المملكة العربية السعودية
ديوان المراقبة العامة
إدارة التطوير الإداري

دليل اللقاء التدريبي
الرقابة على البيانات المالية
باستخدام الحاسب الآلي

الرياض
12-1430/11/17هـ
10/31 -2009/11/5م

المحتويات		
م	البيان	الصفحة
	مقدمة	2
أولاً	موضوع اللقاء وأهدافه	3
ثانياً	العناصر التفصيلية للقاء	3
ثالثاً	موعد ومكان انعقاد اللقاء	4
رابعاً	المحاضرون	4
خامساً	المشاركون في اللقاء	4
سادساً	لغة اللقاء	4
سابعاً	تكاليف اللقاء	4
ثامناً	إدارة اللقاء	5
تاسعاً	وسائل الإيضاح وأساليب التعليم المستخدمة	5
عاشراً	تقويم اللقاء	6
إحدى عشر	الشهادات	7
أثنا عشر	البرنامج الزمني للقاء	8
ثلاثة عشر	الزيارات الميدانية والأنشطة الاجتماعية	10
أربعة عشر	إقامة المشاركين	11
خمسة عشر	معلومات عامة	12

مقدمة :

بمشيئة الله تعالى يعقد اللقاء التدريبي حول موضوع " الرقابة على البيانات المالية باستخدام الحاسب الآلي " خلال الفترة من 12-17ذوالقعدة1430هـ الموافق من 31/10-5/11/2009م ، وذلك في إطار تنفيذ خطة العمل التفصيلية للمجموعة العربية للأجهزة العليا للرقابة المالية والمحاسبة في مجال التدريب والبحث العلمي لعام 2009م ، والتي

أقرها المجلس التنفيذي للمجموعة العربية في اجتماعه الواحد والأربعين الذي عقد بالمملكة الأردنية الهاشمية يومي 22-23 ذو الحجة 1429هـ الموافق20-21 ديسمبر 2008م .

ويسر ديوان المراقبة العامة بالمملكة العربية السعودية أن يضع بين أيدي الأخوة المهتمين باللقاء والمشاركين العاملين بالأجهزة العليا للرقابة الأعضاء بالمجموعة العربية هذا الدليل الذي يتناول الجوانب الإدارية والتنظيمية للقاء والمعلومات التي تهم كل من يشارك فيه .

متمنين لكل المشاركين والمحاضرين والمنفذين على السواء التوفيق بإذن الله .

ديوان المراقبة العامة
الإدارة العامة للتطوير الإداري

أولاً : موضوع اللقاء وأهدافه :

يتمثل موضوع اللقاء في { الرقابة على البيانات المالية باستخدام الحاسب الآلي } ويهدف هذا اللقاء إلى تعريف المتدربين بطبيعة البيانات المالية الآلية ونظام الرقابة الداخلية الإلكتروني وكيفية إجراء الرقابة على تلك البيانات ، وكذلك أنواع التقنيات المستخدمة في تنفيذ الرقابة على البيانات المالية الالكترونية والوقوف على الصعوبات والمشاكل التي تواجه الأجهزة الرقابية في ذلك ، والتعرف على تجربة الجهاز المستضيف والأجهزة الأعضاء من خلال التركيز على حالات عملية تقدم لهذا الغرض .

ثانياً : العناصر التفصيلية لموضوع اللقاء :

يشتمل منهج اللقاء على العناصر الأساسية لموضوعه مع تغليب الجانب العملي والتطبيقي على الجانب النظري ، والعناصر الأساسية للقاء التدريبي هي :

- **أهمية وأهداف الرقابة باستخدام الحاسب الآلي .**
- **تخطيط عمليات الرقابة على البيانات المالية باستخدام الحاسب الآلي .**
- **المشاكل والصعوبات التي تواجه الأجهزة عند عملية الرقابة على البيانات المالية باستخدام الحاسب الآلي .**
- **حالات عملية وتطبيقية .**
- **تمارين عملية لتدعيم الجوانب النظرية (في شكل مجموعات) .**
- **أية عناصر أخرى يرى الجهاز المستضيف إضافتها .**

ثالثاً : موعد ومكان انعقاد اللقاء :

يعقد اللقاء في مقر ديوان المراقبة العامة الرئيسي بمدينة الرياض خلال الفترة من 12-17ذوالقعدة1430هـ الموافق من 10/31-2009/11/5م .

رابعاً : المحاضرون :

تم اختيار المحاضرين من بين الخبراء المتخصصين في مجال موضوع اللقاء من ديوان المراقبة العامة .

خامساً: المشاركون في اللقاء :

يشارك في اللقاء موظفون فنيون ممن هم في درجة مراقب أو مدقق وتتوفر لديهم خبرة عملية في مجال الرقابة المالية والحاسب الآلي لا تقل عن سنتين بالنسبة لحملة الشهادات الجامعية ولا تزيد عن عشر سنوات ، أما بالنسبة لمن يحملون مؤهلات متوسطة فلا تقل عن خمس سنوات ولا تزيد عن خمسة عشرة سنة ، وأن يكونوا ممن لديهم خبرة في مجال الحاسب الآلي ، ويتراوح عدد المشاركين ما بين 20 – 25 متدرباً يمثلون الأجهزة الأعضاء في المجموعة العربية .

سادساً : لغة اللقاء :

تستخدم في اللقاء اللغة العربية .

سابعاً : تكاليف اللقاء :

وفقاً لأحكام المادتين (6 ، 7) من قواعد اللقاءات العلمية والتدريبية والبحث العلمي للمجموعة العربية تكون التكاليف على النحو التالي :

1 – يتحمل ديوان المراقبة العامة بالمملكة العربية السعودية النفقات التالية :

- **توفير مكان اللقاء وتجهيزه بالوسائل اللازمة .**
- **توفير القرطاسية والطباعة وأعمال الإدارة .**

2 – يتحمل كل جهاز من الأجهزة المشاركة في اللقاء نفقات مشاركة موفديه إلى اللقاء " سفر وإقامة " .

ثامناً : إدارة اللقاء :

تم تعيين الأستاذ/ إبراهيم بن ناصر الدوسري مدير إدارة التدريب بالديوان مديراً للقاء .

تاسعاً : أساليب التدريب ووسائل الإيضاح المستخدمة قي اللقاء :

تتمثل أساليب التدريب ووسائل الإيضاح المستخدمة في اللقاء فيما يلي :

1 – جلسات تعريف بالأسس العلمية .
2- حالات عملية ومناقشات .
3 - ملف لكل مشارك يحتوي على المادة العلمية للقاء والحالات العملية للمشاركين في اللقاء .
4 – كمبيوتر وجهاز عرض Data show .

عاشراً : تقويم اللقاء :

يتبع في تقويم اللقاء الأسلوب التالي :

- **يُجيب المشاركون على صحيفة الاستقصاء التي أعدتها الأمانة العامة للمجموعة العربية .**
- **يُجيب الخبراء المحاضرين على صحيفة الاستقصاء التي أعدتها الأمانة العامة للمجموعة العربية .**
- **يُعد مدير اللقاء و ممثل الأمانة العامة تقريراً مشتركاً يعرضان فيه جميع الجوانب المتعلقة بتنفيذ اللقاء وكذلك نتائج تحليل صحائف استقصاء المشاركون والخبراء المحاضرين ، والمقترحات التي أمكن استخلاصها من الإجابات على هذه الصحائف .**

احد عشر: الشهادات :

- **يمنح المشاركون في نهاية اللقاء شهادات "اجتياز دورة تدريبية " وتمنح الأمانة العامة شهادات تقدير إلى رئيس الجهاز المستضيف وإلى مدير اللقاء وإلى الخبراء المدربين .**

ويجب عند إعطاء شهادة اجتياز الدورة التدريبية الأخذ في الاعتبار العناصر التالية :

- حضور المشارك كامل جلسات اللقاء .
- مساهمته في المناقشات والتمارين العملية التي تضمنها اللقاء .
- مدى جودة العرض الذي قدمه مع وفد جهازه حول تجربة هذا الجهاز في إحدى المجالات المتعلقة بموضوع اللقاء .

إثناء عشر :

البرنامج الزمني للقاء

اليوم والتاريخ	الجلسة	الساعة		الموضوع
		من	إلى	
السبت 1430/11/12هـ 2009/10/31م	الأولى	9:00	9:30	- الافتتاح - القرآن الكريم - كلمة الافتتاح
		9:30	10:00	استراحة
	الثانية	10:00	12:00	تقديم المشاركين لأنفسهم ويتناول : - نبذة عن الجهاز الذي ينتمي إليه المشارك - ما يتوقعه المشارك من المشاركة في اللقاء - مقدمة وتعريف الرقابة باستخدام الحاسب الآلي
		12:00	12:30	استراحة والصلاة
	الثالثة	12:30	2:00	- أهمية الرقابة باستخدام الحاسب الآلي - أهداف الرقابة باستخدام الحاسب الآلي - أنواع الرقابة باستخدام الحاسب الآلي - تاريخ بداية التدقيق الآلي بالديوان
الأحد 1430/11/13هـ 2009/11/1م	الأولى	9:00	10:30	- مزايا وعيوب الرقابة باستخدام الحاسب الآلي - - المشاكل والصعوبات التي تواجه الأجهزة والمراجعين عند إجراء عملية الرقابة المالية - الأدوات المستخدمة للرقابة على البيانات باستخدام الحاسب الآلي - أمن المعلومات المادي والمنطقي - الأسئلة التي تطرح على مركز المعلومات الخاصة بالأمن - استعراض بعض تجارب الدول المشاركة
		10:30	10:45	استراحة
	الثانية	10:45	12:00	- الأدوات المستخدمة للرقابة على البيانات باستخدام الحاسب الآلي
		12:00	12:30	استراحة والصلاة

اليوم والتاريخ	الجلسة	الساعة		الموضوع
		من	إلى	
	الثالثة	12:30	2:00	- نبذة عن قواعد البيانات - نبذة عن برنامج التحليل آيديا في تحليل البيانات واكتشاف نتائج التدقيق - خطوات المراجعة الآلية - الأوامر المستخدمة في برنامج التحليل آيديا - استعراض تجارب الدول المشاركة
الاثنين 1430/11/14هـ 2009/11/2م	الأولى	9:00	10:30	- أنواع وطرق تحميل البيانات إلى برنامج آيديا
		10:30	10:45	استراحة
	الثانية	10:45	12:00	- تمارين عملية لاستخدام أوامر البرنامج التحليلي - استعراض لتجارب الدول المشاركة
		12:00	12:30	استراحة والصلاة
	الثالثة	12:30	2:00	استكمال لتمارين تطبيقية عن نظام المدفوعات
الثلاثاء 1430/11/15هـ 2009/11/3م	الأولى	9:00	10:30	دراسة حالات عملية عن برنامج التحليل آيديا خاصة بالمستودعات والمخزون
		10:30	10:45	استراحة
	الثانية	10:45	12:00	تمارين تطبيقية على كيفية كتابة المعادلات التحليلية
		12:00	12:30	استراحة والصلاة
	الثالثة	12:30	2:00	- كتابة التقرير ونقل مرفقات التقارير من آيديا إلى إكسل - استعراض لتجارب الدول المشاركة
الأربعاء 1430/11/16هـ 2009/11/4م	الأولى	9:00	10:30	حالات عملية عن برنامج التحليل آيديا خاصة بمراجعة الرواتب
		10:30	10:45	استراحة
	الثانية	10:45	12:00	استكمال الحالات العملية
		12:00	12:30	استراحة والصلاة
	الثالثة	12:30	2:00	- أهمية وأغراض استخدام برنامج التيم ميت - استعراض لتجارب الدول المشاركة
الخميس 1430/11/17هـ 2009/11/5م	الأولى	9:00	10:30	تمارين ومراجعة
		10:30	10:45	استراحة
	الثانية	10:45	12:00	تمارين ومراجعة
		12:00	12:30	استراحة والصلاة
	الثالثة	12:30	2:00	الختام وتوزيع الشهادات

ثلاثة عشر : الزيارات الميدانية والأنشطة الاجتماعية :

م	التاريخ	الوقت	النشاط الاجتماعي
1	السبت 1430/11/12هـ 2009/10/31م	8:30 مساءً	حفلة عشاء
2	الثلاثاء 1430/11/15هـ 2009/11/3م	4:30 مساءً	زيارة مركز الملك عبد العزيز التاريخي
3	الأربعاء 1430/11/16هـ 2009/11/4م	4:00 مساءً	جولة حـرة

أربعة عشر: إقامة المشاركين :

تم اختيار الفنادق التالية والتي تقع على مقربة من مكان انعقاد اللقاء ، وبياناتها كالتالي :

أسم الفندق	الدرجة	غرفة مفردة	غرفة مزدوجة	ملاحظات
فندق راديسون ساس	5 نجوم	(795)	(1095)	15% رسم خدمة
فندق ماريوت الرياض	5 نجوم	(700)	(800)	15% رسم خدمة
فندق القصر الأبيض	4 نجوم	(310)	(460)	15% رسم خدمة إفطار + عشاء بوفيه مفتوح مجاني
فندق زهرة الشرق	4 نجوم	(250)	(300)	15% رسم خدمة
فندق المنصور	4 نجوم	(200)	(280)	15% رسم خدمة بوفيه إفطار مجاني
برج الحياة للأجنحة الفندقية		جناح صغير غرفة صالةو مطبخ (150)	جناح وسط غرفة3أسرة وصالة ومطبخ (250)	
المهيدب للأجنحة الفندقية		غرفة +صالة ومطبخ (200)		
بيت الدومة للشقق المفروشة		غرفة و صالة (170)	غرفتين وصالة (220)	
نواره للأجنحة الفندقية		غرفة وصالة ومطبخ (180)	غرفتين وصالة ومطبخ (280)	

- علماً بأن الأسعار أعلاه قد يتم تغييرها دون إشعار مسبق .
- الأسعار بالريال السعودي
- $ = 3.76 ريال سعودي

خمسة عشر :

للحصول على معلومات عن المملكة العربية السعودية من خلال زيارة الموقع التالي على الإنترنت :

WWW.Mas.gov.sa

وعن (مدينة الرياض) من خلال زيارة موقعها على الإنترنت :

WWW.alriadh.gov.sa

وعن ديوان المراقبة العامة بالمملكة العربية السعودية من خلال موقعه على الانترنت :

WWW.gab@gab.gov.sa

العنوان البريدي لديوان المراقبة العامة

شارع الجامعة بالرياض

صندوق بريد	7185
رمز بريدي	11128
هاتف	4056770
فاكس	4043887

المملكة العربية السعودية
ديوان المراقبة العامة
الرياض

Kingdom of Saudi Arabia
General Auditing Bureau
Riyadh

اللقاء التدريبي
الرقابة على البيانات المالية
باستخدام الحاسب الآلي

(دليل المدرب)

12-1430/11/17هـ-10/31 -2009/11/5م

إعداد المدربين

خالد بن حسن الصبياني

جمال بن عيد المطيري

عبدالعزيز بن حسين الصبياني

1- التعارف بين المتدربين وتقديم الدورة وعقد التعلم

هدف الجلسة :

- **مساعدة المشاركين بما في ذلك المدربين لمعرفة أشياء عن بعضهم البعض.**
- **جعل المشاركين يشعرون بأكثر أريحية في بيئتهم الجديدة.**
- **خلق جو ملائم للتعلم يتميز بالإقبال على المشاركة والتعبير.**
- **تكوين مجتمع تعلم يسهل فيه العمل الجماعي ضمن فرق.**
- **وصف المخطط الكامل للحلقة.**
- **تحديد بنود العقد المكتوب التي اتفق حولها المدربون والمشاركون بخصوص توقعاتهم والتزاماتهم خلال المحاضرة.**

التحضير :

- مراجعة مواد هذه الجلسة.
- مراجعة كل من دليل المدرب والمشارك .
- إعداد مخطط للجلسة والتدرب عليه إلى أن تشعر بالثقة والراحة التامة.
- التأكد من وجود كافة الشرائح المتعلقة بالجلسة.
- التأكد من جاهزية المعدات التي سوف تستخدم في العملية التدريبية.

النقاط التي ستتم تغطيتها	الأسلوب	مستلزمات التدريب	الهدف	الوقت اللاّزم
التعارف				
الأهداف والمنهجية التي ستعتمد على التعارف	**محاضرة**	**عرض الشرائح**	**توضيح أهداف الجلسة**	
إنجاز المطلوب من قبل المشاركين.	**الإنجاز الفردي**	**نشرة للتوزيع الشريحة**	**تسجيل المشارك للبيانات الشخصية عن نفسه في البطاقة المخصصة له.**	
تحرك كل المشاركين داخل القاعة لقراءة بطاقات بعضهم البعض.	**الإنجاز الجماعي**	**قاعة تمكن من تحرك كل المشاركين بأريحية**	**جعل المشاركين يتواصلون ببعضهم البعض بصفة مباشرة.**	
التعرف على بعض المشاركين	**المشاركة الجماعية**		**تقييم مدى تحقيق الأهداف من إذابة الجليد.**	
1-2- تقديم الحلقة				
تقديم مخطط الدورة	**محاضرة**	**الشرائح**	**تعريف المشاركين بالمادة العلمية للحلقة**	

1-3- عقد التعلم				
أهـداف عقـد الـتعلم والمنهجية التي ستعتمد في إعداده.	محاضرة	الشرائح	تعريف المشاركين بالهدف من عقد التعلم.	
إنجاز المطلـوب مـن المشاركين.	التفكيـــــر الجماعي ضمن فرق.	نشرة للتوزيع	تعويد المشـاركين علـى العمل الجماعي ضمن فرق للتفكير في بنود العقد.	
الاتفاق على بنود العقد	النقاش	ورقـــة كبيـــرة منفصلة	التوصـل إلـى الاتفـاق الجماعي حول بنود العقد.	
الوقت اللازم				

عنوان الجلسة: التعارف وتقديم الدورة وعقد التعلم

التعارف

رحبوا بـالجميع بـالقول نفتـتح اليـوم علـى بركـة الله محاضـرات الـدورة التدريبيـة حـول الرقابـة باستخدام الحاسب الآلي

اعرضوا الشرائح الخاصة

قولوا بأننا سنحاول جميعا أن ننجز تمرينا هو بمثابة اللعبة الجماعية الهدف منه

- مساعدة المشاركين بما في ذلك المدربين لمعرفة أشياء عن بعضهم البعض.
- جعل المشاركين يشعرون بأكثر أريحية في بيئتهم الجديدة.
- خلق جو ملائم للتعلم يتميز بالإقبال على المشاركة والتعبير.
- تكوين مجتمع تعلم يسهل فيه العمل الجماعي ضمن فرق.

أوضحوا بأن تكوين ما يسمى "بمجتمع التعلم" أساسي لنجاح مثل الدورات التكوينية بصفة عامة.

اسألوا السؤال التالي: حسب رأيكم بماذا يمكن أن يتميز مجتمع التعلم؟

تلقوا إجابات المشاركين

الإجابات المرتقبة:

- الاحترام المتبادل
- تبادل الخبرات
- النقاش البناء
- العمل الجماعي

أوضحوا أنه لكي نتوصل إلى تكوين مجتمع التعلم نرجو أن يفتح كل شخص منا نافذة يعرفنا فيها على أشياء عن نفسه.

أظهروا الشريحة الخاصة

اقرؤوا محتوى النشرة.

قولوا للمشاركين بأن لديهم 10 دقائق لإنجاز المرحلة الأولى من التمرين والمتمثلة في تسجيل البيانات التالية على البطاقة:

- اسمك ولقبك في وسط البطاقة.
- هوايتك المفضلة في الركن الأيمن العلوي.
- لونك المفضل في الركن الأيسر السفلي.

- اختصاصك خلال الدراسة الجامعية في الركن الأيسر العلوي.
- أمنية ترجو تحقيقها في الركن الأيمن السفلي.

قوموا بالتحرك داخل القاعة لمشاهدة المشاركين ينجزون المطلوب منهم والتأكد من فهمهم له دون الاقتراب كثيرا لأن بعض المشاركين قد يتحرجون من ذلك.

أذكروا المشاركين بعد 10 دقائق بأن المطلوب منهم الآن التحرك داخل القاعة باتجاه مشاركين آخرين محاولين النظر في أكثر ما يمكن من البطاقات للتعرف على أصحابها، على أن ينظروا إلى وجوه الأشخاص قبل وبعد قراءة البطاقات ويستخدموا ذاكرتهم لحفظ بعض البيانات عن بعض المشاركين فقد يحتاجونها لاحقا.

أطلبوا من المشاركين الجلوس عند انتهاء 20 دقيقة.

قولوا للمشاركين أنكم الآن تعرفون بعض الأشياء عن بعضكم البعض ونود أن نتأكد أنكم تمكنتم من تذكر البعض منها.

قوموا بتجميع بطاقات المشاركين.

