أثناء عمليات التدقيق في نظم المعلومات. تساعد تقنيات التدقيق باستخدام الحاسب المدقق في جمع الأدلة من بيئات الأجهزة المختلفة والبرمجيات والتنسيقات المختلفة للبيانات والملفات.
- تساعد تقنيات التدقيق باستخدام الحاسب CAATs المراجعين في نظم المعلومات على جمع المعلومات بشكل مستقل.
- يُعتبر مصدر المعلومات المحصلة من خلال تقنيات التدقيق باستخدام الحاسب CAATs أكثر موثوقية.

محاذير استخدام
تقنيات التدقيق باستخدام الحاسب CAATs

يجب على المراجعين أخذ الحيطة التالية أثناء استخدام تقنيات التدقيق باستخدام الحاسب CAATs:

- ضمان سلامة البيانات المستوردة عبر حماية صحتها وسلامتها وسرية البيانات.
- الحصول على موافقة لتثبيت برامج CAATعلى خوادم المدقق.
- الحصول على حق الوصول «القراءة فقط» عند استخدام CAATعلى البيانات في بيئة التشغيل الفعلي.
- يجب تطبيق التحرير/التعديل على نسخة مستقلة من البيانات وضمان سلامة البيانات الأصلية.

محاذير استخدام
تقنيات التدقيق باستخدام الحاسب CAATs

تقنيات التدقيق المستمر

- في تدقيق نظم المعلومات، تعتبر تقنيات التدقيق المستمر أدوات مهمة للغاية. وفيما يلي خمسة من أدوات التدقيق المستمر المستخدمة على نطاق واسع.
- منشأة الاختبار المتكاملة (ITF).
- ملف تدقيق النظام الخاص بالرقابة (SCARF).
- تقنية اللقطة السريعة (SnapShot Technique).
- خطاف التدقيق (Audit Hook).
- المحاكاة المستمرة والمتقطعة (CIS).

محاذير استخدام
تقنيات التدقيق باستخدام الحاسب CAATs

منشأة الاختبار المتكاملة (Integrated Test Facility ITF)

- في منشأة الاختبار المتكاملة ITF، يتم إنشاء كيان وهمي في بيئة الإنتاج.
- على سبيل المثال، باستخدام تقنية ITF، يتم إدخال معاملة اختبارية. تتم مقارنة نتائج معالجة المعاملة الاختبارية مع النتائج المتوقعة لتحديد دقة المعالجة. إذا كانت النتائج المعالجة تتطابق مع النتائج المتوقعة، فهذا يعني أن المعالجة تتم بشكل صحيح. بمجرد اكتمال التحقق، يتم حذف بيانات الاختبار من النظام.

محاذير استخدام
تقنيات التدقيق باستخدام الحاسب CAATs

ملف تدقيق النظام الخاص بالرقابة System Control Audit Review File (SCARF)

- في هذه التقنية، يتم تضمين موديول التدقيق (مدمج) في تطبيق المضيف للمنظمة لتتبع المعاملات بشكل مستمر.
- يُستخدم ملف تدقيق النظام الخاص بالرقابة SCARF للحصول على البيانات أو المعلومات لأغراض التدقيق.
- يقوم SCARF بتسجيل المعاملات التي تتجاوز حدًا محددًا أو المعاملات المتعلقة بالانحرافات أو الاستثناءات. ثم يتم تدقيق هذه المعاملات من قبل المدقق.
- يكون SCARF مفيد عندما لا يمكن ايقاف معالجة البيانات العادية.

محاذير استخدام
تقنيات التدقيق باستخدام الحاسب CAATs

تقنية اللقطة السريعة (SnapShot Technique)

- تلتقط هذه التقنية اللقطات أو الصور للمعاملة أثناء معالجتها في مراحل مختلفة داخل النظام.
- يتم التقاط التفاصيل قبل تنفيذ المعاملة وبعد تنفيذها. يتم التحقق من صحة المعاملة من خلال التحقق من صحة اللقطات قبل المعالجة وبعد المعالجة للمعاملات.
- تكون تقنية اللقطة مفيدة عندما يكون من الضروري وجود سجل تدقيق (Audit Trails).