اقرؤوا محتوى البطاقة الأولى

أتيحوا الفرصة للمشاركين للتعرف على المشارك صاحب البطاقة مع التوصية بأن لا يتكلم صاحب البطاقة عندما يعلم أنها تتعلق به.

أنجزوا نفس العملية بالنسبة للبطاقتين الأخريين.

اسألوا المشاركين الأسئلة التالية:

- ما هو شعوركم الآن؟
- هل ساعدكم هذا النشاط على التعرف على بعضكم البعض؟
- هل لديكم أي تعليق؟

تلقوا إجابات المشاركين.

الأجوبة المرتقبة:

- أكثر أريحية
- رغبة في التعرف أكثر على المشاركين
- يشجع على العمل الجماعي

استمعوا جيدا إلى انطباعات المشاركين.

اشكروا الجمع على مشاركتهم الإيجابية.

قولوا أننا بعد أن تعرفنا على بعض سوف نمر الآن إلى التعرف على محتوى الدورة التدريبية حول الرقابة باستخدام الحاسب الآلي من خلال عرض حول مخططها.

اظهروا الشرائح الخاصة

اقرؤوا محتوى الشريحة

- نبذة عن التالي :
- التعريف بالرقابة باستخدام الحاسب الآلي
- أهمية الرقابة على تقنية المعلومات
- أهداف الرقابة على تقنية المعلومات
- مزايا الرقابة باستخدام الحاسب الآلي

- المشاكل والصعوبات التي تواجه الأجهزة والمراجعين عند إجراء عملية الرقابة على البيانات المالية بالحاسب الآلي .
- الأدوات المستخدمة للرقابة على البيانات باستخدام الحاسب الآلي .
- نبذة عن برنامج التحليل آيديا المستخدم في تحليل البيانات واكتشاف نتائج التدقيق .
- الأوامر المهمة المستخدمة في برنامج التحليل آيديا .
- نبذة عن الأمن المادي والمنطقي لمركز المعلومات .
- نبذة عن أمن المعلومات .
- بعض الأسئلة المهمة التي يستخدمها المراجع لفحص مراكز المعلومات .
- حالات عملية لدعم وتوضيح الجوانب النظرية .

مقدمة

هدف الجلسة :
تهدف هذه الجلسة إلى إعطاء المشاركين نبذة عن :
الحاسب الآلي ومكوناته
ووحدة النظام
أجهزة الإدخال
أجهزة التخزين
أجهزة الإخراج
مقاييس التخزين (السعة)
البرامج وأنواعها
أنواع الشبكات وأنظمة التشغيل
فوائد الشبكات
برامج التطبيقات
التحضير :

- مراجعة مواد هذه الجلسة .
- مراجعة كل من دليل المدرب والمشارك .
- إعداد مخطط بالجلسة والتدرب عليه إلى أن تشعر بالثقة والراحة التامة .
- التأكد من وجود كافة الشرائح المتعلقة بالجلسة .
- التأكد من جاهزية المعدات التي سوف تستخدم في العملية التدريبية .

النقاط التي سيتم تغطيتها	الأسلوب	مستلزمات التدريب	الهدف	الوقت اللاّزم
نظرة عامة حول الجلسة	محاضرة ونقاش	عرض الشريحة	إعطاء نظرة عامة حول الجلسة ومحتوياتها	
مفاهيم أساسية	محاضرة ونقاش	عرض الشريحة	مفاهيم في الحاسب الآلي	
الحاسب الآلي ومكوناته	محاضرة ونقاش	عرض الشريحة	تعريف ومكونات الحاسب	

وحدة النظام	**محاضرة ونقاش**	**عرض الشريحة**	**مكونات الجهاز الهاردوير**	
أجهزة الإدخال	**محاضرة ونقاش**	**عرض الشريحة**	**أنواع أجهزة الإدخال**	
أجهزة التخزين	**محاضرة ونقاش**	**عرض الشريحة**	**أنواع أجهزة التخزين**	
أجهزة الإخراج	**محاضرة ونقاش**	**عرض الشريحة**	**أنواع أجهزة الإخراج**	
البرامج وأنواعها	**محاضرة ونقاش**	**عرض الشريحة**	**أنواع البرامج**	
أنواع الشبكات	**محاضرة ونقاش**	**عرض الشريحة**	**أنواع الشبكات**	
أنظمة التشغيل	**محاضرة ونقاش**	**عرض الشريحة**	**أنواع أنظمة التشغيل**	
فوائد الشبكات	**محاضرة ونقاش**	**عرض الشريحة**	**إيضاح فوائد الشبكات**	
برامج التطبيقات	**محاضرة ونقاش**	**عرض الشريحة**	**أنواع برامج التطبيقات**	

<u>تعريف الرقابة باستخدام الحاسب الآلي</u>

هدف الجلسة :

تهدف هذه الجلسة إلى إيضاح ما يلي للمشاركين :

- تعريف بالرقابة باستخدام الحاسب الآلي
- أهمية التدقيق باستخدام الحاسب الآلي
- أهداف تدقيق الحاسب الآلي
- وسائل وسبل إساءة استخدام الحاسب الآلي
- أنواع الرقابة باستخدام الحاسب الآلي
- مزايا المراجعة باستخدام الحاسب الآلي
- خطوات المراجعة
- المشاكل والصعوبات التي تواجه المراجعين
- الأدوات المستخدمة للرقابة على البيانات الآلية
- نبذة عن برنامج التحليل آيديا
- الأوامر المستخدمة في برنامج التحليل
- حالات عملية لدعم وتوضيح النواحي النظرية

التحضير :

- مراجعة مواد هذه الجلسة .
- مراجعة كل من دليل المدرب والمشارك .
- إعداد مخطط بالجلسة والتدرب عليه إلى أن تشعر بالثقة والراحة التامة .
- التأكد من وجود كافة الشرائح المتعلقة بالجلسة .
- التأكد من جاهزية المعدات التي سوف تستخدم في العملية التدريبية .

النقاط التي سيتم تغطيتها	الأسلوب	مستلزمات التدريب	الهدف	الوقت اللازم
تعريف الرقابة باستخدام الحاسب الآلي	محاضرة ونقاش	عرض الشريحة	إعطاء نظرة عامة حول الجلسة ومحتوياتها	
أهمية التدقيق باستخدام الحاسب الآلي	محاضرة ونقاش	عرض الشريحة	إيضاح أهمية استخدام التدقيق الآلي	
أهداف تدقيق الحاسب الآلي	محاضرة ونقاش	عرض الشريحة	إيضاح أهداف التدقيق الآلي	
وسائل وسبل إساءة استخدام الحاسب الآلي	محاضرة ونقاش	عرض الشريحة	كيفية إساءة استخدام الحاسب الآلي	
أنواع الرقابة باستخدام الحاسب الآلي	محاضرة ونقاش	عرض الشريحة	أنواع الرقابة باستخدام الحاسب الآلي	
مزايا المراجعة باستخدام الحاسب الآلي	محاضرة ونقاش	عرض الشريحة	مزايا المراجعة الآلية	
خطوات المراجعة	محاضرة ونقاش	عرض الشريحة	خطوات المراجعة	
المشاكل والصعوبات التي تواجه المراجعين	محاضرة ونقاش	عرض الشريحة	الصعوبات التي تواجه المراجعين	
الأدوات المستخدمة للرقابة على البيانات الآلية	محاضرة ونقاش	عرض الشريحة	الأدوات المستخدمة للرقابة باستخدام الحاسب الآلي	
نبذة عن برنامج التحليل آيديا	محاضرة ونقاش	عرض الشريحة	نبذة عن برنامج التحليل آيديا	
الأوامر المستخدمة في برنامج التحليل	محاضرة ونقاش	عرض الشريحة	الأوامر المستخدمة في برنامج التحليل	
حالات عملية لدعم وتوضيح النواحي النظرية			تمارين عامة على برنامج التحليل	

عناصر التحكم المادية والمنطقية

هدف الجلسة :
تهدف هذه الجلسة إلى تمكين المشاركين من التعرف على عناصر التحكم بأنواعها المادية والبيئية والمنطقية وأهميتها في حماية النظام من أي مخاطر قد يتعرض لها .

التحضير :

- مراجعة مواد هذه الجلسة .
- مراجعة كل من دليل المدرب والمشارك .
- إعداد مخطط بالجلسة والتدرب عليه إلى أن تشعر بالثقة والراحة التامة .
- التأكد من وجود كافة الشرائح المتعلقة بالجلسة .
- التأكد من جاهزية المعدات التي سوف تستخدم في العملية التدريبية .

النقاط التي سيتم تغطيتها	الأسلوب	مستلزمات التدريب	الهدف	الوقت اللاّزم
نظرة عامة حول الجلسة	محاضرة ونقاش		إعطاء نظرة عامة حول الجلسة ومحتوياتها	
مفاهيم أساسية	محاضرة ونقاش		تزويد المشاركين بمعنى المفاهيم المتعلقة بعناصر التحكم	
عناصر التحكم المادية	محاضرة ونقاش		تعريف المشاركين بأهم عناصر التحكم المادية	
مخاطر ضعف عناصر التحكم المادية	محاضرة ونقاش		إكساب المشاركين للمهارات والمعارف الأزمة لتحديد المخاطر المتعلقة بضعف عناصر التحكم المادية	
عناصر التحكم البيئية	محاضرة ونقاش		تزويد المشاركين بأهم عناصر التحكم البيئية .	
مخاطر الضعف في عناصر التحكم البيئية	محاضرة ونقاش		إكساب المشاركين للمهارات والمعارف الأزمة لتحديد المخاطر المتعلقة بضعف عناصر التحكم البيئية	
عناصر التحكم المنطقية	محاضرة ونقاش		تعريف المشاركين بأهم عناصر التحكم المنطقية	

إجراءات الدخول	**محاضرة ونقاش**			
فعالية كلمة السر	**محاضرة ونقاش**		**تعريف المشاركين بالشروط الواجب توافرها بكلمة السر لتكون فعالة**	
عناصر تحكم منطقية أخرى	**محاضرة ونقاش وتمرين**		**تعريف المشاركين بأهم عناصر التحكم المنطقية الأخرى**	
المهاجمون	**محاضرة ونقاش**		**تعريف المشاركين بأنواع المهاجمين لنظام تقنية المعلومات**	
اثر ضعف / غياب عناصر التحكم المنطقية	**محاضرة ونقاش**		**إكساب المشاركين للمهارات والمعارف الأزمة لتحديد المخاطر المتعلقة بضعف عناصر التحكم المنطقية**	
ما هي الأصول التي يجب حمايتها	**محاضرة ونقاش وتمرين**		**تعريف المشاركين بأهم الأصول التي يجب حمايتها ضد المخاطر المحتملة**	

نظرة عامة حول الجلسة

بينوا للمشاركين أن النظام بعد أن تم اقتناءه فان النظام كأي أصل من أصول الجهة يحتاج إلى وضع عناصر تحكم ملائمة لحمايته من أي مخاطر قد يتعرض لها هذا النظام .

وضحوا للمشاركين انه لكي يتم تحديد عناصر التحكم الملائمة لابد في البداية أن يتم تحديد المخاطر التي قد يتعرض لها النظام ومن ثم يتم تحديد عناصر التحكم الملائمة لكل خطر.

اضربوا مثل للمشاركين بأحد أصول الجهة و لتكن النقدية وان احد المخاطر التي قد تتعرض لها هي السرقة لذا فان عناصر التحكم هي وضع النقدية في خزينة محكمة , التامين على أمين الصندوق ضد خيانة الأمانة .. الخ وهكذا بالنسبة لأي أصل .

أوضحوا بعد ذلك للمشاركين بشكل مختصر إننا في هذه الجلسة سنركز على الأتي:

- عناصر التحكم المادية .
- عناصر التحكم البيئية .

مفاهيم أساسية :

بينوا للمشاركين أن هناك مجموعة من المفاهيم التي لابد لهم من معرفتها قبل الدخول في تفاصيل هذه الجلسة .

بينوا للمشاركين إن عناصر التحكم المادية تمثل الآليات والإجراءات المستخدمة لمنع الدخول غيرا لمصرح به لمعدات تقنية المعلومات وإنها هامة لحماية نظام تقنية المعلومات وان سبب تسميتها بعناصر التحكم المادية بسبب تعلقها بعملية منع الدخول المادي من قبل الأشخاص الغير مصرح لهم بالدخول.

وضحوا للمشاركين مفهوم عناصر التحكم البيئية والتي تمثل الآليات والإجراءات المستخدمة لحماية الأجهزة وبرامجه من التعرض للمخاطر البيئية مثل الحرائق والماء والرطوبة .لوحظ في الفحص الميداني **لا يوجد مقياس يقيس نسبة الرطوبة في غرفة** server **يوجد في مكتب الشبكات منظم الكهرباء(** UPS **) المركزي وكابلات الكهرباء والغرفة لا تتعدى حجمها المتر والنصف. اسطوانة الحريق الكبيرة الموجود في غرفة** server **يستحسن أن تنقل إلى غرفة أمنة غير غرفة** server

قدموا للمشاركين التعريف المتعلق بالسجل والذي هو عبارة عن يومية أو سجل يستخدم لتسجيل الإحداث أو الأنشطة المتعاقبة . .لوحظ في الفحص الميداني عدم الإطلاع علي السجل أو اتخاذ إجراءات لازمة

بينوا للمشاركين مفهوم عناصر التحكم المنطقية والتي هي عبارة عن شكل من عناصر التحكم البرمجية التي تستخدم لمنع الدخول غير المصرح به إلى ملفات وبيانات الكمبيوتر .

عناصر التحكم المادية :

بينوا للمشاركين أن عناصر التحكم الموضحة في الشريحة تتلاءم مع الخطر المادي التي قد يتعرض لها النظام وهو الدخول غير المصرح به لمعدات واليات النظام .

بينوا للمشاركين أن هناك أنواع عديدة من عناصر التحكم المادية ومنها الأقفال , كاميرات الفيديو حراس الأمن ,السياجات الحدودية وأجهزة الإنذار .

اذكروا للمشاركين بعض أنواع الأقفال مثل أقفال المفاتيح الميكانيكية , أقفال الأبواب الالكترونية , أبواب الأقفال الحيوية وان اختيار أي نوع من تلك الأقفال يعتمد على عوامل عديدة منها حجم نشاط الجهة , أهمية البيانات والمعلومات .

بينوا للمشاركين أن وجود مثل هذه العناصر ضروري والاهم من ذلك هو تفعيلها وضربوا مثال على ذلك هو ما وجدناه في إحدى الجهات التي تم فحصها والتي كان لدى إدارة تقنية المعلومات فيها قفل الكتروني إلا أن ذلك القفل لم يكن مفعل وكان من الممكن لأي شخص الدخول دون الحاجة لفتح ذلك القفل .

وضحوا للمشاركين أن هناك عناصر تحكم مادية تتمثل في الإجراءات الإدارية مثل التحكم في الموظفين الذين يعملون في أوقات غير أوقات العمل مثل الموظفين المتعاقدين وعمال النظافة وحراس الأمن . .لوحظ في الفحص الميداني **لا يوجد سياسة وإجراءات لمرافق دائرة تكنولوجيا المعلومات يستطيع المستخدم فتح النظام علي أكثر من جهاز بنفس كلمة المرور وكلمة السر الخاصة لا يتم الخروج**

الآلي المؤقت للنظام في حالة ترك الموظف للجهاز لا يوجد معايير مكتوبة من الإدارة بما يخص الرقابـة على الفيروسات

المخاطر المصاحبة لضعف عناصر التحكم المادية :

اسألوا المشاركين ما هي توقعاتهم للمخاطر التي قد يتعرض لها النظام في حال ضعف أو غياب عناصر التحكم المادية
اطلبوا من احد المشاركين تدوين الردود على حامل الأوراق .
ناقشوا المشاركين ردودهم .
اعرضوا الشريحة
قارنوا مع المشاركين بين إجابات المشاركين و بين ما تم عرضه على الشريحة .
وضحوا النقاط التي تضمنتها الشريحة ولم تتضمنها إجابات المشاركين .

عناصر التحكم البيئية (الحرائق) :

بينوا للمشاركين أن الحرائق قد تنتج نتيجة لحوادث عرضية أو لأسباب متعمدة وأي كانت الأسباب فلابد للجهة أن تمتلك العناصر والإجراءات الكفيلة للحيلولة دون وقوع مثل هذه الحوادث ومنها الأتي :

- منع التدخين .
- جعل منشآت تقنية المعلومات مقاومة للحرائق .
- أجهزة إنذار الحرائق .
- معدات إخماد الحرائق مثل الغاز والماء .

ناقشوا المشاركين حول كل العناصر والإجراءات الموضحة في الشريحة . .لوحظ في الفحص الميداني عدم الاهتمام بتثقيف المستخدمين بالمخاطر

عناصر التحكم البيئية (الماء واردة المرافق) :

بينوا للمشاركين أن أجهزة الكمبيوتر لا يمكن أن تجتمع إطلاقا مع الماء وان الماء لا يقل خطرا على النظام عن غيره من المخاطر .
اسألوا المشاركين عن الأسباب التي قد تؤدي إلى وصول المياه إلى غرفة الكمبيوتر وناقشوا ردودهم ثم بينوا أن من أهم تلك الأسباب الفيضانات , الأسقف التي تسرب المياه , فيضانات المياه في المنخفضات التي يتجمع فيها المياه , في الحمامات , التكاثف , التسرب من شبكة التدفئة .
بينوا للمشاركين عدد من عناصر التحكم التي تحول دون وصول الماء إلى غرفة الكمبيوتر والتي من أهمها ما يلي :

- عدم إنشاء غرف الحاسوب في السراديب .
- أجهزة إنذار المياه .
- منع تناول أي مشروبات .

بينوا للمشاركين أننا وجدنا جهات لم يكن لديها أي سياسات تمنع تناول الأطعمة والمشروبات في غرف الكمبيوتر
وضحوا للمشاركين ضرورة الاهتمام بمرافق أجهزة الكمبيوتر وتنظيفها بشكل منتظم لمنع تراكم الغبار والأوساخ .

عناصر التحكم البيئية (أجهزة تزويد الكمبيوتر) :

اذكروا للمشاركين أن عدم توفر الطاقة وانحرافاتها تعتبر من جملة المخاطر التي قد يتعرض لها النظام وبالتالي فان على الجهة أن تمتلك عناصر التحكم التي تحول دون حدوث انقطاع في التيار الكهربائي ومنها الأتي :

- مثبتات الفولتية .
- المولدات الاحتياطية .

- أجهزة تزويد التيار الغير متقطع .
- كابلات التيار البديلة .

وضحوا للمشاركين أن متطلبات تزويد التيار غير المتقطع حسب الاحتياجات المحلية مثل التردد ومدد انقطاع التيار .
اذكروا للمشاركين أننا وجدنا من خلال فحصنا لبعض الجهات عدم وجود العدد الكافي من المثبتات الفولتية لكافة الأجهزة المستخدمة في الجهة . **يوجد اهتزازات في شاشات الكمبيوتر بشكل كبير وقد تكون نتيجة وجـود تأثير كهرومغناطيسي قوي**

المخاطر المصاحبة لضعف عناصر التحكم البيئية :

بينوا للمشاركين أن أي ضعف في عناصر التحكم البيئية قد يؤدي إلى احد المخاطر الآتية :
- الإضرار الناجمة عن الحرائق .
- الماء .
- انقطاع التيار الكهربائي .
- الخلل (التطرف في درجة الحرارة والرطوبة).
- الكهرباء الساكنة .

تمرين رقم (1)

الهدف: الهدف تمكين المشاركين من تحديد عناصر التحكم المادية والبيئية

التعليمات :

- القراءة الفردية للتمرين .
- مناقشة الحلول التي تم التوصل إليها في ضمن المجموعة الصغيرة ودونوا الحل الذي وصلتم إليه على ورقة .
- اختيار شخص يمثل المجموعة ليمثلها في عرض الحل

الوقت المخصص: أربعون دقيقة .

القراءة الفردية : خمسة دقائق

مناقشة المجموعة الفرعية : خمسة عشر دقيقة

استخلاص المعلومات في وجود جميع الأعضاء : خمسة عشر دقيقة

إن الهدف من سيطرة الوصول المادية هو منع الوصول الغير مصرح إلى خدمات تقنية المعلومات. يمكن أن تتراوح عناصر تحكم الوصول المادية من الأنواع المختلفة للأبواب إلى وسائل التحكم الإجرائية الإدارية البسيطة. على نحو مماثل، فإن عناصر تحكم البيئية من أجل منع، كشف وخمد أي ضرر على خدمات تقنية المعلومات من الأخطار البيئية مثل الماء، مصدر الطاقة الخ ،

الجزء الأول

أنت مطالب بأن تناقش في المجموعة الخاصة بك عناصر تحكم المتعددة لأي من العناصر المُعطاة أدناه (ستُخصص عناصر التحكم للمجموعة):

- عناصر تحكم المادية
- منع الحرائق، الكشف والإخماد
- منع ضرر الماء، عناصر تحكم الصيانة وإدارة المرافق .

- حماية وتحكم مصدر الطاقة

بعد مناقشة وسائل السيطرة المتعددة التي قد تكتب في ورقة تعليمات.

الجزء الثاني

I. بعد أن تنتهي المجموعة من كتابة ورقة التعليمات الخاصة بهم بقلم الألوان الذي تم إعطاءه لمجموعتهم ويجب أن يمروا على ورقة التعليمات باتجاه عقارب الساعة للمجموعة التالية.
II. سيلاحظون في استلام ورقة التعليمات للمجموعة الأخرى نقاط إضافية بقلم الألوان الخاص بهم ووضع أيضًا علامة متقاطعة على النقاط التي لا يوافقون عليها ستمر ورقة التعليمات باتجاه عقارب الساعة إلى المجموعة التالية.
III. قم بتكرار الخطوة (الثانية) حتى يرى جميع المجموعات ورقة تعليمات جميع المجموعات الأخرى.

الحل المقترح للتمرين رقم (1)

1- عناصر التحكم المادية :

1- إجراءات إدارية :
موظفون يلبسون شارات هوية أو أسماء .
إلغاء حقوق الوصول للموظفين المطرودين .
الزوار : دخول الزوار يتطلب معرفة من هم , لصالح من يعملون , من يزورون , تاريخ الوصول , تاريخ الخروج .
قد يطلب منهم تزويد نوع من أنواع التعريف قبل السماح لهم بالدخول او قد يتم مرافقتهم .

2- إجراءات مكتبية:
وبمعنى أخر ما هي الإجراءات التي تتم عندما يترك الموظفون مكاتبهم مثلا عندما يذهب الموظفون منازلهم في الليل أو عندما يخرجون لتناول الغداء . توضع أجهزة الكمبيوتر المحمولة في إدراج ويقفل عليها ويقفل على الأقراص المرنة أيضا.

أقفال على الأبواب :
- **أبواب أقفال ميكانيكية .**
- **أبواب أقفال ممزوجة (مفتاح وأرقام)**
- **أبواب أقفال الكترونية .**
- **أبواب أقفال حيوية .**

عناصر تحكم أخرى .
- **كاميرات فيديو .**
- **حراس امن .**
- **أسوار خارجية للمباني**
- **أجهزة إنذار .**

3- منع وكشف وإخماد الحرائق :
- **منع التدخين .**
- **استخدام مواد بناء ضد الحرائق .**
- **أجهزة إنذار اكتشاف الأدخنة .**
- **معدات إخماد الحرائق مثل الماء والغاز .**

4-الماء وإدارة المرافق :

- **غرفة الحاسوب في مكان مرتفع وليست في السرداب .**
- **غرفة الحاسب بعيدة عن أماكن انحدارات المياه أو خزانات المياه .**
- **أجهزة إنذار اكتشاف المياه .**
- **منع الأطعمة والمشروبات في غرفة الكمبيوتر .**
- **التنظيف المنتظم لغرفة الكمبيوتر .**

5- مزود الطاقة :

- **مثبتات الفولتية .**
- **المولدات الاحتياطية .**
- **أجهزة تزويد التيار الغير متقطع .**
- **كابلات التيار البديلة .**

<u>عناصر التحكم المنطقية في مستوى التثبيت :</u>

اسألوا المشاركين عن إعادة تعريف عناصر التحكم المنطقية وانتظروا الإجابة .
ذكروا المشاركين بان الهدف من عناصر التحكم بشكل عام هو حمايته من أي مخاطر قد
بينوا للمشاركين أن عناصر التحكم المادية(كالأقفال وأجهزة الإنذار والحراس) قد لا تكون كافية لحماية النظام من الدخول الغير مصرح به لبيانات النظام خاصة إذا كان النظام مرتبط بشبكة محلية أو بشبكة الانترنت ومن هنا فانه لابد من توافر أسلوب أخر لحماية الأنظمة والبيانات التي تقوم بمعالجتها وانه من هنا يظهر دور عناصر التحكم المنطقية .

بينوا للمشاركين انه توجد ثلاثة عناصر أساسية في أمان الوصول المنطقي وهي
- تعريف المستخدم .
- التحقق من المستخدم .
- حماية الموارد (أو امتيازات الوصول) .

ناقشوا المشاركين حول عمل كل عنصر من العناصر السابقة في حماية بيانات وملفات النظام
بينوا للمشاركين انه من خلال قيامنا بعملية المراجعة في إحدى الجهات وجدنا الموظفين يتداولون كلمات السر فيما بينهم بالرغم من وجود كلمة سر لكل موظف وبينوا لهم خطورة ذلك .

<u>إجراءات الدخول :</u>

بينوا للمشاركين انه لكي تكون عناصر التحكم في الدخول فعالة فانه لابد من توفر الإجراءات التالية والتي تزيد من فاعلية إجراءات الدخول واهم تلك الإجراءات الأتي :

- عدم عرض اسم الجهة .
- عدم الترحيب بمحاولات الدخول .
- عدم الإعلام عن النجاح أو الفشل .
- قطع الاتصال بشكل تلقائي .

وضحوا للمشاركين خطورة عدم الأخذ في الاعتبار مثل هذه الإجراءات من أنها قد تحفز وتساعد المهاجمون في اختراق عناصر التحكم المنطقية . لوحظ في الفحص الميداني عدم الاهتمام بهذه الإجراءات

<u>فعالية كلمة السر :</u>

بينوا للمشاركين أن كلمة السر لكي تكون فعالة يجب أن تتضمن العديد من الشروط والتي من أهمها ما يلي :

- تعقيد كلمة السر .
- الحد الأدنى لطول كلمة السر .
- فترة عمر كلمة السر .
- تاريخ كلمة السر .
- سرية كلمة السر .

ناقشوا المشاركين حول أهمية كل شرط من الشروط السابقة . لوحظ في الفحص الميداني عدم تثقيف المستخدم بمخاطر كلمة السر .وعدم متابعتها وتحديثها

بينوا للمشاركين بقية الشروط المتعلقة بكلمة السر والمتمثلة في الأتي :

- تعطيل كلمات سر العاملين التاركين للجهة .
- تغيير كلمات السر للموردين وكذا الافتراضية .
- تقديم إرشادات وإجراءات وتوعية المستخدم .
- التخصيص الأولي لكلمة السر .
- تشفير كلمة السر.

ناقشوا المشاركين حول مضمون كل شرط من الشروط السابقة وأهميته .

اضربوا للمشاركين مثال من الحالات العملية والتي وجد فيها إن بعض الجهات لا يوجد لديها سياسة واضحة متعلقة بكلمة السر وان وجدت في بعض الجهات فهي غير مفعلة حيث نصت سياسة كلمة السر في بعض الجهات أن تتكون كلمة السر من 5- 8 رموز في حين وجد أن بعض كلمات السر تحتوي فقط على 3 رموز .

تمرين للتطبيق رقم (2)

الهدف: يُعد هدف التمرين هو تحديد/ اقتراح وسائل سيطرة متعددة للوصول المنطقي الذي يمكن أن يُستخدم لمنع/تقليل المخاطر في الحالات المختلفة المُقدمة أدناه .

التعليمات :

- القراءة الفردية للتمرين .
- مناقشة الحلول التي تم التوصل إليها في ضمن المجموعة الصغيرة ودونوا الحل الذي توصلتم إليه على ورقة .
- اختيار شخص يمثل المجموعة ليمثلها في عرض الحل

الوقت المخصص: خمس وثلاثون دقيقة

القراءة الفردية: خمسة دقائق

مناقشة المجموعة الفرعية: خمسة عشر دقيقة

استخلاص المعلومات في وجود جميع الأعضاء: خمسة عشر دقيقة

أ) بينما يتعامل نظام المعاشات المُدار بالكمبيوتر مع طباعة أوامر دفع المعاشات متضمنة مبالغ كبيرة من المال،فقد أرادت الإدارة جعل الأفراد مسئولين عن الإضافات/التعديلات للبيانات

ب) هناك خطر وهو محاولة الموظفين الذين تم وقفهم عن العمل بتخريب النظام.

ج) أثناء محادثة عارضة، فقد وجد المراجع بأن السيد جاك كان يستخدم نفس كلمة السر لأكثر من سنتان.

د) كلمة السر الخاصة بالسيد خالد هي abc.

ه) بينما كانت الآنسة منى مُدخلة بيانات فقط، فقد أراد السيد لين، وهو مسئول النظام بتعيين متطلبات الوصول المطلوب الأدنى.

و) تلبّي تطبيقات البرامج حاجة المبيعات والمالية والمخازن وأقسام إدارة المقترضين والموظفين في هذه الأقسام التي تستخدم التطبيق.

ز) أراد السيد علي، وهو مسئول النظام، التأكد من إنه لا يتم استخدام تطبيق البرنامج في العطلات بدون تصريح خاص.

ح) أراد السيد أحمد، وهو مسئول أمن تقنية المعلومات، بأن يتم إخباره بصورة دورية بمحاولات تسجيل الدخول الفاشلة.

ط) ووجدت الآنسة سلوى، وهي المراجع، أثناء تفتيش عرضي لموقع الكمبيوتر بأن كثير من المداخل الطرفية ما زالت مُسجلة الدخول إلى نظام التطبيق.

ي) أثناء محاولة الآنسة حنان ، وهي المراجع، بفحص مداخل التحكم، حاولت تسجيل الدخول للنظام عن طريق تخمين ثلاثين كلمة سر مُختلفة ولكنها لم تستطيع الوصول لأن كلمة السر ليست سهلة حتى يتم خرقها.

(الحل المقترح للتمرين رقم 2)

أ- يجب أن يكون لكل مستخدم رمز تعريف فريد، و يجب أن يتم تخزين رمز تعريف لآخر أو المستخدم الأخير الذي عدل البيانات ويجب أن تخزن في قاعدة البيانات لتثبيت المسئولية .

ب- يجب أن يكون هناك إجراءات بها تفاصيل إنهاء الخدمة لموظف أو تحويله ويتم إبلاغ مسئول النظام بهؤلاء المستخدمين لإلغاء رمز التعريف الخاص بهم .

ج- يجب أن يجبر النظام المستخدمين بشكل إلى ليغيروا كلمات سرهم في الفترات المحددة , فترة تغيير كلمة السر يمكن أن تتفاوت طبقا لصنف المستعمل , فالمستخدمين المهمين مثل المبرمجين يجب أن تتغير كلمات سرهم بشكل أكثر .

د- طول كلمة السر يجب أن تحدد , قد تكون مابين 6 إلى 8 رموز .
- يجب أن يضمن النظام أن كلمة السر هي مزيج حرفي رقمي .
- يجب نصح المستخدمين أن لا يخصصوا كلمات السر التي يمكن أن تخمن بسهولة .

ه- حقوق القراءة والكتابة هي التي يمكن أن تزود بينما حقوق التعديل أو الحذف فلن تزود
- حقوق الدخول إلى الجداول الرئيسية لن تزود .
- برنامج دخول مكتوب قد يزود للدخول الضروري .
- كتابة برنامج خاص للدخول إلى أماكن معينة فقط

و- يجب تخصيص برامج دخول منفصلة في التطبيق .
- يجب أن يخصص المستخدمون وصول أو دخول إلى الوحدات ذات العلاقة بهم .
- برنامج الدخول لكل قسم يحدد الدخول فقط إلى الوحدات الخاصة بهم .
- دخول طرفي محدد حيث أن وحدات طرفية معينة مخصصة لكل قسم .

- دخول من خلال أطراف معينة ومخصصة للأقسام المعنية فقط.

ز- تحديد أوقات وأيام يسمح بالدخول إلى التطبيق .

ح- سجل تدقيق لتسجيل محاولات الدخول الفاشلة .

- مسئول الأمن يجب أن يبلغ رسميا في فترات معينة بأي انتهاكات أمنية .

- انقطاع الكهرباء أو غلق تلقائي للمحطات الطرفية المهملة لفترة معينة .

ي- يجب أن يكون هناك حد أقصى لعدد محاولات الدخول بحيث انه إذا تم إدخال كلمة السر الخاطئة لأكثر من عدد محدد فان تعريف المستخدم يجب أن يقفل بشكل ألي .

عناصر تحكم منطقية أخرى:

بينوا للمشاركين أن هناك عناصر تحكم منطقية أخرى تتمثل في الأتي :

- تحديد عدد جلسات العمل المتزامنة .
- وضع حدود على ساعات العمل .
- حصر محاولات تسجيل الدخول .
- انتهاء وقت الوحدات الطرفية بشكل تلقائي .
- تخصيص الوصول بوحدات طرفية .

ناقشوا المشاركين حول كل عنصر من تلك العناصر و أهميته في حماية البيانات .

بينوا للمشاركين أننا لاحظنا من خلال مراجعة بعض الجهات أن بعض الأنظمة كانت تسمح بفتح عدة جلسات في آن واحد وباستخدام نفس كلمة السر .

اذكروا للمشاركين إننا وجدنا في إحدى الجهات التي تم مراجعتها إن النظام المستخدم لديها يحتوي على خاصية السجل LOG إلا أن هذه الجهة لم تقم بتفعيل تلك الخاصية كما انه في جهة أخرى وجدنا تفعيل مثل هذا السجل لتسجيل كافة الحركات إلا أن الجهة لا تقوم بمراجعته .

مواضيع للمناقشة :

حفزوا المشاركين على مناقشة الاستفسارات الآتية :

- الحاصلين على الدخول غير المصرح به في حال غياب إجراءات عناصر التحكم (المهاجمون).
- اثر ضعف/غياب عناصر تحكم الدخول المنطقية .
- ما هي أصول تقنية المعلومات التي تحتاج إلى حماية ؟

أسالوا المشاركين عن الأشخاص الذين لهم مصلحة في المهاجمة وانتظروا ردودهم .

ناقشوا المشاركين ردودهم دونوها إجابات المشاركين على حامل الورق .

المهاجمون :

قارنوا إجابات المشاركين مع ما هو معروض بالشريحة .

وضحوا النقاط التي لم تغطيها إجابات المشاركين وناقشوها معهم .

اثر ضعف غياب عناصر التحكم المنطقية :

ناقشوا المشاركين حول الآثار المترتبة على عدم كفاية عناصر التحكم المنطقية والتي قد تتمثل في إحدى الآتي :

- كشف معلومات غير مصرح بها .
- تعديل غير مصرح لبيانات .
- خرق تكامل النظام .

ما هي الأصول التي يجب حمايتها :

ناقشوا المشاركين حول الموارد والملفات التي تحتاج إلى حماية والتي من أهمها الأتي :

- بيانات الملفات .
- التطبيقات .
- ملفات كلمات السر .
- برامج النظام .
- ملفات السجل .
- الملفات المنتظرة والمؤقتة .

بينوا للمشاركين أهمية حفظ مثل هذه الموارد ووضحوا خطورة إمكانية الوصول لإحدى هذه الموارد والملفات والتعديل فيها . لوحظ في الفحص الميداني حفظ البيانات في مكان واحد

لخصوا مع المشاركين النقاط الرئيسة التي تطرقتم إليها خلال هذه الجلسة وهي :

- عناصر التحكم المادية والبيئية ومخاطر ضعفها .
- عناصر التحكم المنطقية ومخاطر ضعفها .

أساليب الرقابة المدعومة بالحاسب

هدف الجلسة :

في نهاية هذه الجلسة سيكون في مقدور المشتركين وصف دور أساليب الرقابة المدعومة بالحاسوب (CAATs) والأنواع المختلفة المتاحة لتأكيد صلاحية البرامج وتحليل البيانات.كما سيتعرفون أيضا على متى وأين يستخدمون هذه الأساليب.

الإعداد :

1- مراجعة دليل المدرب ودليل المشارك بشكل مفصل.

2- إعداد مخططكم للجلسة والتدريب عليه إلى أن تشعروا بالثقة والراحة التامة.

3- التأكد من وجود جميع الشرائح والنشرات للتوزيع الخاصة بهذه الجلسة ومرتبة حسب الأرقام

4- فحص التجهيزات للتأكد من أنها تعمل بشكل جيد (آلات العرض وحاملات الأوراق والأقلام .الخ)

النقاط التي سيتم تغطيتها	الأسلوب	مستلزمات التدريب	الهدف	الوقت اللازم
نظرة عامة عن الجلسة	محاضرة	عرض الشرائح		
هدف الجلسة	محاضرة	عرض الشرائح		

التعريف بأساليب الرقابة المدعومة بالحاسوب	محاضرة	عرض الشرائح		
خيارات العبور إلى بيانات الجهة الخاضعة للرقابة.	محاضرة ونقاش	عرض الشرائح		
مسائل متعلقة بتنزيل البيانات	محاضرة ونقاش	عرض الشرائح		
أدوات تحليل البيانات	محاضرة ونقاش	عرض الشرائح		

1- نظرة عامة عن الجلسة

قدموا هدف الجلسة بشكل مختصر مع التركيز على وصف دور CAATs والأنواع المختلفة المتاحة لتأكيد صلاحية البرامج وتحليل البيانات و أيضا على متى وأين يستخدمون CAATs وطرق النفوذ للبيانات..

بينوا
للمشتركين أنه في هذه الجلسة سيتم التركيز كذلك على مفاهيم قاعدة البيانات.

2- أهداف التعلم :

بينوا للمشاركين أنه في نهاية الجلسة سيكون في مقدورهم وصف دور CAATs والأنواع المختلفة المتاحة لتأكيد صلاحية البرامج وتحليل البيانات.كما سيتعرفون أيضا على متى وأين يستخدمون CAATs وطرق النفوذ للبيانات.

أعرضوا الشريحة

3- التعريف بأساليب الرقابة المدعومة بالحاسوب

أعرضوا الشريحة

ومن خلال هذه الشريحة

بينوا للمشاركين إن أساليب الرقابة المدعومة بالحاسب أو CAATs قد تُعرّف كأدوات معتمدة على الحاسوب يمكن استخدامها لتحسين فعالية وكفاءة عملية الرقابة؛ والتعريف البديل هو "أساليب يستخدمها المراقبون يُستخدم فيها الحاسب كأداة لجمع وتحليل بيانات الرقابة".

وضحوا أن استخدام CAATs لا يغير أهداف الرقابة، ولكن التغييرات مطلوبة فقط على مستوى منهجيات الرقابة. و حاليا في أغلب، بيئات معالجة المعلومات، تكون مستندات الرقابة إما غير متاحة على ورق، أو تكون النسخة الورقية متحصل عليها من البيانات الإلكترونية(ونتيجة لذلك تكون أقل موثوقية منها). وبالتالي، و يجب على المراقب الاعتماد على CAATs لجمع مستندات كافية وذات صلة ويعتمد عليها.

أعرضوا الشرائح الخاصة

ومن خلال هذه الشريحة

وضحوا أنه نتج عن استخدام CAATs فوائد، ليست فقط على مستوى تنفيذ عمليات الرقابة ولكن أيضًا في

مرحلة التخطيط. رغم أن التركيز الأولي لـ CAATs كان في الرقابة المالية ورقابة المطابقة، وتمشيًا مع الطبيعة المتغيرة واهتمام الأجهزة العليا للرقابة ، تزايد استخدام CAATs لتحقيق نتائج جيدة في رقابة الأداء والرقابة التفتيشية.

4 - أنماط أساليب الرقابة المدعومة بالحاسوب

أعرضوا الشرائح

من خلال هذه الشريحة

بينوا للمشاركين أنه يمكن تقسيم CAATs إلي مجالين منفصلين من العمليات . يتعلق الأول بتأكيد صلاحية البرنامج و يتعلق الثاني بتحليل البيانات.

وضحوا أن CAATs الموجهة للبرامج تركز على التحقق من صحة مختلف العمليات في البرامج، (التي يمكن القيام بها نظريا رغم ندرة ذلك عمليًا) ، ثم أمتد استخدام CAATs إلى الرقابة الكاملة للبرامج.

أشيروا إلى أن CAATs الموجهة للبيانات تتجاهل البرامج المستخدمة لإنتاج البيانات، وتركز حصرياً على تحليل البيانات.ولا يعني ذلك بالضرورة أن CAATs الموجه لتحليل البيانات هي تمكّن من إجراء الاختبارات الأساسية والفنية دون سواها مع CAATs الموجة لفحص البرامج الموجودة بالأنظمة بينما تكون رقابة البرنامج عمومًا مفيدة فقط في الرقابة على المطابقة أو في أفضل الظروف في التصديق على القوائم المالية، كما يمكن استخدام تحليل البيانات في رقابة الأداء وأيضًا الرقابة التفتيشية.

بينوا أنه يمكن أن يستخدم تحليل البيانات غالبًا على نحو فعال جدًا في تقييم الفعالية الحقيقية لعناصر التحكم، بدلاً من الاعتماد على تحليل البرامج (التي هي عنصر واحد فقط من عناصر التحكم بتقنية المعلومات).