محاذير استخدام
تقنيات التدقيق باستخدام الحاسب CAATs

خطاف التدقيق .(Audit Hook)

- تُدمج خطافات التدقيق في نظام التطبيق لالتقاط الاستثناءات.
- يمكن للمدقق تحديد معايير مختلفة لالتقاط الاستثناءات أو المعاملات المشبوهة.
- على سبيل المثال، من خلال المراقبة الدقيقة للمعاملات النقدية، يمكن للمدقق تحديد معايير لالتقاط المعاملات النقدية التي تتجاوز 10,000 دولار. ثم يتم تدقيق جميع هذه المعاملات من قبل المدقق لتحديد وجود أي تزوير.
- تكون خطافات التدقيق مفيدة في التعرف المبكر على الانحرافات، مثل الاحتيال أو الخطأ.
- عادةً ما يتم تطبيق خطافات التدقيق عندما تحتاج فقط إلى تقييم المعاملات المختارة.

محاذير استخدام
تقنيات التدقيق باستخدام الحاسب CAATs

المحاكاة المستمرة والمتقطعة (CIS)

- تقوم تقنية المحاكاة المستمرة والمتقطعة CIS بتقليد أو محاكاة معالجة التطبيق الأصلي.
- في هذه التقنية، يقوم المحاكي بتحديد المعاملات وفقًا للمعايير المحددة مسبقًا. ثم يتم تدقيق المعاملات المحددة لمزيد من التحقق والمراجعة.
- تقارن CISالنتائج التي تنتجها مع النتيجة التي ينتجها أنظمة التطبيقات. إذا تم ملاحظة أي اختلافات، يتم تسجيلها في ملف سجل الاستثناءات.

تقنيات التدقيق باستخدام الحاسب CAATs

التقنية	الاستخدام
SCARF	يستخدم في الحالات التي لا يمكن فيها إيقاف العمليات الجارية.
SnapShot	يستخدم الصور واللقطات عندما يتطلب الأمر وجود مسار للمراجعة (Audit Trail).
Audit Hooks	تستخدم في حالات الرغبة في الكشف المبكر عن الغش والأخطاء.
ITF	يتم استخدام بيانات الاختبار في بيئة التشغيل الفعلية.
CIS	تستخدم لاختيار المعاملات بناء على معايير محددة مسبقاً في الأنظمة المعقدة.

شكراً لكم

جمهورية مصر العربية
الجهاز المركزي للمحاسبات

خطة استمرارية العمل (BCP)
وخطة استعادة الأوضاع بعد الكوارث (DRP)

هدف الجلسة

سيتمكن المشاركون في نهاية الجلسة من:

- ❑ التعرف على مفهوم خطة استمرارية الأعمال في المؤسسة
- ❑ التعرف على أهمية خطة استمرارية الأعمال في المؤسسة
- ❑ التعرف على مكونات خطة استمرارية الأعمال
- ❑ الفرق بين خطة استمرارية الأعمال وخطة استعادة الأوضاع بعد الكوارث
- ❑ تطوير خطة استمرارية الأعمال وتنفيذ تحليل تأثير الأعمال
- ❑ التعرف على كل من هدف وقت الاسترداد RTO – هدف نقطة الاسترداد

المحتويات

مقدمة

- لا شك ان الحفاظ على استمرار أعمال المؤسسات من أهم الأولويات التي يجب أن تحافظ عليها تلك المؤسسات.
- الأمر الذي يحتاج إلى الدعم الكامل من الإدارة العليا بالمؤسسة لإنجاح مثل تلك الخطط.