أعرضوا الشرائح الخاصة

من خلال هذه الشرائح

بينوا للمشاركين أنه يمكن يستخدم لـ CAATs كذلك لتحليل بيانات الجهة الخاضعة للرقابة.و هذا هو الأسلوب السائد بسبب سهولة استخدامه. يتوفر لتحليل البيانات تشكيلة من برمجيات التدقيق وأدوات لغة SQL ، والتي صممت بصفة عامة للاستخدام في أنظمة الحاسب الشخصي.وتتلاءم هذه الأدوات مع رقابة المطابقة والأداء والرقابة القضائية / التفتيشية بالإضافة إلى التدقيق المالية.

أشيروا إلى أن أساليب تحليل البيانات الشائعة تشتمل على عمليات التجميع والترصيف (التقسيم إلى طبقات) ومنجم البيانات واختيار العينات والتقارير الاستثنائية وفحص التسجيلات المكررة وكذلك التقادم وكشف الثغرات.

5- اعتبارات استخدام أساليب الرقابة المدعومة بالحاسوب

وضحوا للمشاركين أنه هناك مخاطر محتملة تنشأ من اعتماد المراقب على نتائج تحليل البيانات لأجل قراراته الخاصة بالرقابة. يجب أن يكون المراقبون على دراية بالمخاطر إذا كانوا يعتمدون حصريًا على تحليل البيانات لنتائج الرقابة أو إضافة CAATs لفحوصات الرقابة غير المثبتة في الحاسب لتقديم سند أو دليل مؤيد. يجب أن يقوم المراقبون بالتحقق من نتائج تحليل البيانات كلها (أو على الأقل عينة منها) عن طريق الاستشهاد بالوثائق الورقية. من المهم جدًا إجراء مراجعة لعناصر التحكم بنظام تقنية المعلومات لتقييم درجة الموثوقية للبيانات التي أُدخلت أو عولجت بواسطة النظام ، كما يجب على المراقب التحقق من تكامل البيانات المنزلة عن طريق التوفيق مع عنصر تحكم أو ملخص التجميعات.

أكدوا على وجوب فهم المراقبين نظام تقنية المعلومات للجهة الخاضعة للرقابة، والأكثر من ذلك أهمية هو فهم البيانات. و سوف يعتمد ذلك على مدى التدريب الذي تلقوه ومدى الخبرة في استخدام هذه الأدوات.

أعرضوا الشرائح الخاصة

من خلال هذه الشرائح

بينوا أن التطبيقات المستخدمة من قبل الجهة الخاضعة للرقابة ، والتي تعتمد عليها الأعمال التجارية الجوهرية، تعتبر من أحد أسباب استخدام تحليل البرنامج. وقد يكون هناك سبب آخر وهو أن تحليل البيانات بمفرده لا يمكن الاعتماد عليه لتقديم تأكيد فيما يتعلق بكفاية وفعالية عناصر التحكم.

أعرضوا الشرائح الخاصة

من خلال هذه الشرائح

أشيروا إلى أن استخدام أساليب الرقابة المدعومة بالحاسب له فوائد عديدة للأجهزة العليا للرقابة، وبالتالي فإنه يحبذ إجراء تحليل التكلفة مقارنة بالعائد لاستخدام CAATs في بيئة رقابة محددة. غالبا ما قد يكون هذا التحليل تقييم نوعي، وبرغم ذلك فهو يساعد على خلق اتجاه لتوقعات أكثر واقعية للعوائد والتكاليف المستخدمة.

بينوا للمشاركين أن بعض العوامل الهامة ترجح وتشجع على استخدام CAATs في العمل الرقابي مثل إمكانية الاستخدام المتكرر لـ CAATs في المهمات الرقابية المستقبلية أو منح أولوية هامة للمجالات ذات مخاطر الرقابة العالية وكذلك أساليب الرقابة المماثلة التي لا تعتمد على الحاسب تكون غير عملية أو عالية التكاليف.

6- خيارات العبور إلى بيانات الجهة الخاضعة للرقابة

أعرضوا الشريحة
من خلال هذه الشريحة

إلى وجود طريقتين يمكن للمراقب أن يستخدم فيهما CAATs لتحليل بيانات العميل:

أشيروا
- تشغيل CAAT على نظام تقنية المعلومات الخاص بالجهة الخاضعة للرقابة، سواء مباشرة من حاسب شخصي أو شاشة طرفية أو عن طريق توصيل حاسب المراقب بشبكة الجهة الخاضعة للرقابة
- تنزيل البيانات على نظام تقنية المعلومات الخاص بالمراقب أو جهاز الرقابة وتشغيل CAAT من حاسبه.

بينوا أن تثبيت برنامج CAATs على نظام تقنية المعلومات الخاص بالجهة الخاضعة للرقابة قد يكون غير عملي بسبب اختلافات البرامج الفنية الخ. في العادة، بدلاً من تثبيت برنامج CAATs الخاص بجهاز الرقابة، وقد يستخدم المراقب الأدوات الموجودة في نظام الجهة الخاضعة للرقابة.في هذه الحالة سيحتاج المراقب للتعرف على الأدوات المتاحة في تشكيلة متنوعة وكبيرة في محيط تقنية معلومات العميل

أشيروا إلى أن تشغيل CAATs على نظام الجهة الخاضعة للرقابة له بعض المخاطر المحتملة مثل اضطرابات أنظمة الجهة الخاضعة للرقابة، مع تبعات محتملة لكل من الأداء وتكامل البيانات (هناك احتمال أن تتغير أو تُحذف بيانات الجهة الخاضعة للرقابة بدون قصد) تظهر هذه المشكلة أيضًا في الطريقة التي يستخدم فيها ارتباطيه البيانات بين حاسب المُراجع ونظام تقنية المعلومات الخاص بالجهة الخاضعة للرقابة.

7 - مسائل متعلقة بتنزيل البيانات

بينوا للمشاركين أن العامل الهام في التنزيل الناجح للبيانات هو تأكيد تكامل البيانات المنزلة، والذي غيابه يجعل كامل عملية CAATs غير موثوقة. هناك عدة مسائل متصلة بتكامل البيانات مثل:

- الحصول بلا استثناء على عدد سجلات البيانات في كل ملف من الجهة الخاضعة للرقابة. ومن المستحسن أيضًا إما تجميع إجماليات التحكم لكل ملف من الجهة الخاضعة للرقابة و/أو الحصول على وثائق مطبوعة تمثل أرقام إجمالية للبيانات التي تحتويها هذه الملفات (مثل ملخصات التقارير المالية).
- إجراء تأكيد تكامل البيانات المنزلة باستخدام أداة CAAT لإعادة حساب عدد التسجيلات وإجماليات البيانات التي تم جلبها إلى داخل برنامج CAAT، ومقارنتها بالأرقام التي قدمتها الجهة الخاضعة للرقابة.
- الاحتفاظ بالبيانات المستلمة في صيغتها الأصلية من الجهة الخاضعة للرقابة سليمة ولا تُمس. في حالة الطلب من المراقب إعادة البيانات الأصلية إلى الجهة الخاضعة للرقابة، يجب أن يتم الاحتفاظ بنسخة من البيانات بدون مس على نظام تقنية معلومات المراقب.

أكدوا للمشاركين على ضرورة الربط بصفة واضحة بين أسلوب الرقابة المدعوم بالحاسوب وهدف (أهداف) الرقابة وتجنب إغواء الحصول على بيانات زائدة أو غير ذات صلة. مع الإشارة إلى أنه قد يكون من الأسهل أحيانًا تنزيل جميع جداول أو حقول الجداول الموجودة في قواعد بيانات الجهة الخاضعة لرقابة حيث قد يتطلب الأسلوب الأفضل انتقاءً وقت وموارد أكثر. يجب الربط بصفة واضحة بين أسلوب الرقابة المدعوم بالحاسوب وهدف (أهداف) الرقابة وتجنب إغواء الحصول على بيانات زائدة أو غير ذات صلة. لكن، قد يكون من الأسهل أحيانًا تنزيل جميع جداول أو حقول الجداول الموجودة في قواعد بيانات الجهة الخاضعة لرقابة حيث قد يتطلب الأسلوب الأفضل انتقاءً وقت وموارد أكثر.

أشيروا إلى أن المراقب مطالب بانتهاج أسلوب أكثر انتقائية في اختيار البيانات عند ما يتعلق الأمر بالرقابة المالية ورقابة المطابقة، حيث أن المراقب يتجه إلى "تعريف" البيانات من أجل إبراز النزعات أثناء القيام برقابة الأداء أو الرقابة التفتيشية.

بينوا أنه يجب على المراجع، بقدر الإمكان، اختيار بيانات في الشكل الأقرب للمعاملات الأصلية (الصفقة أو الملفات الأولية / الجداول الرئيسية بدلاً من الملخصات أو الملفات / الجداول الثانوية) وذلك لكي تبقى معالجة البيانات في أقل حد.

أكدوا للمشاركين أنه لكي يتم اختيار البيانات المطلوبة، يحتاج المراقب للتفهم الكامل للبيانات المتاحة في نظام تقنية المعلومات الخاص بالجهة الخاضعة للرقابة والمتعلقة بالأعمال التجارية بدلا من منظور فني ويمكن تحقيق هذا التفهم من مصدرين، وثائق النظام ذات الصلة بهيكل البيانات والمناقشة مع العاملين في الجهة الخاضعة للرقابة (وخاصة إدارة تقنية المعلومات و"صاحب النظام"). والمصدر الآخر هو مراجعات النظام السابق من قبل المراقبين.

قدموا للمشاركين الأدوات المتاحة للمراقبين لتحليل البيانات مثل برامج التدقيق المعممة وأدوات SQL ومنظومة أكسس وجداول البيانات.

مفاهيم تصميم قاعدة البيانات

هدف الجلسة

- تحليل قاعدة البيانات
- التعرف على قاعدة البيانات العلائقية
- تعلم IDEA
- تطبيق عملي على IDEA

التحضير

- مراجعة مواد هذه الجلسة
- مراجعة كل من دليل المدرب والمشارك
- إعداد مخطط جلسة والتدريب عليه إلى أن تشعر بالثقة والراحة التامة

- التأكد من وجود كافة الشرائح المتعلقة بالجلسة
- التأكد من جاهزية المعدات التي سوف تستخدم في العمليات التدريبية

النقاط التي يتم تغطيتها	الأسلوب	الوقت
أدوات تحليل البيانات	عرض الشرائح ومناقشة	
تصميم مفاهيم قاعدة البيانات	عرض الشرائح ومناقشة	
قاعدة البيانات العلائقية	عرض الشرائح ومناقشة	
أمثلة لتطبيقات قاعدة البيانات العلائقية	عرض الشرائح ومناقشة	
مفاهيم العلاقات	عرض الشرائح ومناقشة	
مثال على تصميم قاعدة البيانات	عرض الشرائح ومناقشة	
تركيبة البيانات ووصف السجل	عرض الشرائح ومناقشة	
جلب ملف إلى IDEA	عرض الشرائح ومناقشة	
تنزيل ملف	عرض الشرائح ومناقشة	
التواصل عبر الشبكات	عرض الشرائح ومناقشة	
هيئة الملف	عرض الشرائح ومناقشة	
تعديل الملف	عرض الشرائح ومناقشة	
التوثيق	عرض الشرائح ومناقشة	
نظرة شاملة على IDEA	عرض الشرائح ومناقشة	
مشروع IDEA	عرض الشرائح ومناقشة	

مفاهيم تصميم قاعدة البيانات

1	*** أدوات تحليل البيانات** **أسأل :** ما هي البرامج الرقابية المخصصة **أسأل :** ما هي لغة الاستعلام المدمجة والأدوات المبنية على– لغة الاستعلام المدمجة **أسأل :** ما هو ميكروسوفت أكسس	(2/1)	•**برامج رقابة مخصصة** وهذه عبارة عن حزم برامج جاهزة أنشئت خصيصًا للمراجعين لاستخدامها في تنوع كبير من البيئات الفنية. الحزمتان الرئيسيتان للأغراض العامة هما IDEA (استخراج وتحليل البيانات التفاعلي) وIDEA (لغة أمر الرقابة) •**لغة الاستعلام المدمجة والأدوات المبنية على–لغة الاستعلام المدمجة**SQL هي لغة تستخدم على نطاق كبير لتحديد ومعالجة البيانات المخزنة في نظم الإدارة بقاعدة بيانات علائقية (RDBMS). • **Microsoft Access:** Microsoft Access هو تطبيق قاعدة بيانات علائقية لسطح المكتب (desktop) يشكل جزء من مجموعة Microsoft's Office Professional لتطبيقات الأتمتة المكتبية. إضافة لاستخدامه العادي لتطبيقات قاعدة البيانات الصغرى، يمكن لـ إمداد المراجع بأداة استعلام سهلة الاستعمال وفي المتناول.
2	*** تصميم مفاهيم قاعدة البيانات** **أعرض :** الشريحة رقم **أسأل :** ما هو الفرق بين البيانات و المعلومات .	3	الفرق بين البيانات والمعلومات. البيانات هي المفردات أو المادة الخام المخزنة في نظام الحاسب في صيغة إلكترونية لا يمكن فهمها، في معظم الحالات، بمفردها. في حين المعلومات هي نفس البيانات في صيغة معالجة تكون ذات معنى للمستخدمين.
3	**قاعدة البيانات العلائقية** **أعرض :** الشريحة رقم **أسأل :** ما هو الفرق بين قاعدة البيانات و قاعدة البيانات العلائقية	4	قاعدة البيانات هو مجموعة من "الكائنات" objectes– جداول tables،الاستعلام queries or views، تقاريرreports، إطارات forms. قاعدة البيانات العلائقية RDBMS هي مجموعة من الجداول المرتبطة ببعضها البعض عن طريق علاقات. تتضمن قواعد البيانات العلائقية على بيانات وتركيب هذه البيانات من حيث الأسماء، والأنواع والأحجام وهي مرتبطة ببعضها لتشكيل تكاملية للبيانات. ولها ميزة أخرى مثل الأمن والتحكم، ومدير قاعدة البيانات
4	*** قاعدة البيانات العلائقية** **أسأل :** ما هي مكونات قاعدة البيانات العلائقية		البيانات ، تركيبة البيانات، علاقات البيانات، تكامل البيانات، ضوابط وأمن البيانات.
5	*** قاعدة البيانات العلائقية** **أشرح :** للمشاركين المثال الموجود في الشريحة.		
6	*** قاعدة البيانات العلائقية**		

	أشرح : للمشاركين العناصر الموجودة على الشريحة وفي نفس الوقت أعط مثال		
7	*** أمثلة لتطبيقات قاعدة البيانات العلائقية** **أسأل :** ما هي قواعد البيانات المشهورة التي هي من نوع علائقية		هي OrIDEAe، IBM DB2، Microsoft SQL Server، Sybase SQL Server، Informix وIngress ولكن أكثر المنتجات استخداما على نطاق واسع هي OrIDEAe وMS-SQL Server
8	*** مفاهيم العلاقات** **أشرح :** للمشاركين بالتفصيل محتويات هذه الشريحة مع ذكر مثال لقاعدة بيانات علائقية		**المفتاح الرئيسي Primary Key** : هو عبارة عن حقل وحيد في الجدول ولا يمكن أن يتكرر أو تكون قيمته null .(فراغ) **العلاقاتٌ Relationships:** هناك أربع أنواع من العلاقات هي : One to one , One to many , many to one , many to many . **المفتاح الثانوي Forgien Key:** هو عبارة عن مفتاح رئيسي في جدول آخر ولكنه ليس مفتاح رئيسي بمفرده في هذا الجدول بالذات.
9	*** مثال على تصميم قاعدة البيانات** **أشرح :** للمشاركين بأن هذه الرسمة تبين العلاقات في قاعدة البيانات العلائقية		
10	*** تركيبة البيانات ووصف السجل** **أشرح :** للمشاركين الشريحتين وبين محتوياتهما **أعط :** للمشاركين مثال وأكتب على لوح الكتابة وأرسم جدول يحتوي على أسماء الحقول وأنواعها وأطوالها. **وزع :** المثال على المشاركين رقم 1.4 ب ووضح لهم المثال وأطلب منهم الحل خلال 10 دقائق وبعد ذلك وزع عليهم الحل للسؤال		
11	*** جلب ملف إلى IDEA** **وضح :** للمشاركين بإيجاز محتوى الشريحة ,إن الشرائح القادمة سوف تتحدث عن كل عنصر في الشريحة		
12	*** تنزيل ملف** **أعرض :** الشريحة رقم **أسأل :** ما هي وسائط التخزين المتاحة		**تنزيل الملف Downloading file:** هناك وسائل عديدة يمكن تنزيل الملف بها، هذه الوسائل تشمل القرص المرن والقرص المدمج والشرائط والبريد الإلكتروني ووسائل الاتصال أو ارتباط بالشبكة.

13	*** التواصل عبر الشبكات** **أشرح :** للمشاركين وبين لهم مدى أهمية نقل البيانات عبر الشبكات	15	وسائل الاتصال أو ارتباط بالشبكة. ارتباط الشبكة يكون أصعب في الإعداد للمرة الأولى. لكن، لاستخدام علائقية قاعدة البيانات المفتوحة (ODBC) في الشبكة المحلية، يحتاج المراجعين إلى صلاحية لاستخدام قاعدة البيانات من الجهات الخاضعة للرقابة التي في معظم الوقت ستعارض إعطاء هذه الصلاحيات. إن هذه الطريقة أثبتت أنها فعالة وسريعة وخاصة لتنزيل البيانات الكبيرة جدًا.
14	*** هيئة الملف** **ناقش وأشرح :** للمشاركين بالتفصيل عن أنواع هيئة الملفات	16	**هيئة الملف File Format:** هناك عدة هيئات للملفات كالآتي: **ملفات ذات طول ثابت** : الملفات ذات الطول الثابت تحتوي على سجلات لها نفس الطول ولا يوجد فواصل تعريفيّة أو تعريف ذاتي لطول البيانات التي سوف تكون في السجل ويجب أن يعرف طول السجل في هذه الحالة. **وملفات محددة** : الملفات المحددة هي طريقة من طرق استرداد البيانات ووضع البيانات على شكل صفوف وأعمدة كالجدول وتعتبر ملف نصي ويفصل بين السجلات بالطرق التالية (فراغ ، فاصلة، نقطة، وكوما) **ملفات تقرير، ملفات ذات طول متغير**: الملفات ذات الطول المتغير تستخدم طول ملف معروف مسبقا تحتوي على طول السجل في الملف وكل سجل يحتوي على حقل يحدد طول السجل والملفات المتغيرة تستخدم فاصل أو محدد لتعريف نهايات كل سجل. ويمكن أن تكون MS-Excel أو MS-Access. بينما عند استخدام علائقية قاعدة البيانات المفتوحة لا يهم تنسيق الملف.
15	*** تعديل الملف** **ناقش وأشرح :** للمشاركين تعديل الملفات		**تعديل الملف File Modification:** عند تنزيل البيانات قد تتغير أو يحصل لها تلف أو إضافات رموز أخرى. ولذا، على المراجعين أن يكونوا على علم بهذه المواقف ويجهزوا أنفسهم بالأدوات القادرة على تعديل البيانات إلى حالتها الأصلية وحذف الرموز التي أضيفت.

16	*** التوثيق** **ناقش و أشرح :** للمشاركين أهمية عملية التوثيق		**الوثائق Documentation :** هذا هو أهم جزء من عملية تنزيل وتحليل البيانات. يجب أن يتضمن التوثيق نوع الاستفسارات المستخدمة، ومتى وأية بيانات تم تنزيلها وماذا كانت نتائج الاستعلامات والتقارير التي نتجت. يجب تخزين الوثائق في صيغة إلكترونية وورقية.
17	*** نظرة شاملة على IDEA** **أعرض :** للمشاركين برنامج IDEA وأعرض لهم الشاشات الرئيسة في هذا البرنامج مثل شاشة Overview وشاشة Dataview وشاشة Log		
18	*** مشروع IDEA** **أعرض :** للمشاركين المشروع الذي سوف يطبقونه عمليا IDEA الموجود لديهم في دليل المشارك وسوف نعمل جماعيا نبدأ في كل مرحلة جديدة بعد انتهاء من تنفيذ المرحلة السابقة. **أسال :** المشاركين بأن لا يتحرجوا إذا أرادوا توضيح أي من الأوامر التي تم شرحها وتطبيقها وابلغهم بأن هناك تمارين سوف يطبقونها لتطبيق ما أخذوه علميا.		
19	*** تمارين**		

نبذة عن نظام التيم ميت

دليل الاستخدام
Team mate
نظام إدارة التدقيق
EWP
أوراق عمل الكترونية
كيفية الدخول إلى البرنامج
إنشاء مشروع جديد
إكمال إعدادات المشروع وتحديد فريق العمل والأدوار
إحضار برامج العمل من مكتبة Team Store
ملاحظات التدقيق

بعض الأسئلة التي يستخدمها المراجع لفحص مراكز المعلومات

مرفق ضمن دليل المشارك نبذة عن تلك الأسئلة

المملكة العربية السعودية
ديوان المراقبة العامة
الرياض

Kingdom of Saudi Arabia
General Auditing Bureau
Riyadh

اللقاء التدريبي
الرقابة على البيانات المالية
باستخدام الحاسب الآلي

(دليل المشارك)

12-1430/11/17هـ-10/31 -2009/11/5م

إعداد المدربين

خالد بن حسن الصبياني

جمال بن عيد المطيري

عبدالعزيز بن حسين الصبياني

مقدمة

نظرا للتطور الكبير والملحوظ للجهات الخاضعة للفحص والرقابة في مجال الحاسب الآلي وأصبح من الضروري تبني المراجعة الآلية للبيانات الآلية للجهات وتوفير الوسائل اللازمة للرقابة والتدريب الكافي للمراجعين وتوفير البنية التحتية للأجهزة وتطوير النظم المختلفة ونشر ثقافة الحاسب الآلي وكذلك التدريب المستمر في مجال الحاسب الآلي بشكل عام والمراجعة الآلية على وجه الخصوص مما سيسهل عملية التحول للمراجعة الآلية كما انه حدثت تغييرات هائلة في تقنية المعلومات وبيئة تشغيلها في السنوات الأخيرة وهذه التغيرات تؤكد على الحاجة لإدارة المخاطر التي تتعلق بتقنية المعلومات بشكل أفضل والاعتماد على أنظمة المعلومات الإلكترونية وتقنية المعلومات من الأعمال الجوهرية. بالإضافة إلى ذلك فإن البيئة التنظيمية تفرض رقابة أكثر صرامة على المعلومات بدافع كوارث تزايد إفشاء المعلومات والتزييف الإلكتروني المتزايد، وتفهم المخاطر التي تتعلق بتقنية المعلومات في الوقت الحاضر.

وبالإضافة إلى أهمية الأجهزة والبرامج والبيانات المستخدمة في تقنية المعلومات كأصول هامة لأي جهة، فإن تقنية المعلومات غالباً ما تنطوي على عمليات الكترونية للمعاملات اليومية للجهة ، الأمر الذي يجعل من هذه المعلومات بيئة هامة لإنجاز المعاملات التي في النهاية ينتج عنها عمليات مالية، مثل الشراء أو البيع أو صرف الرواتب وغيرها.

وبناءً على ما تقدم فإن مهنة المراجعة جعلت من بيئات تقنية المعلومات مجالاً واسعاً لعملها، وذلك لدرء المخاطر المترتبة على استخدام تقنية المعلومات من جهة، والاستفادة من التسهيلات والإمكانيات التي يتيحها استخدام تقنية المعلومات في أعمال المراجعة من جهة أخرى، ويطلق على تعامل المراجع مع تقنية المعلومات مصطلح "المراجعة الآلية"، والتي تعني تعامل المراجع مع تقنية المعلومات من ناحية تحليل أنظمتها أو فحص مخرجاتها أو استخدامها في عملية المراجعة.

المراجعة الآلية

في مفهومها الواسع فإن المراجعة الآلية تشمل:

1. المراجعة خلال الحاسب الآلي:- وفي هذا النوع من المراجعة يقوم المراجع بفحص السياسات والإجراءات الأمنية والصلاحيات والتكامل في الأنظمة الآلية عن طريق الفحص الميداني والتحليلي للنظم الآلية والتأكد من تحقق الاعتمادية والجاهزية والسرية للأنظمة الآلية وتعبئة ومناقشة الاستبيانات الخاصة بمركز المعلومات (Questioners)
2. المراجعة حول الحاسب الآلي:- وتعني القيام بعمليات المراجعة على مدخلات ومخرجات النظام وبحث إجراءات النظام الخاصة بالضوابط والصلاحيات وإمكانية التعديل، ويهدف هذا النوع إلى التأكد من مصداقية (موثوقية) البيانات المستخرجة عن طريق النظم الآلية.
3. المراجعة باستخدام الحاسب الآلي:- وفي هذا النوع يقوم المراجع باستخدام تطبيقات آلية لتحليل ودراسة البيانات محل المراجعة –مثل استخدام برنامج IDEA وقواعد البيانات الأخرى لتحليل البيانات، كذلك يندرج تحت هذا النوع تنظيم أعمال المراجعة وأوراق العمل

باستخدام النظم الآلية مثل استخدام نظام "تيم ميت". وهذا الجانب الذي سنركز عليه في دورتنا الرقابة على البيانات المالية باستخدام الحاسب الآلي .

ومن منطلق اختصاص الديوان والأجهزة الرقابية الأخرى بالرقابة اللاحقة على أموال الدولة المنقولة والثابتة والتأكد من حسن استخدامها، فقد جعل من أولوياته التعامل مع تقنية المعلومات كمراجع على بيئاتها وكمستخدم مستفيد منها في الوقت نفسه وذلك بتطبيقه أنواع المراجعة الآلية السابقة .

الاستعداد لتلقي تدفق البيانات الواردة من الجهات

انه نتيجة لتحول الجهات الحكومية إلى استخدام الوسائل الإلكترونية في تعاملاتها فان ذلك يؤدي إلى نشوء بيانات آلية يتم تناقلها بين الجهات الحكومية عوضاً عن المستندات الورقية لذا فإن الديوان عليه الاستعداد لتلقي الكم الهائل من البيانات حيث أنها تمثل حسابات الأشهر ومرفقاتها الواردة له من الجهات المشمولة برقابته للتعامل معها من حيث استقبالها والتعرف عليها وحفظها وتحويلها للإدارة المختصة وتوزيعها على مدققي تلك الإدارة للقيام بمهمة التدقيق ومن ثم تصديرها ، وأيضاً التأكد من أن ما تديره الجهات المشمولة برقابته من أنظمة آلية وقواعد معلومات تحقق الأهداف المرجوة وتتفق مع متطلبات الأنظمة وخصوصاً الأنظمة ذات العلاقة بالنواحي المالية منها وتساعد في المحافظة على أموال الدولة المنقولة والثابتة , ويشمل الاستعداد لها توفير الوسائط الآلية والنظم التطبيقية التي تتيح التعامل معها، وكذلك توفير الكفاءات المهنية القادرة على التعامل مع البيانات الآلية ومراجعتها , ومن أجل ذلك تم إعداد هذا الإطار العام لخطة تتيح للديوان التحول بطريقة مدروسة ومتماشية مع نظم الجهات المشمولة برقابته بشكل انسيابي دون أن يؤثر ذلك بشكل كبير على قدرة الديوان على القيام بمهامه المحددة في نظامه.

خيارات الديوان والأجهزة الرقابية الأخرى للمراجعة في ظل

في ظل استخدام الجهات المشمولة بالرقابة على الأنظمة الآلية، وتزويد الأجهزة الرقابية بالبيانات بشكل آلي تكون طريقة وصول البيانات على أحدى طريقتين:

1. تقديم البيانات للمراجعة دون الدخول على أنظمة الجهة (تقديم البيانات على وسائط النقل المختلفة مثل الأقراص المضغوطة أو عن طريق مشروع ربط الديوان بالجهات الحكومية آلياً) ، وتأخذ هذه الطريقة الأشكال التالية:
   - أ- تقديم بيانات (Raw data) عن سجلات العمليات المالية فقط، مثل كشف الحساب الشهري أو كشف الرواتب أو كشف العهد أو تعاميد الشراء أو المصاريف السفرية وغيرها , دون تقديم الوثائق (المستندات المؤيدة لهذه العمليات).
   - ب- تقديم البيانات المالية وصور ممسوحة ضوئياً من المستندات المؤيدة لها بحيث يكون كل مستند ومرفقاته محفوظة ضمن البيانات المقدمة للجهاز الرقابي .
   - ج- تقديم البيانات المالية على شكل مخرجات أنظمة تستخدم نظام الاعتماد الإلكتروني والوثائق الإلكترونية.

وعلى سبيل المثال ، يمكن أن تكون البيانات المقدمة من الجهات (Raw data) على قرص مضغوط (CD) وتشمل (رقم مر اعتماد الصرف / تاريخه / مبلغه رقما وكتابة / رقم التعميد / تاريخه / مبلغه / تاريخ التوريد المتوقع / تاريخ الاستلام المؤقت / الغرامة / الحسميات / إجمالي المبلغ بعد الخصم / رقم الفاتورة / قيمة الفاتورة / تاريخ الفاتورة), حيث أن معظم المصاريف تحتوي على معظم البيانات السابقة , بالإضافة إلى أي بيانات مهمة, وذلك لكل شهر على حدة ويقوم مدققوا الديوان بتحليلها بالآيديا. وأيضاً قد يتم إرفاق CD آخر يتضمن مسوغات الصرف النظامية ممسوحة بالماسح الضوئي ومن الممكن أخذ عينة للمطابقة فيما بعد , وإذا تم استخدام هذه الطريقة فإن معظم موظفي الديوان مدربون على هذا البرنامج .

2. منح مراجعي الأجهزة الرقابية صلاحية الدخول (قراءة فقط) على أنظمة الجهة الآلية للإطلاع على البيانات المالية، وسواء كان هذا الدخول عبر شبكة الانترنت أو عبر الربط الإلكتروني أو كان محلياً على الشبكة الداخلية للجهة فإنه يأخذ أحد الشكلين التاليين:

أ- الدخول على النظام كمتصفح بحيث يمكن للمراجع تتبع العمليات المالية أو الوصول إلى السجلات المصدر وانتهاءً إلى شاشة إدخال العملية وتحديد الإعتمادات الالكترونية التي تمت على المتصفح، والسجلات التجميعية وصولاً إلى كشف الحساب الشهري أو الحساب الختامي وذلك للجهات الجاهزة للربط آلياً مع الديوان .

ب- الدخول المشروط باستعلامات محددة (Queries) بحيث يتم منح المراجع صلاحية الدخول على هذه الاستعلامات ولا يستطيع الوصول إلى بيانات أخرى أو تعديل البيانات.

وهذين الشكلين يمكن أن يطبقا على بيانات الجهات الجاهزة للربط بالجهاز الرقابي , ويحتاجان إلى التدريب على أنظمة الجهة محل الفحص في نفس الجهات .

مما سبق يتبين تغير البيانات التي يتم الوصول إليها من قبل مراجعي الجهاز الرقابي حسب تغير طريقة الوصول للبيانات، وبالتالي فإن اختبارات المراجعة المنفذة عن طريق المراجعة الآلية سوف تتغير بتغير طريقة الوصول إلى البيانات.

وكحالة عامة فإنه لا يمكن أن يتم تحقيق جميع اختبارات المراجعة (المالية أو رقابة الأداء) عن طريق المراجعة الآلية فقط. فعلى سبيل المثال قد يتمكن المراجع من الحصول على صور المستندات الممسوحة ضوئياً للعمليات المالية، ولكن العديد من العمليات المالية تتطلب أصل الوثائق - مثل قرارات الانتدابات أو المستخلصات- وفي هذه الحالة لن يتمكن مراجع الجهاز الرقابي من تطبيق اختبار المراجعة الخاص باستخدام أصول القرارات في المراجعة عند تطبيق المراجعة الآلية. كذلك فإن التحقق المادي من وجود الأصول (مثل جرد الصناديق أو المخزون أو الوقوف المادي على المشاريع) لا يمكن تحقيقه عن طريق المراجعة الإلكترونية (الآلية).

وما سبق لا يعني أن المراجعة الآلية غير ذات جدوى وإنما يعني أن هناك بعض اختبارات المراجعة لا يمكن تنفيذها عبر المراجعة الآلية، وبالتالي فإن هناك خطوات تكميلية للمراجعة الآلية يجب أن تأخذ في الاعتبار حتى تتم عملية المراجعة بطريقة مهنية. غير أن اعتماد المراجعة الآلية

سوف يفتح للأجهزة الرقابية مجالاً للتوسع في المراجعة التحليلية التي تعتمد على البيانات نظراً لما يوفره وجود البيانات الإلكترونية والبرامج المساعدة في التحليل مثل (Idea و Microsoft Access وMicrosoft Excel) من سرعة ودقة في إجراء التحليلات.

وهذا الأسلوب من المراجعة قد يوصل الأجهزة الرقابية إلى اكتشاف أنواع جديدة من الملاحظات الناتجة عن التحليل التي تكشف عن الممارسات المالية التي تتبعها الجهات المشمولة بالرقابة. على سبيل المثال قد تكشف المراجعة التحليلية لجهة ما إجراء عدة عمليات شراء مباشر لصنف واحد خلال فترة زمنية قصيرة.

ويمكن أن يجري الجهاز الرقابي الخطوات التكميلية للمراجعة على نطاق محدود واعتمادا على قوة أنظمة الرقابة الداخلية لدى كل جهة مشمولة برقابته، وذلك عن طريق المعاينة الإحصائية، أو المعاينة الانتقائية.

تاريخ بداية المراجعة الآلية

تم إنشاء تدقيق الحاسب الآلي منذ أوائل عام 1404هـ ضمن الإدارات التابعة لمركز المعلومات وتم تشكيل فريق لمباشرة العمل حيث باشر الفريق بعد تشكيله أعماله وألحق الفريق في منتصف عام 1406هـ بالإدارة العامة لمراجعة حسابات المؤسسات العامة والشركات لتتولى الإشراف عليه إدارياً , علماً بأن الديوان ومنذ أوائل الثمانينات حرص على تبني التدقيق بواسطة الحاسب الآلي وكأحد المجالات التي ساهم الفريق الأمريكي في تطويرها كان مجال تدقيق الحاسب الآلي وتشكيل فريق متخصص به , وكتثمين لجهود الديوان ومسئوليه في مجال الاهتمام بتدقيق الحاسب الآلي وبمبادرته كأول جهاز رقابي على مستوى العالم العربي ولحاقه المبكر بالدول الرائدة في هذا المجال فقد تم منحه جائزة كاندوتش وهي أعلى جائزة تمنحها المنظمة الدولية لأجهزة الرقابة العليا (انتوساي) في مؤتمر برلين عام 1989م لتبنيه تدقيق الحاسب الآلي كجهاز سبّاق في هذا المجال على مستوى العالم .

وقد بذل أعضاء الفريق جهوداً ملحوظة لتطوير مستوى أدائهم المهني الذي أنعكس إيجابياً على أداء الديوان بشكل عام من خلال قيامهم بمهام التدريب العملي والنظري وعلى رأس العمل لمنسوبي الديوان على مهارات التدقيق والتحليل الآلي .

تعريف الرقابة باستخدام الحاسب

تعريف الرقابة المدعومة بالحاسب قد تُعرّف كأدوات معتمدة على الحاسوب يمكن استخدامها لتحسين فعالية وكفاءة عملية الرقابة؛ والتعريف البديل هو "أساليب يستخدمها المراقبون ويُستخدم فيها الحاسب كأداة لجمع وتحليل بيانات الرقابة" يجب ملاحظة أن استخدام CAATs لا يغير أهداف الرقابة، ولكن التغييرات مطلوبة فقط على مستوى منهجيات الرقابة , وحاليا في أغلب بيئات معالجة المعلومات تكون مستندات الرقابة إما غير متاحة على ورق أو تكون النسخة الورقية

متحصل عليها من البيانات الإلكترونية(ونتيجة لذلك تكون أقل موثوقية منها) وبالتالي يجب على المراقب الاعتماد على CAATs لجمع مستندات كافية وذات صلة ويعتمد عليها.

أهمية التدقيق باستخدام الحاسب

- انتشار استخدام الحاسبات في كافة المجالات
- ضخامة الاستثمار في هذا المجال
- ضخامة الخسارة المصاحبة لسوء الاستخدام

أهداف التدقيق باستخدام الحاسب

تقييم ما إذا كان الحاسب الآلي في أي منظمة يحقق ما يلي :

- المحافظة على الأصول
- المحافظة على تكامل البيانات وسلامتها
- فاعلية الأنظمة -والتأكد من تحقيقها للأهداف
- كفاءة الأنظمة - تحقيق الأهداف بأقل الموارد

وسائل وسبل إساءة استخدام

- تغيير أو تزوير البيانات عند الإدخال
- تغيير البرامج أو إعدادها لأغراض سيئة
- سرقة وقت الحاسب الآلي
- سرقة البيانات وإساءة استخدامها
- سرقة برامج الحاسب الآلي

أنواع الرقابة باستخدام الحاسب

رقابة النظم التطبيقية

نظم مالية - اليومية والأستاذ المساعد المبيعات والمشتريات المستودعات القوائم المالية , الفواتير , ..الخ

نظم إدارية - الرواتب,وشئون الموظفين ,الاتصالات الإدارية ...الخ

رقابة أمن النظم

أمن مادي (رقابة الوصول للأجهزة والمواقع)

أمن منطقي (حماية المعلومات - حماية البرامج - حماية التقارير)

مزايا المراجعة باستخدام الحاسب

- يمكن فحص بيانات أي نظام لسنوات عديدة أو منذ نشأة الجهة محل الفحص وتطور النظام حتى تاريخ نسخ البيانات .
- سهولة الحصول على البيانات بوسائل مختلفة دون الحاجة إلى نقل كم هائل من المستندات .
- سهولة الربط بين الملفات والنظم المختلفة .
- الحصول على نتائج سريعة .
- اكتشاف الفراغات في البيانات .
- اكتشاف التكرار في البيانات .
- اكتشاف التداخل في البيانات .
- اكتشاف البيانات الغير منطقية .
- تصدير البيانات إلى ملفات اكسل لقراءتها بسهولة .

خطوات المراجعة باستخدام الحاسب

-دراسة وفحص استخدام الحاسب الآلي في الجهات الخاضعة لرقابة الجهاز الرقابي ومدى اعتمادها على المعالجة الآلية للبيانات.

- التعرف على الأنظمة الآلية المطبقة بالجهات من حيث اشتمالها على وسائل الرقابة الداخلية اللازمة وتقيدها بالنظم والتعليمات المالية السارية.

- تحديد النظام المطلوب للفحص والحقول المطلوبة للنسخ والمدة المراد فحصها .
- نسخ بيانات النظام المطلوب فحصه على اسطوانات ممغنطة أو أي وسائل نقل أخرى .
- تحليل البيانات بواسطة برنامج التحليل المتوفر في الجهة الرقابية ومن عمليات التحليل التي يمكن إجرائها:
  - التحليل الزمني للبيانات والنسب المئوية لها.
  - مقارنة الحقول الآلية مع بعضها البعض مثلا حقل الراتب مع حقل الدرجة والمرتبة التي يشغلها الموظف .
  - توزيع البيانات تكراريا مثال توزيع مصاريف الرواتب والأجور في الجهة حسب كل قسم أو إدارة .
  - استخراج العينات الإحصائية آليا.
  - تطبيق العينات ومقارنتها بالمستندات والملفات اليدوية.
  - تقييم النظم في ضوء النتائج التي يسفر عنها الفحص من حيث شموليتها في معالجة كافة البيانات ودقتها في معالجة وتوفر نظم الرقابة الذاتية داخل الحاسب الآلي،ومدى ترابط الأنظمة الآلية مع بعضها والاستفادة من بيانات نظام معين في عمليات النظم الأخرى مثال بيانات مدفوعات الرواتب في نظام شئون الموظفين هي جزء من بيانات المصروفات في النظام المالي.
  - مطابقة نتائج التحليل مع الجهة محل الفحص .

دراسة النواحي الأمنية لمركز

- دراسة وثائق النظم الالية وخرائط سير العمليات الآلية وتحديد الملفات الآلية المستخدمة في حفظ واسترجاع البيانات.
- فحص ومراجعة شبكات الحاسب الآلي

فحص ومتابعة الإجراءات

- الأمن المادي لمركز المعلومات
- أمن البيانات (الأمن المنطقي)
- عمليات التشغيل
- خطة مواجهة الكوارث

- كتابة التقارير (بنتائج التدقيق ودراسة النظم الآلية)شاملة للتحليلات والبيانات التي تم الحصول عليها عن طريق الحاسب الآلي.
- اقتراح التوصيات الكفيلة بسد الثغرات الموجودة في النظام الآلي محل الفحص ورفع كفاءته.