مفهوم خطة استمرارية العمل

مفهوم خطة استمرارية العمل BCP :

- تُعد خطة استمرارية العمل (BCP) جانبًا حاسمًا في استراتيجية إدارة المخاطر لأي مؤسسة. يتضمن إنشاء خطة لضمان استمرار وظائف العمل الأساسية في العمل في حالة وقوع كارثة أو خلل.
- الهدف من BCP هو تقليل تأثير الكارثة على العمليات التجارية والتأكد من إمكانية استعادة الوظائف الحيوية في أسرع وقت ممكن. ويتضمن ذلك تحديد المخاطر المحتملة، ووضع استراتيجيات للتخفيف من تلك المخاطر، ووضع إجراءات للاستجابة للكارثة والتعافي منها.

الجوانب الرئيسية لخطة استمرارية العمل

1- إجراء تقييم المخاطر لتحديد التهديدات المحتملة للمنظمة

ويتضمن ذلك تحليل التأثير المحتمل للكوارث المختلفة، مثل الكوارث الطبيعية أو الهجمات السيبرانية أو فشل المعدات، على عمليات المؤسسة. من خلال فهم المخاطر المحتملة التي تواجهها المؤسسة، يمكن لقادة الأعمال وضع خطة للتخفيف من تلك المخاطر والتأكد من أن الوظائف الحيوية يمكن أن تستمر في حالة وقوع كارثة. وقد يتضمن ذلك تنفيذ أنظمة النسخ الاحتياطي، أو إنشاء مواقع عمل بديلة، أو تطوير خطط اتصال لإبقاء الموظفين على اطلاع أثناء الأزمات.

تابع الجوانب الرئيسية لخطة استمرارية العمل

2- تطوير خطة مفصلة للاستجابة والتعافي.

وتوضح هذه الخطة الخطوات التي يجب اتخاذها للاستجابة لكارثة واستعادة وظائف العمل الهامة. وقد تشمل إجراءات إجلاء الموظفين وتفعيل أنظمة النسخ الاحتياطي والتواصل مع أصحاب المصلحة الرئيسيين. من خلال وجود خطة واضحة، يمكن للمؤسسات الحد من الفوضى والارتباك الذي غالبًا ما يصاحب الكارثة والتأكد من إمكانية استعادة الوظائف الحيوية بسرعة. كما يُعد الاختبار والتحديث المنتظم لخطة استمرارية العمل أمرًا ضروريًا أيضًا لضمان بقائها فعالة وحديثة في مواجهة التهديدات المتطورة.

مفهوم خطة استعادة الأوضاع بعد الكوارث

تُعد خطة التعافي من الكوارث جانبًا حاسمًا في التخطيط لاستمرارية الأعمال، حيث يركز على الاستعداد والتعافي من الكوارث المحتملة التي قد تعطل العمليات التجارية. الهدف من التخطيط للتعافي من الكوارث هو تقليل تأثير الكارثة على المؤسسة والتأكد من أن وظائف العمل الحيوية يمكن أن تستمر في حالة حدوث خلل. يتضمن ذلك تحديد المخاطر المحتملة، ووضع استراتيجيات للتخفيف من تلك المخاطر، ووضع خطة للتعافي السريع واستعادة العمليات في أعقاب وقوع الكارثة.

تابع مفهوم خطة استعادة الأوضاع بعد الكوارث

أحد الجوانب الرئيسية لتخطيط التعافي من الكوارث هو إجراء تقييم للمخاطر لتحديد التهديدات المحتملة للمنظمة. ويتضمن ذلك:

- تحليل احتمالية الكوارث المختلفة وتأثيرها المحتمل، مثل الكوارث الطبيعية أو الهجمات السيبرانية أو فشل المعدات. من خلال فهم المخاطر المحددة التي تواجه المؤسسة، يمكن لها تطوير خطة مستهدفة للتعافي من الكوارث تعالج هذه التهديدات المحتملة وتضمن إمكانية استعادة وظائف الأعمال المهمة بسرعة وفعالية، بالإضافة إلى تحديد المخاطر.
- يتضمن التخطيط للتعافي من الكوارث أيضًا تطوير وتنفيذ استراتيجيات للتخفيف من تلك المخاطر. وقد يشمل ذلك تنفيذ أنظمة النسخ الاحتياطي وحلول تخزين البيانات، وإنشاء بروتوكولات اتصال للموظفين أثناء وقوع الكارثة، وإنشاء خطة مفصلة لكيفية الاستجابة لمختلف أنواع الكوارث والتعافي منها. من خلال التخطيط الاستباقي للكوارث المحتملة وتنفيذ استراتيجيات للتخفيف من تأثيرها، يمكن للمؤسسات تقليل وقت التوقف عن العمل وتقليل الخسائر المالية وحماية سمعتها في حالة وقوع كارثة.

الفرق بين BCP &DRP

تُعد خطة استمرارية العمل (BCP) وخطة التعافي من الكوارث (DRP) عنصرين حاسمين في الاستراتيجية الشاملة للمؤسسة لضمان استمرارية عملياتها في مواجهة الأحداث غير المتوقعة. بينما يهدف كل من BCP وDRP إلى تقليل وقت التوقف عن العمل والحفاظ على الوظائف الأساسية أثناء الأزمات.

الفرق بين BCP &DRP

BCP	DRP
يركز BCP على تحديد المخاطر المحتملة وتطوير الاستراتيجيات لضمان استمرارية المؤسسة.	بينما يتعامل DRP على وجه التحديد مع الجوانب الفنية لاستعادة أنظمة تكنولوجيا المعلومات والبنية التحتية بعد وقوع الكارثة.
BCP هو نهج أكثر شمولاً و يشمل جميع جوانب عمليات المؤسسة، بما في ذلك الموظفين والعمليات والتكنولوجيا. ويتضمن تقييم المخاطر، ووضع استراتيجيات للتخفيف من تلك المخاطر، وتنفيذ التدابير اللازمة لضمان استمرارية الأعمال في حالة حدوث أي انقطاع	يركز DRP بشكل أضيق على أنظمة تكنولوجيا المعلومات والبنية التحتية التي تعتبر بالغة الأهمية لعمليات المؤسسة، ويتضمن إنشاء خطط النسخ الاحتياطي والاسترداد للبيانات والتطبيقات والأجهزة لتقليل تأثير الكارثة على قدرة المؤسسة على العمل.

تابع الفرق بين BCP &DRP

BCP	DRP
يهتم BCP في المقام الأول بالحفاظ على السلامة العامة ومرونة المؤسسة في مواجهة التهديدات المختلفة، مثل الكوارث الطبيعية أو الهجمات السيبرانية أو الخطأ البشري. ويهدف إلى ضمان استمرار وظائف العمل الأساسية دون انقطاع أو استعادتها بسرعة بعد انقطاعها.	يركزDRP بشكل أكبر على الجوانب الفنية لاستعادة أنظمة تكنولوجيا المعلومات والبنية التحتية بعد وقوع الكارثة ويمثل هدفه الرئيسي في تقليل تأثير التعطيل على قدرة المؤسسة على الوصول إلى البيانات والتطبيقات الهامة واستخدامها.

أهمية خطة استمرارية العمل واستعادة الأوضاع بعد الكوارث

تحتاج المؤسسات إلى التخطيط مسبقًا للأحداث غير المتوقعة التي قد تعطل عملياتها. ومن خلال إنشاء خطة لكيفية الاستمرار في العمل أثناء الكوارث مثل الأعاصير أو انقطاع التيار الكهربائي، ويُمكنهم من تقليل التأثير على أعمالهم والحفاظ على سير الأمور بسلاسة. فإن وجود خطة جيدة يُظهر أيضًا للعملاء وغيرهم أن المؤسسة جاهزة لأي شيء ويمكن أن تساعدهم في التميز عن منافسيهم.