المشاكل والصعوبات التي تواجه المراجعين عند إجراء الرقابة باستخدام

- تقاعس بعض الجهات بتزويد البيانات المطلوبه .
- عدم الإلمام بمتطلبات البيانات ونقص الخبرة .
- الإجازات لبعض الموظفين وعدم توفر البديل .
- التأخر في نسخ البيانات المطلوبة للفحص .
- إمكانية تعديل البيانات قبل تزويد الجهة بها .
- عدم تزويد البيانات بحجة سريتها .
- تخوف بعض المسئولين من إعطاء البيانات بحجة إنها سرية والخوف من انتشارها علماً بان الديون يلتزم بالسرية ويؤكد على عدم استخدم البيانات إلا للفرض الذي طلبت من اجله البيانات علماً بأنه يوجد أمر ملكي رقم 3218/م/ب وتاريخ 1427/4/23 هـ الذي ينص على تقديم كافة المستندات والمعلومات لديوان المراقبة العامة ونص الأمر الملكي هو (على جميع الجهات الخاضعة لرقابة الديوان تقديم كافة البيانات الحسابية وغيرها والمستندات والوثائق التي تمكن الديوان من مباشرة اختصاصاته وفقا لهذا النظام وكذلك تقديم كافة التسهيلات اللازمة لمندوبيه ومفتشيه وفقاً للوائح التنفيذية التي تصدر بهذا الصدد) .
- عدم تعاون المسئولين في الجهة تخوفاً من اكتشاف أخطاء أو ملاحظات في الأنظمة موضوع الفحص

- عدم التعاون من الجهة الخاضعة للرقابة لعدم التأكد من سلامة البيانات وعدم معرفة الهدف الحقيقي من التحليلات التي ستجرى على هذه البيانات .
- تأخر إدخال بعض البيانات الأساسية للنظام مثل تأخير إدخال بيانات بعض العقود .
- عدم إعطاء البيانات المطلوبة بالشكل الصحيح مما يترتب عليه إعادة طلب نسخ البيانات مما يتسبب في إضاعة الوقت
- التأخر في الرد على ملاحظات الديوان مما يستدعي إرسال تعقيب أول وثاني للجهة مما يزيد مدة مهمة فحص النظام .
- عدم تكامل النظام الآلي لدى بعض الجهات بحيث يكون النظام الآلي جزئيا
- عدم توفر الكوادر الفنية الوطنية في بعض الجهات للحصول على البيانات والاعتماد على الفنيين غير السعوديين .

أنواع التطبيقات التي يتناولها

إن جميع انواع التطبيقات سواء كانت مالية أو إدارية يجب إن تكون متكاملة مع بعضها البعض بحيث تكون مخرجات تطبيق معين هي في الوقت نفسه مدخلات للتطبيق الآخر وتقيل المدخلان اليدوية لكي نقلل من أخطاء الإدخال والتلاعب كذلك . ويجب التركيز تحليل هذه التطبيقات على أي حقل له قيمة مالية سواء كان التطبيق مالي أو إداري ومن أهم هذه التطبيقات ما يلي :

أولا: شئون الموظفين ويشمل الملفات

- الرواتب
- الإجازات
- الانتداب
- خارج الدوام
- الدورات
- الترقيات
- الحسميات
- العلاوات
- الغياب
- بدلات أخرى.

ويتم إعداد برنامج عمل يبين الخطوات المراد تحليلها والتأكد من سلامة البيانات فعلى سبيل المثال 1- التأكد من عدم تداخل بيانات الإجازات والانتداب أو خارج الدوام والانتداب لان التداخل مخالف للنظام حيث ينص النظام على عدم الجمع بين خارج الدوام والانتداب للموظف كذلك يتم التأكد من الملفات الأخرى مثل الإجازات بأنواعها والتأكد من التجاوز لهذه الإجازات للمدة المحددة لكل نوع .

2-ا لتأكد من أن العلاوات والمكافئات لا تصرف إلا لمستحقيها
3- التأكد من حساب الراتب الصافي
4- التأكد من عدم وجود تكرار للبيانات مثل رقم السجل المدني للموظف.

ثانياً : ملف المستودعات والمخزون

1- الملف الرئيسي
2- ملف العمليات

الملف الرئيسي : يتضمن المعلومات الأساسية عن الأصناف وكمياتها والحد الأقصى والأدنى ونقطة إعادة الطلب.

ملف المعاملات : يتضمن المعلومات الأساسية عن الصرف والاستلام لجميع الأصناف والحركة عليها وينشئ برنامج عمل لتحليل البيانات والتأكد من سلامة الإجراءات وتطبيق اللوائح والأنظمة في هذه التطبيقات فمثلا التأكد من الرقابة الداخلية على عملية الصرف والاستلام

- الأصناف بطيئة وعديمة الحركة
- الجرد الدوري

ثالثـــاً : المشـــتريات

يتم كذلك مراجعة التطبيقات والأنظمة الخاصة بالمشتريات والمبيعات ويعد برنامج عمل يتضمن التأكد من توفر الرقابة الداخلية في المشتريات والمبيعات والتأكد من الأسعار سواء في البيع أو الشراء والتحقق من أوامر الشراء المفتوحة وأسبابها ومعالجتها

رابعاً : القروض في

حكومية مثل بنك الزراعي وبنك التسليف السعودي والصندوق الصناعي .

حيث تم وضع برنامج عمل للتأكد من وجود رقابة داخلية للنظام تجبر المستخدم على إتباع جميع اللوائح والأنظمة الخاصة بالبنك .

ويحول الديوان حاليا إيجاد برامج العمل لجميع التطبيقات الحالية بحيث يتم مراجعة جميع الأنظمة باستخدام الأدوات المتوفرة

الأدوات المستخدمة للرقابة على البيانات المالية باستخدام

1- أجهزة حاسب آلي متطورة نسبياً .
2- برنامج التحليل المستخدم في الجهة مثل IDEA, ACL
3- برنامج عمل وخطوات للفحص

4- مراجعين أكفاء وملمين باستخدام البرنامج

أمن المعلومات

الإنترنت سلاح ذو حدين، فهو مدخل للكثير من الأشياء النافعة، ولكن مع الأسف، فهو يفتح المجال أمام الكثير من الأشياء المؤذية للدخول إلى جهازك. وثمة العديد من المسائل الأمنية الواجب الاعتناء بها للإبقاء على سلاسة تشغيل أجهزة الكمبيوتر والشبكات. وسنناقش في هذا المقال أهم القضايا الأمنية وبعض الحلول لها.

ما هو أمن

يعني أمن المعلومات إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة، أي بمعنى عدم إمكانية الوصول لها من قبل أي شخص آخر دون إذن منك، وان تكون على علم بالمخاطر المترتبة عن السماح لشخص ما بالوصول إلى معلوماتك الخاصة , أنت بالتأكيد لا ترغب أن يكون للآخرين مدخلاً لمعلوماتك الخاصة. ومن الواضح أن معظم الأشخاص يرغبون في الحفاظ على خصوصية معلوماتهم الحساسة مثل كلمات المرور ومعلومات البطاقة الائتمانية وعدم تمكن الآخرين من الوصول إليها، والكثير من الأشخاص لا يدركون بأن بعض المعلومات التي قد تبدو تافهة أو لا معنى لها بالنسبة لهم فإنها قد تعني الكثير لأناس آخرين وخصوصاً إذا ما تم تجميعها مع أجزاء أخرى من المعلومات .فعلى سبيل المثال، يمكن للشركة الراغبة في الحصول على معلومات شخصية عنك للأغراض التسويقية أن تشتري هذه المعلومات من شخص يقوم بتجميعها من خلال الوصول إلى جهاز كمبيوترك بشكل غير شرعي.
ومن المهم كذلك أن تفهم أنك حتى ولو لم تقم بإعطاء معلوماتك لأي شخص عبر الإنترنت، فقد يتمكن بعض الأشخاص من الوصول إلى نظام الكمبيوتر لديك للحصول على المعلومات التي يحتاجونها دون علم أو إذن منك.

مواطن الضعف في شبكة الانترنت

تعتبر شبكة الإنترنت عرضة للعيوب والضعف في دفاعاتها. وقد يكون هذا الضعف ناجما عن الأخطاء البرمجية والعيوب في تصميم النظام. ويعود سبب بعض نقاط الضعف إلى الإدخال الخاطئ للبيانات، حيث أن غالبا ما يسمح بتنفيذ الأوامر المباشرة أو عبارات لغة SQL وأحيانا يخفق المبرمج في التحقق من حجم البيانات المخزنة، حيث يؤدي ذلك إلى فيض من البيانات والذي يسبب فساد المكدس أو مناطق الشجرة الثنائية في الذاكرة , وغالبا ما تتيح مواطن الضعف للمهاجم إمكانية التحايل على البرنامج بتجاوز فحص إمكانية الوصول أو تنفيذ الأوامر على النظام المضيف لهذا البرنامج , وهناك عدد من نقاط الضعف والتي يكون جهازك أو شبكتك عرضة لها.
ومن أكثرها شيوعا هي أخطاء تدقيق صحة إدخال البيانات مثل الأخطاء البرمجية الناجمة عن تنسيق الرموز النصية، والتعامل الخاطئ مع الرموز المتغيرة لغلاف البرنامج ولذلك يتم تفسير هذه الرموز، وإدخال عبارات SQL وتضمين النصوص البرمجية متعارضة-الموقع داخل تطبيقات الويب. ومن نقاط الضعف الشائعة أيضا تحطم المكدس وفيض البيانات في ذاكرة التخزين المؤقت بالإضافة إلى ملفات الروابط الرمزية.(Symlinks)

فحص مواطن الضعف

يمكن أن تكون هناك نقاط ضعف في جميع أنظمة التشغيل مثل الويندوز، ماكنتوش، لينوكس، OpenVMS، وغيرها , ويمكن فحص نقاط الضعف في الشبكة والخوادم من خلال إجراء اختبار خاص عليها يتم من خلاله فحص الخوادم والصفحات الإلكترونية وجدران النار وغير ذلك لمعرفة مدى تعرضها لنقاط الضعف. ويمكن تنزيل برامج فحص نقاط الضعف من الإنترنت.

المشاكل الأمنية

تحدث المشكلة الأمنية عندما يتم اختراق النظام لديك من خلال أحد المهاجمين او المتسللين (الهاكر) أو الفيروسات أو نوع آخر من أنواع البرامج الخبيثة , وأكثر الناس المستهدفين في الاختراقات الأمنية هم الأشخاص الذي يقومون بتصفح الإنترنت، حيث يتسبب الاختراق في مشاكل مزعجة مثل تبطئ حركة التصفح وانقطاعه على فترات منتظمة. ويمكن أن يتعذر الدخول إلى البيانات وفي أسوأ الأحوال يمكن اختراق المعلومات الشخصية , وفي حالة وجود أخطاء برمجة أو إعدادات خاطئة في خادم الويب، فمن الجائز أن تسمح بدخول المستخدمين عن بعد غير المصرح لهم إلى الوثائق السرية المحتوية على معلومات شخصية أو الحصول على معلومات حول الجهاز المضيف للخادم مما يسمح بحدوث اختراق للنظام. كما يمكن لهؤلاء الأشخاص تنفيذ أوامر على جهاز الخادم المضيف مما يمكنهم تعديل النظام وإطلاق هجمات إغراقية مما يؤدي إلى تعطل الجهاز مؤقتاً، كما أن الهجمات الإغراقية تستهدف إبطا أو شل حركة مرور البيانات عبر الشبكة. كما أنه من خلال الهجمات الإغراقية الموزعة ، فإن المعتدي يقوم باستخدام عدد من الكمبيوترات التي سيطر عليها للهجوم على كمبيوتر أو كمبيوترات أخرى , ويتم تركيب البرنامج الرئيسي للهجمات الإغراقية الموزعة في أحد أجهزة الكمبيوتر مستخدماً حساباً مسروقاً , وإن التجسس على بيانات الشبكة واعتراض المعلومات التي تنتقل بين الخادم والمستعرض يمكن أن يصبح أمراً ممكناً إذا تركت الشبكة أو الخوادم مفتوحة ونقاط ضعفها مكشوفة.

الهاكر

الهاكر هو الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي. وقد أصبح هذا المصطلح ذا مغزى سلبي حيث صار يطلق على الشخص الذي يقوم باستغلال النظام من خلال الحصول على دخول غير مصرح به للأنظمة والقيام بعمليات غير مرغوب فيها وغير مشروعة. غير أن هذا المصطلح (هكر) يمكن أن يطلق على الشخص الذي يستخدم مهاراته لتطوير برمجيات الكمبيوتر وإدارة أنظمة الكمبيوتر وما يتعلق بأمن الكمبيوتر.

فيروسات

فيروسات الكمبيوتر هي الأكثر شيوعاً من بين مشاكل أمن المعلومات التي يتعرض لها الأشخاص والشركات .وفيروس الكمبيوتر هو برنامج غير مرغوب فيه ويدخل إلى الجهاز دون إذن ويقوم بإدخال نسخ من نفسه في برامج الكمبيوتر، والفيروس هو أحد البرامج الخبيثة أو المتطفلة . والبرامج المتطفلة الأخرى تسمى الديدان أو أحصنة طروادة أو برامج الدعاية أو برامج التجسس يمكن للبرامج الخبيثة أن تكون فقط للإزعاج من خلال التأثير على استخدامات الكمبيوتر وتبطئيه وتتسبب في حدوث انقطاعات وأعطال في أوقات منتظمة وتؤثر على البرامج والوثائق المختلفة

التي قد يرغب المستخدم في الدخول إليها. أما البرامج الخبيثة الأكثر خطورة فيمكن أن تصبح مشكلة أمنية من خلال الحصول على معلوماتك الشخصية من رسائلك الإلكترونية والبيانات الأخرى المخزنة في جهازك.
أما بالنسبة لبرامج الدعاية وبرامج التجسس فهي مزعجة في الغالب وتؤدي إلى ظهور نوافذ دعائية منبثقة على الشاشة. كما أن برامج التجسس تجمع معلوماتك الشخصية وتقدمها إلى جهات أخرى تطلب الحصول عليها لأغراض تجارية يمكنك حماية كمبيوترك وحماية نفسك باستخدام برامج مناسبة لمكافحة البرامج الخبيثة غير المرغوب فيها والتي قد تكون نتائجها مدمرة. للمزيد من المعلومات،

اللصوصية

يستخدم مصطلح (**Phishing**) للتعبير عن سرقة الهوية، وهو عمل إجرامي، حيث يقوم شخص أو شركة بالتحايل والغش من خلال إرسال رسالة بريد إلكتروني مدعياً أنه من شركة نظامية ويطلب الحصول من مستلم الرسالة على المعلومات الشخصية مثل تفاصيل الحسابات البنكية وكلمات المرور وتفاصيل البطاقة الائتمانية. وتستخدم المعلومات للدخول إلى الحسابات البنكية عبر الإنترنت والدخول إلى مواقع الشركات التي تطلب البيانات الشخصية للدخول إلى الموقع هناك برامج لمكافحة اللصوصية **Phishing** والكشف عن هوية المرسل الحقيقي ، وأفضل وسيلة لحماية الشخص من نشر معلوماته الشخصية لمن يطلبها هو أن يكون الشخص متيقظاً وحذراً ولديه الوعي الكافي، فلا يوجد هناك أي بنك معروف أو مؤسسة فعلية يطلبون من عملائهم إرسال معلوماتهم الشخصية عبر البريد الإلكتروني.

البريد

يجدر بنا ان نتذكر دائماً إلى أن البريد الإلكتروني لا يضمن الخصوصية، فخصوصيته تشابه خصوصية البطاقة البريدية. ويتنقل البريد الإلكتروني في طريقه إلى المستلم عبر العديد من الخوادم حيث يمكن الوصول إليه من قبل الأشخاص الذين يديرون النظام ومن الأشخاص الذين يتسللون إليه بشكل غير نظامي. والطريقة الوحيدة للتأكد إلى حد ما من خصوصية بريدك الإلكتروني هو تشفيره. انظر الفقرات التالية..

كيف تحمي شبكتك ونظامك

عليك بالحذر والحرص الدائمين لحماية نظامك كي لا يكون عرضة للهجمات بسبب نقاط الضعف فيه، ويمكنك تركيب برامج فعالة لجعل استخدام الإنترنت أكثر أماناً لك.

وسائل الحماية المادية

سنستعرض في الفقرات التالية المزيد من المعلومات حول البرمجيات المختلفة والوسائل المتعلقة بالأنظمة الأخرى للإبقاء على معلوماتك آمنة، لكن علينا أن نتذكر أن ثمة العديد من الطرق الأخرى التي يسلكها المتسللون للوصول إلى معلوماتك. ضع كمبيوترك وخصوصاً الكمبيوتر المحمول دائماً في مكان آمن. قم بحماية كمبيوترك بكلمة مرور ويستحسن أن تطفئه وأنت بعيداً عنه. عليك أن تشك في أي شخص يرغب في الحصول على أي من كلمات المرور الخاصة بك،

حتى أولئك الأشخاص الذي يعملون (أو يدعون بأنهم يعملون) في الدعم الفني في شركتك. فإن أرادوا الحصول على كلمة المرور الخاصة بك، قم أنت بطباعتها (إدخالها) بنفسك (بحيث لا يرونها) ولا تبلغها لهم شفوياً أو خطيا. قم بانتظام بتغيير كلمة المرور إذا تصادف أن اطلع عليها أحد غيرك، أو حتى إذا شعرت أن أحد ما تمكن من الوصول إليها. ولا تكتب كلمات المرور الخاصة بك في أي مكان ولكن عليك أن تتذكرها بنفسك.

التحديثات

حافظ على تحديث جميع برامجك بما في ذلك أحدث نسخة من برنامج التشغيل الذي تستخدمه. وإذا كنت تستخدم التحديث التلقائي الذي يقوم بالبحث يومياً عن التحديثات عند بدء تشغيل الجهاز، فعليك إعادة تشغيل جهازك يومياً.

جدار الحماية Firewall

يكون جدار الحماية الناري إما برنامجاً أو جهازاً يستخدم لحماية الشبكة والخادم من المتسللين. وتختلف جدران النار حسب احتياجات المستخدم. فإذا استدعت الحاجة إلى وضع جدار النار على عقدة منفردة عاملة على شبكة واحدة فإن جدار النار الشخصي هو الخيار المناسب. وفي حالة وجود حركة مرور داخلة وخارجة من عدد من الشبكات، فيتم استخدام مصافي لجدار النار في الشبكة لتصفية جميع الحركة المرورية. علماً بأن الكثير من الشبكات والخوادم تأتي مع نظام جدار نار افتراضي، ولكن ينبغي التأكد فيما إذا كان يقوم بعمل تصفية فعالة لجميع الأشياء التي تحتاج إليها، فإن لم يكن قادراً على ذلك، فينبغي شراء جدار حماية ناري أقوى منه.

برامج مراقبة بيانات الشبكة Packet

طريقة فعالة لمراقبة الحركة المرورية عبر الشبكة باستخدام أحد برامج مراقبة بيانات الشبكة، حيث يتم من خلاله تجميع البيانات الداخلة والخارجة، وهي طريقة ممكن أن تكون مفيدة في الكشف عن محاولات التسلل عبر الشبكة، وكذلك يمكن استخدامها لتحليل مشاكل الشبكة وتصفية وحجب المحتوى المشكوك فيه من الدخول إلى الشبكة.

التشفير

التشفير هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات. ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس. ويجعل التشفير المعلومات في جهازك غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن .ومن أشهر برامج التشفير **(PGP)**

أمن الشبكات

تنمو الشبكات اللاسلكية في كل مكان وتنمو بشكل غير طبيعي ولا توجد دلالات على توقف ذلك النمو على المستوى المنظور. وهناك العديد من القضايا الأمنية المصاحبة لهذه الشبكات اللاسلكية، كما أن بإمكان أي شخص الوصول إلى الشبكة اللاسلكية من أي مكان تتوفر فيه الوصلة اللاسلكية. وبالإضافة إلى التدابير الأمنية العامة المتبعة لحماية الشبكات اللاسلكية، فإنه من الضروري إتباع المبادئ العامة البسيطة لتوفير أفضل مستوى من الأمن لشبكتك اللاسلكية.

التشفير

يتم حماية الشبكة اللاسلكية باستخدام بروتوكول تشفير الشبكات اللاسلكية .(**WEP**) ويعمل هذا البروتوكول بتضمين مفتاح مشترك 64 أو 128 بت بين العملاء ونقطة الدخول، ومن ثم يتم استخدام هذا المفتاح لتشفير وفك تشفير البيانات بينهم، وهذا يوفر قدر كاف من الأمن للشبكات المنزلية. عليك الرجوع إلى الوثائق الخاصة بالأجهزة اللاسلكية لديك لتعرف كيفية تمكين وإعداد بروتوكول التشفير اللاسلكي (**WEP**) على شبكتك. أما بالنسبة لبيئات الشركات، فيجب اعتبار هذا البروتوكول (**WEP**) فقط كنقطة بداية للترتيبات الأمنية، وعلى الشركات البحث جدياً في ترقية شبكاتهم اللاسلكية إلى مستوى (**WPA**) أكثر أماناً.

التعريف

يكون للأجهزة ومديرو الشبكات أسماء تعريف افتراضية في النظام، ومن السهل كثيراً على الهاكر إيجاد هذه الأسماء، ومن ثم عمل كلمات مرور واسم مستخدم شخصي لك من خلال تعديل أسماء التعريف الافتراضية في النظام. لذا ننصح بإعطاء الأجهزة لديك أسماء لا تكشف عن هوية صاحبها أو أماكنها، ومثال ذلك بدلاً من استخدام عنوانك الفعلي مثل اسم المبنى أو اسم الشركة كأسماء لأجهزتك، يمكنك استخدام أسماء مختلفة مثل "الجبل Mountain" أو "جهازي My Device".

الإعلان عن المعرف Identifier

قد يكون في جهازك وظيفة افتراضية لبث (الإعلان عن) حالة التوصيلة، وحيث أنه قد يكون سهلاً على الهاكرز اختراق الشبكة اللاسلكية، لذا عليك تعطيل عمل خاصية الإعلان عن المعرف Identifier broadcasting.

ترشيح العناوين MAC filtering

يعرف عنوان (MAC) كذلك بأنه العنوان المادي، وهو معرف فريد لكل جهاز في الشبكة .ويعني مصطلح ترشيح العناوين أن تقوم يدوياً بإدخال قائمة بالعناوين الموجودة في شبكتك المحلية وتقوم بإعداد الموجه لديك (router) ليسمح فقط بتوصيل هذه العنوانين المحددة عبر الشبكة اللاسلكية. ويمكن بسهولة العثور على العناوين (MAC Addresses) من خلال الذهاب إلى مؤشر الأوامر (Command Prompt)في كل نظام وكتابة هذه العبارة:

```
ipconfig /all
```

الخلا

يمكنك من خلال إتباع هذه التدابير والتعليمات الأمنية جعل شبكتك واستخدامك للإنترنت أكثر أماناً. ونظراً لأن تقنيات وأساليب الهاكرز والمتسللين الآخرين تتطور مع مرور الزمن، لذا فإن عليك تثقيف نفسك باستمرار من خلال متابعة المعلومات الأمنية ضمن المواقع الإلكترونية التي تقدمها.

عناصر امن

1- السرية :

وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها أحد من غير المخولين

2- التكاملية وسلامة المحتوى :

وتعني التأكد من أن محتوى المعومات صحيح ولم يتم التعديل أو العبث بأية مرحلة من مراحل التخزين أو المعالجة .

3- استمرارية توفير المعلومات :

استمرارية توفير المعلومات: التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل معه من قبل المستخدمين

4- الإتاحة:

وتعني أن تكون متاحة لكافة الأشخاص المخولين .

وسائل الأمن

هناك مجموعه من وسائل الأمن , هذه الوسائل يمكن تقسيمها لعدة طبقات:

- أنظمة حماية الشبكات والتوصيلات
- أنظمة حماية البنية التحتية
- أنظمة حماية نظم التشغيل
- أنظمة حماية البرامج والتطبيقات
- أنظمة حماية قواعد البيانات
- أنظمة حماية الولوج

وأبسط أنواع الحماية هي استخدام نظام التعريف بشخص المستخدم موثوقية الاستخدام ومشروعيته وهذه الوسائل تهدف إلى ضمان استخدام النظام أو الشبكة من الشخص المخول بالاستخدام وتضم هذه الطائفة كلمات السر بأنواعها، والبطاقات الذكية المستخدمة للتعريف، ووسائل التعريف البيولوجية والتي تعتمد على سمات معينة في الشخص المستخدم متصلة ببنائه البيولوجي المفاتيح المشفرة ويمكن أن نضم إلى هذه الطائفة ما يعرف بالأقفال الالكترونية التي تحدد مناطق النفاذ.

إذاً نلاحظ مما سبق أن كل هذه التكنولوجيا التي وصل إليها العالم لا يمكن أن تعيش من دون امن المعلومات فعلى سبيل المثال نظام البنوك لو لم يكن هناك امن المعلومات لاستطاع أي شخص أن يدخل على النظام ويغير حسابه ويصبح مليونير من لا شيء.

اعتماد وتدقيق أمن

أصبحت النظم المعلوماتيه وقواعد البيانات وشبكات الاتصال عصب العالم المعرفي والصناعي والمالي والصحي وغيرها من القطاعات. حيث أصبح من المهم الحفاظ على أمن المعلومات بعناصره الرئيسية الثلاث: السرية والصوابية والاستمرارية , وعلى المستوى العالمي يبرز نظام الإيزو للاعتماد والتقييم والقياس 27001 لضمان أمن المعلومات , كما يوجد نظام HIPAA في الولايات المتحدة الأمريكية لضمان أمن المعلومات الصحية ونظام COBIT من ISACA لأمن المعلومات.

شهادات لخبراء أمن

تعد CISA مدقق نظم المعلومات المعتمد أحد أبرز الشهادات في إدارة وتدقيق النظم المعلوماتية , كما تعتبر شهادة CISSP خبير أمن معلومات معتمد شهادة مهمة في أمن المعلومات. كما توجد شهادات متخصصة في أغلب الشركات الكبيرة لتخصص أمن المعلومات مثل مايكروسوفت وسن وسيسكو وغيرها من الشركات.

عناصر التحكم المادية

- عناصر التحكم المادية والبيئية
- عناصر التحكم المنطقية

المبادئ الأساسية

هناك بعض المصطلحات التي سيتم استخدامها في هذه الدورة التدريبية ، لأغراض التوضيح ، من الضروري أن نحصل على فهم عام لهذه المصطلحات , تم توفير وصف مختصر لهذه المصطلحات أدناه:

عناصر التحكم المادية

الآليات المادية والإجراءات الإدارية التي يتم استخدامها لحظر الوصول غير المعتمد وغير المسموح به إلى معدات تقنيات المعلومات أو للتسبب في قصورها عن أداء وظائفها.

عناصر التحكم البيئية

هي الأفعال أو الإجراءات التي يتم استخدامها لحماية أجهزة وبرامج الكمبيوتر من الإصابة بالضرر، لأسباب مرتبطة بالمخاطر البيئية مثل الرطوبة أو الحرائق أو القاذورات أو انقطاع التيار الكهربي.

السجل (Log)

هو عبارة عن تسجيل أو سجل لسلسلة من الأحداث أو الأنشطة.

الوصول المنطقي

هو أحد عناصر التحكم من خلال البرامج لحظر الوصول غير المعتمد لبرامج وبيانات الكمبيوتر.

عناصر التحكم المادية

الهدف من عناصر التحكم المادية والبيئية هو حظر الوصول غير المعتمد ومنع التدخل في خدمات تقنيات المعلومات.وللوفاء بهذا الهدف، يجب حماية أجهزة الكمبيوتر والمعلومات التي تحتوي عليها وتتحكم فيها من وصول المستخدمين غير المصرح لهم بالوصول. كما يجب أن تتم حماية تلك الأجهزة من المخاطر البيئية التي تتسبب فيها الحرائق أو الماء (سواء الماء الفعلي أو الرطوبة الزائدة)أو الزلازل أو حرائق الغابات أو الانزلاقات الأرضية أو الزيادة المفاجئة في التيار الكهربي أو انقطاع التيار الكهربي.

وحسب ما تورده جمعية تدقيق أنظمة المعلومات والتحكم فيها (ISACA)، يعد ثاني أكثر الأسباب المحتملة التي تؤدي إلى حدوث الأخطاء هو الكوارث الطبيعية (حيث تحتل أخطاء المستخدمين المكانة الأولى، والخداع والغش المكانة الثالثة، وأخطاء الأجهزة المكانة الرابعة).

وهناك طريقتان لحظر الوصول إلى أنظمة الكمبيوتر، الوصول المادي والوصول المنطقي.

المخاطر المرتبطة بضعف/غياب عناصر التحكم المادية أو

الأضرار العرضية أو المتعمدة من العاملين:

* موظفي تقنيات المعلومات
* القائمون على النظافة، حراس الأمن
* غيرهم من الموظفين

سرقات أجهزة الكمبيوتر أو المكونات الفردية لها (تتزايد نسبة سرقات الكمبيوتر ويحتمل أن يستمر هذا التزايد. لاحظ أنه، بالمقارنة، تعتبر رقائق الكمبيوتر أغلى من الذهب وبالتالي فإنها تجذب اللصوص بشدة)

حالات الخلل في التيار الكهربي أو الزيادة المفاجئة به التي قد تؤدي إلى حدوث أضرار في المكونات وفقد أو تلف البيانات.

تجاوز عناصر تحكم الوصول المنطقي على سبيل المثال، يمكن إساءة استغلال الوصول إلى الخادم المزود لتجاوز عناصر التحكم المنطقية مثل كلمات السر، والمعلومات السرية أو الحساسة، مثل سياسات التسعير أو النتائج التي لم يتم نشرها أو السياسات الحكومية.

البيئية

الأضرار الناجمة عن الحرائق/الماء (أو الأضرار الناجمة عن الكوارث الطبيعية الأخرى)؛

الكهرباء:انقطاع التيار، يؤدي إلى فقدان البيانات الموجودة في الذاكرة المؤقتة (RAM) الخلل مما يؤدي إلى حدوث حالات الفشل في الأنظمة، وأخطاء في المعالجة أو في حدوث أضرار لمكونات الأجهزة , حالات الفشل في المكونات بسبب تطرف درجات الحرارة أو الرطوبة (أو تجاوزها للدرجات التي يمكن تحملها بدرجات قليلة) الأضرار الناجمة عن التفجيرات،.يبدو أن الإرهاب يتزايد على مستوى العالم ومن السهل مهاجمة مراكز الكمبيوتر، حيث أن تدمير تلك المراكز يكون له نتائج غير مباشرة على الحكومات .

الكهرباء الساكنة: يمكن أن تؤدي إلى تدمير المكونات الكهربية الضعيفة.تعد رقائق الكمبيوتر (مثل الروم والرام والمعالج) مكونات ضعيفة ويسهل تدميرها من خلال صدمات الكهرباء الساكنة،

غير ذلك: مثل الصواعق، وتجمع الأتربة أو القاذورات ، ويعد الاهتمام الأساسي لمراجع أنظمة المعلومات المالية هو أن أي حادث مرتبط بضعف عناصر التحكم المادية أو البيئية يؤدي إلى زيادة مخاطر أي من :

حدوث أضرار في أجهزة الكمبيوتر العملية والبيانات المالية، مما يؤدي إلى تقليل قدرتها على تسجيل العمليات المالية وإنتاج مجموعة بيانات مالية يمكن مراجعتها،

حدوث أضرار في الحسابات، تنجم عن الغش أو أخطاء الأجهزة العملية.

لوحظ في الفحص الميداني لا يوجد مقياس يقيس نسبة الرطوبة في غرفة server يوجد في مكتب الشبكات منظم الكهرباء(UPS) المركزي وكابلات الكهرباء والغرفة لا تتعدّى حجمها المتر والنصف , اسطوانة الحريق الكبيرة الموجود في غرفة server يستحسن أن تنقل إلى غرفة أمنة غير غرفة server

أسلوب للتعامل مع المخاطر المادية

لضمان تواجد عناصر تحكم داخليه كافية لحماية أصول وموارد الأعمال التجارية، يجب أن يقوم العميل بإجراء تقييم للمخاطر.وقد يشمل هذا التقييم على تحديد التهديدات المحتمل حدوثها في الأنظمة، وقابلية حدوث المشاكل في مكونات الأنظمة، والتأثير المحتمل لحدوث أية حادثة. كما يجب أن يحدد الإجراءات المقاومة لتقليل التعرض إلى مستوى مقبول.وللقيام بذلك، يجب أن يعمد إلى موازنة المخاطر المحددة بتكاليف تطبيق عناصر التحكم.

فقد يكون تطبيق بعض العناصر مكلفًا، وقد لا يكون مبررًا إلا في البيئات التي تتسم بالخطورة العالية. وهناك بعض عناصر التحكم الأخرى التي يتم اعتبارها عناصر تحكم أساسية، مثل أقفال الأبواب، وهي عناصر قد تتواجد لدى كل العملاء.

ويجب أن تشتمل سياسة تأمين تقنيات المعلومات في الكيان على اعتبارات للمخاطر المادية والبيئية.

وتختلف الإجراءات المقاومة، أو عناصر التحكم التي يضعها الكيان، بحسب العميل. على سبيل المثال، يكون لدى الوزارات الحكومية الكبيرة التي تمتلك مراكز البيانات الخاصة بها درجة أكبر من عناصر التحكم في منشئات تقنيات المعلومات لديها، وبشكل يختلف عن مؤسسة صغيرة الحجم تستخدم أنظمة أتمتة المكاتب مثل معالجة الكلمات والجداول.

عناصر التحكم المادية

التحكم المادي في المناطق

تهدف عناصر التحكم المادية في الوصول بشكل خاص إلى ضمان ألا يتمكن أي أحد غير أولئك الذين تمنحهم الإدارة القدرة على الوصول المادي لأنظمة الكمبيوتر. ويجب أن يقوم تأمين الوصول المادي على مبدأ تصميم محيطات وحدود تحيط بمنشئات معالجة تقنيات المعلومات. على سبيل المثال، قد يقوم العميل بتصميم حدود لتقنيات المعلومات حول المبنى، أو حول شبكة أجهزة الكمبيوتر، أو حول غرفة الطابعة، وما إلى ذلك. ويجب أن يتم تحديد تلك الحدود بشكل واضح ويجب أن يعرف الموظفون تلك الحدود.

ويجب التحكم في إمكانية الوصول إلى موقع العميل والمناطق الآمنة باستخدام طبقات متعددة من عناصر التحكم، بدءًا من السياج المحيط بالحدود ومرورًا بمدخل المبنى ووصولاً إلى شبكة أجهزة الكمبيوتر والوحدات الطرفية. وقد تكون عناصر التحكم المادية واضحة، مثل وجود أقفال على الأبواب، أو ضمنية، مثل أن ينطوي الوصف الوظيفي لموظف ما على ضرورة دخول منطقة عمليات تقنيات المعلومات.

عناصر التحكم

إلغاء الموظفين للبطاقات تشتمل على أسمائهم أو التعريف بهم وإلغاء حق الوصول للموظفين الذين يتم فصلهم، على سبيل المثال، يتم إخبار حراس الأمن عندما يترك الموظفون العمل، كما تتم إعادة المفاتيح عند فصل العمالة. ويجب أن تتوافر إجراءات لتحديد من يرحلون ولضمان عدم السماح لهم بالوصول المادي للمبنى (والوصول المنطقي للأنظمة).

الزوار: تسجيل دخول الزوار، بما في ذلك تسجيل هوياتهم، ولمن يعملون، ومن يزورون، ووقت الوصول ووقت الخروج , قد يطلب من الزوار توفير أي نوع من أنواع وسائل التعريف بالهوية قبل السماح لهم بالدخول، مثل رخص القيادة والبطاقات الشخصية. وقد يطلب من الزوار أن تتم مرافقتهم طوال الوقت؛

الإجراءات عند ترك المكان خاليًا: أي ماذا يجب أن يحدث عندما يترك الموظفون مكاتبهم خالية، مثلاً عندما يرحل الموظفون إلى بيوتهم في نهاية اليوم أو عند خروجهم لتناول الغداء في وقت الراحة. ويمكن أن تشتمل تلك الإجراءات على قفل لوحات المفاتيح الخاصة بهم، ووضع أجهزة الكمبيوتر المحمولة في أدراج مغلقة ووضع الأقراص المضغوطة في مكان مغلق.

الأقفال على الأبواب

يتطلب وجود الأقفال على الأبواب شيء من اثنين لإتاحة الدخول: ما هي صفة الشخص، أو ما هي معلومات الشخص. وأي طريقة يتم استخدامها، يجب التحكم بشدة في "مفتاح" كل نوع، على سبيل المثال، من هم الذين يجب منحهم مفتاحًا، أو من هم الذين يجب إطلاعهم على كلمة السر.وتشتمل الأقفال التي تتم مصادفتها بكثرة على ما يلي :

أقفال المفاتيح الميكانيكية: يجب أن يتم وضع علامات تشير إلى عدم نسخ مفاتيح الأبواب، كما يجب ألا تشير المفاتيح إلى الأبواب التي يمكنها فتحها.

الكلمات السرية لأقفال الأبواب أو الأقفال المشفرة: تشتمل تلك الأقفال بشكل طبيعي على لوحات مفاتيح رقمية. ويتم إعطاء الموظفين المعتمدين الأرقام السرية لإتاحة الدخول. ويمكن أن تختلف الأرقام السرية وتتراوح بين 3-6 أرقام، ويجب تغييرها بشكل متكرر، أو عندما يترك أحد العاملين في فريق تقنيات المعلومات العميل أو ينتقل إلى قسم آخر من أقسام المؤسسة.

أقفال الأبواب الإليكترونية: وغالبًا ما يستخدم هذا النوع البطاقات البلاستيكية التي تحتوي على شريحة ممغنطة على الخلف. وتستخدم الشريحة الممغنطة بحيث تشتمل على كود خاص يستطيع قارئ البطاقات قراءته. فإذا كان الكود صحيحًا، يتم تحرير آلية الغلق، وبالتالي يتم السماح بالدخول. وتوفر أقفال الأبواب الإلكترونية بعض المميزات التي تميزها على أقفال المفاتيح اليدوية حيث أنها:

* يمكن إعدادها للتعرف على الأشخاص وتسجيل تحركاتهم؛
* حظر الوصول على مناطق معينة من المؤسسة حسب احتياجات المستخدم (أو حسب الوقت و اليوم)،
* يصعب نسخ البطاقات، خصوصًا إن كانت البطاقات عبارة عن بطاقات ذكية تحتوي على شريحة رقيقة مدمجة،
* يمكن التحكم فيها بسهولة من خلال وحدة طرفية مركزية، فعلى سبيل المثال، عندما يترك أحد الموظفين الشركة، يمكن تعطيل إمكانيات وصوله في الشركة خلال ثوانٍ معدودة، و
* يمكن توصيلها بوحدات إنذار لا تطلق اصواتاً إلا في غرفة تحكم عندما تتم محاولة وصول غير مشروعة.

أقفال الأبواب الحيوية: تتم برمجة هذه الأقفال بحيث تتعرف على المميزات الحيوية للمستخدمين المعتمدين.وتشتمل الميزات الحيوية التي يمكن استخدامها على بصمات الأيدي أو بصمات

الصوت أو بصمات الأصابع أو فحص شبكة العين أو التوقيعات.وتميل الأنظمة الحيوية إلى ارتفاع الثمن، ولا يتم استخدامها إلا في منشئات الكمبيوتر الحساسة للغاية.

وتشتمل عناصر التحكم المادية

كاميرات تصوير الفيديو: يمكن وضع كاميرات تصوير الفيديو في مناطق إستراتيجية لمراقبة الدخول والخروج. وإذا تمت مراقبة كاميرات الفيديو تلك لمدة 24 ساعة في اليوم، فيمكن أن تقوم بدور عنصر التحكم الوقائي. كما يمكن أن تقوم بدور عنصر التحكم الكشفي حيث إنها توفر سجلات مرئية.

حراس الأمن: يمكن نشر حراس الأمن في مداخل مناطق العميل.كما يمكن أن يتم استخدامهم للتحقق من هوية من يدخلون إلى المنشئة. كما يمكن الاعتماد عليهم لتنفيذ دوريات خارج أوقات الدوام الرسمية.

السياجات الحدودية: تحيط بأجهزة الكمبيوتر .

أجهزة الإنذار ضد السرقة: _قد تفيد تلك الأجهزة لمراقبة مناطق الدخول غير النشطة مثل مخارج الحريق، أو عندما لا يتواجد أحد في منشئات تقنيات المعلومات.

التحكم في الموظفين الذين يعملون في أوقات غير أوقات العمل: لمعظم العملاء، يضم هؤلاء الموظفين العاملين على نظافة المكاتب، والصيانة، وحراس الأمن والمقاولين المتعاقدين مع الشركة. ومن الطبيعي أن تلاحظ أن العميل يكون لديه عناصر تحكم قوية على تحركات الموظفين، إلا أن عناصر التحكم المفروضة على المتعاقدين الذين يعملون خارج أوقات العمل تكون هشة. على سبيل المثال، يمكن أن يكون لحارس الأمن القدرة على الوصول إلى معظم أرجاء مبنى العميل، كما يمكن أن يدخل أو يخرج خارج ساعات العمل دون التعرض لإجراءات الأمن المعتادة. ولقد حدثت حالات عديدة كان فيها عمال النظافة ليسوا مجرد عمال نظافة عاديون، بل كانت لديهم أجندات أخرى (مثل الصحافة أو التجسس أو السرقة)،

- أبواب الشخص الواحد:يمكن أن تتواجد أبواب الشخص الواحد في مداخل الأماكن الحيوية مثل غرفة الكمبيوتر. وهي تتكون من بابين، لا يمكن فتح إلا باب واحد منهما في أي وقت. وهي مفيدة لمنع دخول أفراد غير مصرح لهم بالدخول خلف أفراد مصرح لهم بالدخول إلى المنشأة، أي أنها تمنع الدخول المخادع خلف المصرح لهم. وهناك عناصر تحكم أخرى مشابهة لأبواب الشخص الواحد مثل الأبواب الدوارة .
- **أقفال الكمبيوتر:** بعض أجهزة الكمبيوتر تحتوي على أقفال مفاتيح تساعد على قفل لوحة المفاتيح أو آليات الإدخال/الإخراج في الكمبيوتر، لحظر الدخول غير المعتمد عليها. والمشكلة في عنصر التحكم هذا أن المستخدمين غالبًا ما يفقدون المفاتيح أو ينسونها في الأقفال طوال الوقت.