مكونات خطة استمرارية العمل واستعادة الأوضاع بعد الكوارث

1- تحديد وظائف العمل الهامة:

يتضمن ذلك إلقاء نظرة شاملة على جميع جوانب المؤسسة وتحديد الوظائف التي تعتبر حاسمة لاستمرار تشغيل الأعمال. ومن خلال تحديد هذه الوظائف الحيوية، يمكن وضع خطة لضمان استمرارها في حالة حدوث أي انقطاع.

2- وضع استراتيجية الاتصال:

في حالة وقوع كارثة، من الضروري أن يكون جميع الموظفين على دراية بما يحدث وما هي الخطوات التي يجب اتخاذها لضمان استمرار المؤسسة في العمل. ويجب أن تحدد استراتيجية الاتصال كيفية نشر المعلومات للموظفين والعملاء وأصحاب المصلحة الآخرين، وكذلك كيفية ضمان بقاء قنوات الاتصال مفتوحة أثناء الأزمة. فمن خلال وجود استراتيجية اتصال واضحة، يمكن للمؤسسة تقليل الارتباك والتأكد من أن الجميع على نفس الصفحة.

تابع مكونات خطة استمرارية العمل واستعادة الأوضاع بعد الكوارث

3- الاختبار والتدريب:

لا يكفي مجرد وضع خطة؛ ومن الأهمية أن يكون جميع الموظفين على دراية بالخطة وأن يفهموا أدوارهم ومسؤولياتهم في حالة حدوث أي خلل. وينبغي عقد دورات تدريبية منتظمة للتأكد من أن الجميع يعرف ما يجب القيام به في حالات الطوارئ، ويمكن استخدام تمارين الطاولة لمحاكاة سيناريوهات مختلفة واختبار فعالية الخطة. ومن خلال اختبار الموظفين وتدريبهم بشكل منتظم على خطة الاستمرارية، يمكن للمؤسسة أن تكون مستعدة بشكل أفضل للتعامل مع أي أحداث غير متوقعة قد تنشأ.

تقييم المخاطر

تقييم المخاطر

هي عملية تتضمن تحديد وتحليل وتقييم المخاطر المحتملة التي قد تواجهها المؤسسة أو الفرد. وتعتبر عنصر حاسم في إدارة المخاطر الذي يستخدم لتحديد احتمالية وتأثير المخاطر المحتملة، وكذلك لوضع استراتيجيات للتخفيف من تلك المخاطر أو تجنبها. ويكمن الغرض من تقييم المخاطر في مساعدة المؤسسات والأفراد على اتخاذ قرارات مستنيرة حول كيفية إدارة المخاطر بشكل أفضل وتطوير خطة استمرارية العم

تحليل تأثير الأعمال
Business Impact Analysis (BIA)

يُعد تحليل تأثير الأعمال عنصرًا أساسيًا في استراتيجية إدارة المخاطر لأي مؤسسة. إنها عملية منهجية تهدف إلى تحديد وتقييم التأثيرات المحتملة التي يمكن أن يحدثها أي خلل أو حادث على وظائف الأعمال الحيوية للمؤسسة. ومن خلال إجراء تقييم الأعمال، يمكن للمؤسسات الحصول على فهم شامل لنقاط الضعف لديها ووضع خطط فعالة للتخفيف من المخاطر وضمان استمرارية الأعمال.

وفيما يلى خطوات تحليل تأثير الأعمال :

تابع تحليل تأثير الأعمال
Business Impact Analysis (BIA)

الخطوة الأولى: في إجراء تقييم الأعمال من خلال تحديد وظائف العمل الهامة وترتيب أولوياتها، وهذه هي الأنشطة الضرورية للمؤسسة لمواصلة عملياتها والوفاء بالتزاماتها تجاه العملاء والموظفين وأصحاب المصلحة. ومن خلال فهم الوظائف المهمة، يمكن للمؤسسات تركيز جهودها على حماية هذه المناطق واستعادتها في حالة حدوث خلل. ويتضمن ذلك تقييم الآثار المحتملة للاضطرابات، مثل الخسائر المالية، والضرر بالسمعة، وعدم الامتثال التنظيمي، واستياء العملاء.

الخطوة التالية: هي تحديد التبعيات والترابط بين وظائف العمل المختلفة. ويتضمن ذلك رسم العلاقات والتبعيات بين الأشخاص والعمليات والتكنولوجيا والبنية التحتية. على سبيل المثال، قد يكون للخلل في أحد الأقسام تأثير متتالي على الأقسام أو الأنظمة الأخرى، مما يؤدي إلى تأثير أكثر أهمية على المؤسسة ككل. ويُعد فهم هذه التبعيات أمرًا بالغ الأهمية لتطوير استراتيجيات فعالة لتقليل تأثير الاضطرابات وضمان التعافي في الوقت المناسب.

تقدير هدف وقت الاسترداد (RTO) وهدف نقطة الاسترداد (RPO)

يمثل هدف وقت الاسترداد (RTO) وهدف نقطة الاسترداد RPO مقياسين رئيسيين تستخدمهما المؤسسات لقياس مدى سرعة تعافيها من كارثة أو فقدان للبيانات.

**هدف وقت الاسترداد (RTO) : يحدد الوقت الذي يستغرقه استعادة تشغيل نظام أو خدمة بعد وقوع حادث. ويشمل ذلك الوقت المستغرق لإعادة تشغيل الأنظمة عبر الإنترنت واستعادة البيانات واستئناف العمليات الطبيعية. يقاس هدف وقت الاسترداد عادةً بالساعات أو الأيام وهو عامل مهم في تحديد تأثير الكارثة على العمليات التجارية.

**هدف نقطة الاسترداد (RPO) : يشير إلى كمية البيانات التي ترضى المؤسسة بفقدانها في حالة وقوع كارثة. ويقاس هدف نقطة الاسترداد بالوقت ويستخدم لتحديد مقدار البيانات المطلوب نسخها احتياطيًا ومدى تكرار إجراء النسخ الاحتياطي.

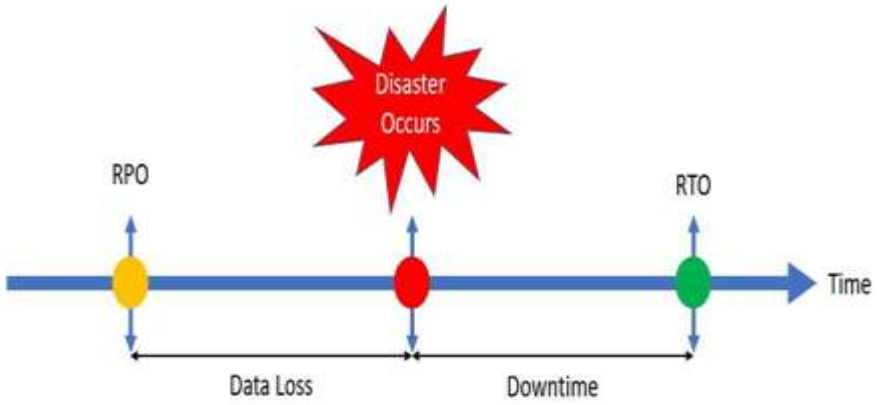
على سبيل المثال، إذا كان لدى مؤسسة هدف نقطة استرداد ساعة واحدة، فهذا يعني أنها على استعداد لفقدان ما يصل إلى ساعة واحدة من البيانات في حالة وقوع كارثة.

أهمية هدف وقت الاسترداد (RTO) وهدف نقطة الاسترداد (RPO)

ويساعد هذا المقياس المؤسسات على تحديد تكرار الحاجة إلى نسخ بياناتها احتياطيًا لضمان فقدان أقل للبيانات.

ومن خلال فهم هدف وقت الاسترداد (RTO) وهدف نقطة الاسترداد (RPO) وتحديد أهداف واقعية، يمكن للمؤسسات ضمان استعدادها للتعافي من أي كارثة أو فقدان للبيانات بسرعة وفعالية.

ومن المهم أيضًا للمؤسسات تدقيق وتحديث أهداف وقت الاسترداد وهدف نقطة الاسترداد بشكل منتظم لضمان مواءمتها مع احتياجات المؤسسة المتغيرة وأولوياتها.



تابع أهمية هدف وقت الاسترداد (RTO) وهدف نقطة الاسترداد (RPO)

لا يمكن التغاضي عن أهمية RTO و RPO في تخطيط استعادة العمل بعد الكوارث. فمن خلال تحديد هذه الأهداف، يمكن للمؤسسات تحديد أولويات جهود الاستعادة وتخصيص الموارد بشكل فعال. على سبيل المثال، إذا كان لدى مؤسسة أهداف قصيرة لكل من RTOو RPO، فقد تحتاج إلى الاستثمار في أنظمة متكررة وحلول نسخ احتياطي وخدمات استعادة بعد الكوارث لضمان قدرتها على التعافي بسرعة من كارثة بأقل قدر من فقدان البيانات. من ناحية أخرى، قد تعتمد المؤسسات التي لديها أهداف أطول لكل من RPOو RPO على حلول أقل تكلفة أو تقبل مستوى أعلى من المخاطر في تخطيط استعادة العمل بعد الكوارث لديها.

تنفيذ هدف وقت الاسترداد (RTO) وهدف نقطة الاسترداد (RPO)في خطة استعادة العمل بعد الكوارث

عند تنفيذ كل من RTOو RPOفي خطة استعادة العمل بعد الكوارث، تحتاج المؤسسات إلى:

1- تحديد أنظمتها وبياناتها الحيوية، وهذه هي الأنظمة والبيانات الأساسية لعمل المؤسسة بشكل صحيح.

2- بمجرد تحديد الأنظمة والبيانات الحيوية، يمكن للمؤسسات بعد ذلك تحديد أهداف RTO و RPO لكل منها. يجب أن تكون هذه الأهداف واقعية وقابلة للتنفيذ بناءً على موارد المؤسسة وقدراتها، ومن المهم تدقيق وتحديث هذه الأهداف بشكل منتظم مع تطور العمل وتغير التكنولوجيا.

3- امتلاك الأدوات والتقنيات المناسبة. يمكن أن يشمل ذلك حلول النسخ الاحتياطي(Backup) وتقنيات النسخ المتماثل (Replication technologies) وخدمات استعادة العمل بعد الكوارث.

4- إجراء اختبارات وتدريبات منتظمة لضمان استعادة أنظمتها ضمن أهداف RTO و RPO المحددة. من المهم إشراك جميع أصحاب المصلحة في عملية التخطيط والتنفيذ لضمان أن يكون الجميع على اطلاع ويفهمون أدوارهم ومسؤولياتهم في حالة وقوع كارثة.

تابع أهمية هدف وقت الاسترداد (RTO) وهدف نقطة الاسترداد (RPO)

في الختام، يُعد فهم أهمية RTO و RPO في تخطيط استعادة العمل بعد الكوارث أمرا ضروريا للمؤسسات التي تسعى إلى حماية بياناتها والحفاظ على استمرارية العمل في مواجهة كارثة. ومن خلال تحديد أهداف واضحة وتنفيذ استراتيجيات قوية لاستعادة العمل بعد الكوارث، يمكن للمؤسسات تقليل وقت التعطل وفقدان البيانات والخسائر المالية في حالة وقوع كارثة. وفي النهاية، يمكن أن يساعد تحديد أولوية كل من RTO و RPO في تخطيط استعادة العمل بعد الكوارث للمؤسسات وضمان استعدادها للتعافي بسرعة وفعالية من أي أحداث غير متوقعة قد تهدد عملياتها.

شكراً لكم

دراسة حالة: حوكمة نظم المعلومات في مستشفىXYZ

السيناريو:

مستشفى XYZ هو مستشفى تعليمي كبير به أكثر من 1000 سرير وطاقم عمل يزيد عن 5000 موظف. يتمتع المستشفى ببنية تحتية معقدة لتكنولوجيا المعلومات تتضمن مجموعة واسعة من الأنظمة، مثل السجلات الصحية الإلكترونية (EHRs) والنظم المالية ونظم الموارد البشرية.(HR)

برنامج حوكمة تكنولوجيا المعلومات في المستشفى ضعيف ومجزأ. لا يوجد إطار عمل واضح لحوكمة تكنولوجيا المعلومات، وقسم تكنولوجيا المعلومات ليس لديه علاقة قوية مع وحدات الأعمال. أدى ذلك إلى عدد من المشكلات، بما في ذلك:

- **ارتفاع تكاليف تكنولوجيا المعلومات :**ينفق المستشفى مبلغًا كبيرًا من المال على تكنولوجيا المعلومات، ولكنه لا يحصل دائمًا على أقصى استفادة من استثماره.
- **ضعف اتخاذ القرار في تكنولوجيا المعلومات :**غالبًا ما يتم اتخاذ قرارات تكنولوجيا المعلومات دون مراعاة احتياجات وحدات الأعمال.
- **مخاطر الأمان :**لا يتم حماية أنظمة تكنولوجيا المعلومات في المستشفى بشكل كافٍ من تهديدات الأمان.
- **مشكلات الامتثال :**لا يلتزم المستشفى بجميع لوائح تكنولوجيا المعلومات ذات الصلة.

أسئلة للمناقشة:

1. ما هي المكونات الرئيسية لإطار عمل فعال لحوكمة تكنولوجيا المعلومات؟
2. كيف يمكن لمستشفى XYZ تطوير إطار عمل واضح لحوكمة تكنولوجيا المعلومات؟
3. ما هي أدوار ومسؤوليات لجنة حوكمة تكنولوجيا المعلومات؟
4. كيف يمكن لمستشفى XYZ تحسين التواصل والتعاون بين قسم تكنولوجيا المعلومات ووحدات الأعمال؟
5. ما هي بعض الاستراتيجيات لخفض تكاليف تكنولوجيا المعلومات؟
6. كيف يمكن لمستشفى XYZ اتخاذ قرارات أفضل بشأن تكنولوجيا المعلومات؟
7. ما هي بعض أفضل الممارسات لأمان تكنولوجيا المعلومات؟
8. ما هي لوائح تكنولوجيا المعلومات ذات الصلة التي يجب على مستشفى XYZ الامتثال لها؟

مدة التمرين : 15 دقيقة

دراسة حالة: كارثة تضرب!

السيناريو:

شركتك، XYZ Technologies، هي مزود رائد لحلول البرامج المستندة إلى السحابة. لديك قاعدة عملاء عالمية وفريق من أكثر من 500 موظف.

في أحد الأيام، ضرب زلزال كبير منطقتك، مما تسبب في أضرار واسعة النطاق وانقطاع التيار الكهربائي. يتأثر مركز بيانات شركتك بشدة، وأنظمة تكنولوجيا المعلومات الخاصة بك معطلة. تحتاج إلى تنفيذ خطة

أسئلة للمناقشة:

1. ما هي الخطوات الفورية التي عليك اتخاذها لتقييم تأثير الكارثة؟
2. كيف ستحدد وظائف العمل الحرجة وتحدد أولويات استعادتها؟
3. من هم الأعضاء الرئيسيون في فرق BCP و DRP الخاصة بك؟ ما هي مسؤولياتهم؟
4. كيف ستبلغ الموظفين والعملاء والشركاء بالحالة؟
5. ما هي الحلول المؤقتة التي يمكنك تنفيذها للحفاظ على تشغيل وظائف العمل الحرجة؟
6. ما هي عملية استعادة أنظمة تكنولوجيا المعلومات والبيانات؟
7. كيف ستراقب عملية الاسترداد وإجراء التعديلات حسب الحاجة؟

مدة التمرين 15 دقيقة