في حالة إمكانية حدوث خطورة عالية بسرقة أجهزة الكمبيوتر أو تخريبها، هناك العديد من عناصر التحكم التي يمكن أن يضعها العميل أمام عينيه:

خزائن الأمن: مع تزايد وتيرة السرقات التي تطال رقائق الكمبيوتر، بدأ موفرو المنتجات الأمنية في إنتاج خزائن أمنية معدنية. وتتكون تلك الخزائن من أغلفة معدنية يمكن توصيلها بالأسطح المعدنية. وبالتالي، يتم وضع جهاز الكمبيوتر والإغلاق عليه داخل الأغلفة المعدنية. وهذا الأمر يصعب فتح جهاز الكمبيوتر وإزالة الرقائق منه.

الماء الذكي: يتكون من ماء يشمل على توقيع كيميائي فريد. وعندما يتم اقتحام مبنى العميل، يتم تشغيل نظام للكشف عن المقتحم، ويتم رش الماء "الذكي" من فتحات رش في السقف. ويمكن حينئذ اقتفاء أثر كل الأشخاص (اللصوص وغيرهم) ممن تصل إليهم المياه وإعادتهم إلى مسرح الجريمة.

"حواجز الضباب": يتم تنشيط هذه الأجهزة عند اكتشاف دخول مقتحم بحيث تقوم بنشر ضباب في الغرفة مما يؤدي إلى توجه ضباب كثيف بها. وهذا يقلل من الرؤية إلى درجة أنه يكون من الصعب حينها على اللص رؤية ما يفعله.

عناصر التحكم

منع الحرائق، واكتشافها وإخمادها

هذه الأنظمة مصممة لمنع اندلاع الحرائق أول الأمر، وفي حالة حدوث حريق، تقوم بالتعامل معها بشكل يتسم بالكفاءة.

وتشتمل عناصر التحكم التي تساعد على منع اندلاع الحرائق على:

جعل منشئات تقنيات المعلومات مقاومة للحرائق من خلال استخدام مواد بناء مقاومة للحرائق،

فرض سياسة لعدم التدخين في المبنى أو في مكان شبكة الكمبيوتر،

تنظيف غرفة الكمبيوتر، بحيث لا يسمح بتراكم الأتربة أو الأوراق،

وتشتمل عناصر التحكم التي تساعد على اكتشاف اندلاع الحرائق على :

كاشفات الدخان والحرارة.

وتشتمل عناصر التحكم التي تساعد على إخماد الحرائق على:

مطافئ الحريق المحملة باليد: يجب توخي الحذر لضمان استخدام طفاية الحريق الصحيحة. على سبيل المثال، بعض مطافئ الحريق لا تتناسب مع الحرائق الكهربية. أما مطافئ حريق ثاني أكسيد الكربون المحمولة أو مطافئ الهالون (BCF) فهي مناسبة للاستخدام في الحرائق الكهربية. ويجب أن تتوافر مطافئ الماء في أو بالقرب من مخازن معدات الكمبيوتر المستهلكة، مثل أوراق الطابعة والأدوات المكتبية،

أنظمة إخماد الحرائق التلقائية: يتم تنشيط تلك الأنظمة بشكل تلقائي، عند اكتشاف اندلاع حريق. وبشكل طبيعي، فإنها تصدر صوتًا مسموعًا عند تنشيطها وتبدأ في عمل عد عكسي محدد قبل تحرير مطافئ الحريق. ويجب أن يقسم النظام المبنى إلى مناطق أو قطاعات. ويسمح ذلك بتنشيط النظام في تلك المناطق التي يندلع فيها الحريق فقط. وغالبًا ما تستخدم أنظمة إخماد الحريق الماء أو الهالون , ويفضل استخدام الهالون، حيث إنه لا يؤدي إلى تدمير المعدات مثل الماء، كما أنه أقل خطورة فيما يتعلق بالصحة من مطافئ ثاني أكسيد الكربون.

ويجب صيانة أنظمة إخماد الحريق بشكل منتظم لضمان أنها في حالة تشغيل صحيحة. كما يجب فحص مقر المبنى من قبل إدارة أو سلطات المطافئ.

كما يجب تدريب الموظفين على كيفية الاستخدام الصحيح لأجهزة إخماد الحريق.

الحماية من الأضرار التي قد تنجم

لا تختلط مكونات أجهزة الكمبيوتر (وعلى وجه الخصوص الكهرباء التي توفر الطاقة للمعدات) مع الماء.وبالتالي، يجب أن تتواجد منشئات أجهزة الكمبيوتر منذ البداية في أماكن يقل فيها احتمالية وصول الماء إليها، وثانيًا، في حالة وصول الماء إليها، يجب توفر القدرة على اكتشاف ذلك.

ويمكن أن تصل المياه إلى غرفة الكمبيوتر من أكثر من مصدر، مثل:

الفيضانات؛

الأسقف التي تسرب المياه؛

انفجار أنابيب الماء؛

فيضان المياه في المنخفضات التي يتجمع فيها، وفي الحمامات؛

التسرب من شبكة التدفئة؛

التكاثف ؛

وحيث أن الماء يغمر بناءً على تأثير الجاذبية، يمكن تقليل المخاطر التي تنجم عن الماء من خلال وضع منشئات الكمبيوتر في مناطق مرتفعة، أي ليس في الأدوار السفلى أو السراديب. ومن الشائع أن يتم وضع منشئات الكمبيوتر في الدور الثالث أو السادس من المبنى.

ويجب أن يتم وضع مجسات اكتشاف الماء تحت الأرضيات المرفوعة. ويجب توصيلها بأجهزة إنذار مرئية ومسموعة , وحتى عندما تتواجد منشئات الكمبيوتر فوق مستوى الأرض، لا تزال توجد خطورة من انفجار أنابيب الماء أو من الأسقف التي تسرب الماء. والأسقف المسطحة مشهورة بتسريبها للماء.

حماية مصدر توفير الطاقة

وترتبط الاهتمامات الأساسية للمراجع بالتأثيرات المحتملة للكهرباء على توافر الأنظمة وتكامل البيانات التي تتم معالجتها.

ويجب أن تحتوى أنظمة العميل على عناصر تحكم موجودة لتقليل تأثير انقطاع التيار أو انحرافات التيار الكهربي (مثل حالات الخلل في الطاقة، أو قلة الفولتية). ويمكن تحقيق ذلك بشكل طبيعي من خلال تواجد:

أجهزة الحماية ضد زيادة التيار: يمكن أن تختلف فلولتية وتردد تيار المصدر. ويمكن أن تكون أجهزة الكمبيوتر حساسة لهذه التغيرات ويجب حمايتها من حالات الخلل في التيار وانخفاضه ومن التغيرات التي تحدث في التردد. وتراقب منظمات الفولتية الكهرباء القادمة وتقوم بتعديلها حسب متطلبات الأنظمة. وبشكل عام، يتم دمج أجهزة الحماية ضد زيادة التيار في أجهزة تزويد التيار غير المتقطع.

أجهزة تزويد التيار غير المتقطع: تسمح أجهزة تزويد التيار غير المتقطع (UPS) باستمرارية عمل أجهزة الكمبيوتر إلى أن تعود الطاقة مرة أخرى، حيث يمكن تشغيل المولد الاحتياطي أو إغلاق النظام بالطريقة الطبيعية.

وتختلف متطلبات أجهزة تزويد التيار غير المتقطع حسب الاحتياجات المحلية، مثل التردد ومدد انقطاع التيار.

ويمكن أن تشتمل عناصر التحكم الإضافية في التيار الكهربي على:

المولدات الاحتياطية: : يتم استخدامها في الغالب عندما يستمر انقطاع التيار لمدة تزيد على عدة ساعات قليلة. يوجد نوعان من أنواع المولدات، مولدات الديزل ومحركات الغاز؛
كابلات التيار البديلة: في بعض الحالات، يشعر العملاء بالحاجة إلى توصيل أجهزة الكمبيوتر لديهم بمحطتين فرعيتين للطاقة آملين ألا يؤثر أي انقطاع في أحد المصدرين على المصدر الآخر.
من خلال فحصنا لبعض الجهات عدم وجود العدد الكافي من المثبتات الفولتية لكافة الأجهزة المستخدمة في الجهة . يوجد اهتزازات في شاشات الكمبيوتر بشكل كبير وقد تكون نتيجة وجود تأثير كهرومغناطيسي قوي السخونة والتهوية وتكييف الهواء:
تتطلب الكثير من أجهزة الكمبيوتر الضخمة وأجهزة الكمبيوتر الرئيسية وأجهزة الكمبيوتر الصغيرة تواجد بيئة خاضعة للتحكم حتى تعمل بكفاءة وقد يتطلب من تلك الأجهزة التحكم في درجة الرطوبة ودرجة الحرارة , وقد تؤدي أجهزة الكمبيوتر الرئيسية إلى توليد مقادير كبيرة من الحرارة، وإن لم تتوافر تهوية جيدة، قد تكون هناك خطورة من حدوث فشل في المعدات.
ويمكن التحكم في ذلك من خلال تشغيل أجهزة تكييف الهواء.
فإذا كان من الضروري تكييف الهواء لاستمرار عمل أجهزة الكمبيوتر، يجب أن يراجع المراجع على إجراءات وتعاقدات الصيانة لدى العميل.

الصيانة وإدارة

قد يتواجد لدى العميل بعض عناصر التحكم لضمان أن أجهزة الكمبيوتر والأماكن الموجودة فيه تتسم بالنظافة والخلو من القمامة (الأوراق والأتربة والدخان وغير ذلك).
كما يمكن أن تتوافر سياسات تمنع تناول الأطعمة والمشروبات في المنطقة التي تتواجد بها أجهزة الكمبيوتر. فقد يؤدي قلب كوب من القهوة إلى حدوث تأثيرات خطيرة على جهاز الكمبيوتر. لوحظ في الفحص الميداني عدم الاهتمام بتثقيف المستخدمين بالمخاطر

عناصر تحكم الوصول

لقد أصبحت الأيام التي تعودنا فيها على كتابة المعلومات على الأوراق وتخزينها في خزانات، في معظم الأحوال، جزءًا من التاريخ البعيد والمظلم. واليوم، فإن معظم الأنظمة المالية التي يتم تدقيقها من قبل المراجعين تستخدم الكمبيوتر.
فالعملاء يعتمدون على أجهزة الكمبيوتر التي لديهم للبدء في تسجيل وعمل التقارير للعمليات المالية لديهم.
والأمر الآخر الذي يجب وضعه في الاعتبار هو كيفية حماية البيانات ومواد الأعمال.
فأنظمة الكمبيوتر قد لا يمكن التحكم فيها بسهولة من خلال عناصر التحكم في الوصول المادي مثل الأدراج المغلقة والدواليب. و على وجه الخصوص عندما تكون أجهزة الكمبيوتر لدى العميل متصلة بشبكات محلية أو واسعة.

<u>على سبيل المثال</u>

توصيل نظام مالي بشبكة واسعة باستخدام وصلات الاتصال عبر الهاتف مثل أجهزة مودم الاتصال الهاتفي. وفي تلك الحالة لا تتمكن الأقفال الموضوعة على الأبواب وأجهزة الإنذار ضد السرقة وحراس الأمن من إيقاف أي شخص من الوصول إلى أنظمة الكمبيوتر عبر تلك الشبكة.

ويجب توافر أسلوب آخر لحماية الأنظمة والبيانات التي تقوم بمعالجتها. وهنا، يظهر دور عناصر التحكم في الوصول المنطقي.
ويتم تعريف عناصر التحكم في الوصول المنطقي على أنها "نظام بالإجراءات، التي يتم تطبيقها في المؤسسة وبرامج الكمبيوتر التي يتم استخدامها، والذي يهدف إلى حماية موارد الكمبيوتر (البيانات والبرامج والأجهزة الطرفية) ضد محاولات الوصول غير المعتمدة."
ويوجد ثلاثة عناصر أساسية في أمان الوصول المنطقي.

تعريف المستخدم:
حيث يشمل ذلك على تعريف المستخدم بنفسه للكمبيوتر من خلال استخدام اسم مستخدم أو معرف لتسجيل الدخول وما إلى ذلك.

التحقق من المستخدم:
يتطلب الكمبيوتر توافر تأكيد بأن المستخدم هو بالفعل من يزعم أنه هو. وهو أمر يمكن تحقيقه من خلال توفير المستخدم لشيء يملكه أو يعرفه، أو كلاهما. وتعد كلمات السر وسيلة شائعة للتصديق. وتشتمل الوسائل الأخرى للتصديق على أرقام PIN (التي تستخدم للتصديق عليك بعد وضع بطاقتك البنكية في آلة الصرف الآلي)، والتوقيعات أو البيانات الحيوية مثل بصمة اليد.

حماية الموارد (أو امتيازات الوصول)
تعد الموارد هنا هي ملفات الكمبيوتر، والأدلة والأجهزة الطرفية الملحقة. وتقوم حماية الموارد على احتياجات كل مستخدم. على سبيل المثال، عندما يقوم مستخدم ما بالدخول (من خلال تعريف نفسه والتصديق عليه)، يعرف الكمبيوتر من هو هذا المستخدم ويحظر قدرة الوصول إلى ملفات أو تطبيقات أو موارد أخرى بعينها حسب المتطلبات الوظيفية لهذا المستخدم.

ويجب أن يضع المراجع في رأيه أن بعض أنظمة التشغيل وخيارات التحكم للوصول إلى المنطقة المرتبطة بها والملفات وغيرها هي أمور ذات طبيعة تقنية عالية. وعندما تكون أنظمة العميل معقدة تقنيًا ولا يمتلك المراجع المعرفة اللازمة بالأنظمة الخاصة بالعميل، قد يحتاج مراجع تقنية المعلومات للحصول على دعم إضافي من مراجع متخصص في مجال تقنية المعلومات و الذي يمتلك تلك الخبرات والمهارات.
ومن غير المحتمل أن يمتلك مراجع تقنية المعلومات الخارجي معلومات تفصيلية لأكثر من عدة أنظمة (على سبيل المثال، أنظمة التشغيل الشائعة مثل يونكس ونوفيل ووينوز إن تي).
مثل تدقيق جهاز كمبيوتر رئيسي يستخدم MVS. فإذا لم تتوافر عند المراجع الخارجي الخبرة اللازمة لتشغيل مثل هذه الأنظمة أو تدقيقها، فمن غير المحتمل أن يمتلك المراجع معلومات كافية حول النظام لإجراء عمليات تدقيق تقني متعمقة.
فعندما يتم تكليف مراجع تقنيات المعلومات بمهمة لعمل مراجعة عميقة لعناصر التحكم في الوصول المنطقي في نظام معقد، قد يحتاج المراجع للحصول على دعم إضافي من شخص متخصص في بيئة التشغيل المطلوب مراجعتها.

المخاطر المرتبطة بعناصر تحكم الوصول المنطقي

نتركز التأثيرات الاساسيه التي قد تنجم عن نقص عناصر تحكم الوصول المنطقي فيما يلي:

كشف الأشخاص غير المعتمدين للمعلومات
تعديل الأشخاص غير المعتمدين للمعلومات
وخرق تكامل النظام
وقد يكون التأثير المحتمل لخرق عناصر تحكم الوصول المنطقي أكبر، فيما يتعلق ببدء أجهزة الكمبيوتر للمعاملات وتسجيلها لها. ففي الأنظمة اليدوية، اعتاد المسئولون الماليون على العناية بدفاتر الشيكات وغيرها من المستندات المالية. وعندما أصبح أحد العملاء يمتلك نظام كمبيوتر، يجب أن يتم تطبيق نفس المبادئ وأن تتوافر لدى العميل عناصر التحكم اللازمة للحيلولة دون حصول الأشخاص غير المعتمدين على إمكانية الوصول إلى السجلات المالية الإلكترونية (مثل ملفات الدفع الإلكترونية قبل نقلها إلى البنك).
وفي حالة توصيل أنظمة العميل بشبكة واسعة مثل الإنترنت، تكون المخاطر أكبر من ذلك بكثير. فطبيعة السجلات الإلكترونية قد لا تساعد على توضيح أن أحد الأشخاص قد قام بعمل تعديلات غير معتمدة في الملفات.
وهذا أمر يشير إلى أهمية وضع عناصر تحكم في الوصول المنطقي لضمان تكامل وإتاحة وسرية نظام العميل المالي. لوحظ في الفحص الميداني عدم الاهتمام بهذه الإجراءات .

1- <u>المهاجمون</u>

يمكن مهاجمة أنظمة الكمبيوتر من اتجاهات عدة. وأول مهاجم يخطر على العقل هو المخرب. والمخربين هم أشخاص لديهم معرفة كبيرة بأجهزة الكمبيوتر يحاولوا الوصول إلى الأنظمة لإثبات قدرتهم على الوصول إليه. وهم يرون في هذا الأمر تحديًا شخصيًا لأنفسهم. وعلى الرغم من أن هدفهم الأول هو مجرد الوصول، فقد يقوموا على نحو غير متعمد بالتسبب في حدوث الأضرار في الأنظمة أو البيانات. كما أنه من الممكن أن يكونوا من صغار السن المستخدمين لبرامج وأدوات التطفل التي يمكن الحصول عليها مجانًا من على الإنترنت.
الموظفون:وقد يكون هؤلاء الموظفون في إدارة تقنيات المعلومات، أو غيرهم من المستخدمين العاديين للنظام.يجب أن يلاحظ المراجع عناصر التحكم المفروضة على الموظفين المؤقتين أو العاملين لفترات. انه من خلال قيامنا بعملية المراجعة في إحدى الجهات وجدنا الموظفين يتداولون كلمات السر فيما بينهم بالرغم من وجود كلمة سر لكل موظف وبينوا لهم خطورة ذلك .
الموظفون السابقون: الموظفون السابقون، خصوصًا ممن يكون لديهم ضغينة ضد الشركة، قد يحاولوا الوصول إلى النظام للثأر من الشركة.
الأطراف الخارجيين : قد يضم المنافسين أو قوى خارجية (تجسس) أو الجرائم المنظمة.
الموردون والمستشارون: وغالبًا ما يكون هؤلاء الأطراف هم من ينشئون النظام أو يقومون على صيانته.

2- <u>تبعات خرق أمان عناصر تحكم الوصول المنطقي</u>

أسلوب التدقيق: قد يؤدي ضعف عناصر تحكم الوصول المنطقي إلى جعل الاعتماد على عناصر التحكم أمرًا صعبًا إن لم يكن مستحيلاً.
رأي التدقيق: بصفتك مراجعًا خارجيًا، يكون هذا الأمر هو أكثر الاهتمامات من ناحية الوضوح والأهمية. فقد لا يمكن تدقيق الحسابات بسبب فقد سلسلة التدقيق المالي، أو قد تحتوي الحسابات على أخطاء مادية تنتج عن فقد تكامل البيانات.

الخسائر المالية: قد تكون الخسائر عبارة عن خسائر مباشرة نتيجة الغش والخداع، أو غير مباشرة تنجم عن تكلفة تعديل النظام وتصحيح البيانات.
الالتزامات القانونية: قد تكون على العميل بعض الالتزامات القانونية فيما يتعلق بالتخزين والإفصاح عن البيانات، على سبيل المثال، إذا كان هناك قانون يتطلب من العميل الحفاظ على سرية أية بيانات شخصية. وفي بيئة البنوك، قد تؤدي خسارة التكامل إلى حدوث خرق في التشريعات المنظمة والإجراءات التأديبية في البنك.
خسارة في حصة السوق، و/أو المصداقية: وهذا الأمر هام على وجه الخصوص في قطاع الخدمات المالية، مثل البنوك أو البورصات أو الهيئات الاستثمارية. وقد يؤدي حدوث خرق أمني إلى فقد المصداقية وفي النهاية خسارة المشروعات التجارية.
تعطيل العمل : على سبيل المثال، في حالة قدرة أحد المخربين للوصول إلى أنظمة الكمبيوتر وتغيير كل أبعاد المنتجات في نظام التعامل مع التصنيع.

الموارد والملفات والمنشئات التي تحتاج

1. ملفات البيانات
قد تتكون تلك الملفات من ملفات أو قواعد بيانات العمليات. وتجب حماية أية ملفات تحتوي على ملفات أصلية أو معلومات وبيانات ثابتة، مثل ملفات معدلات المرتبات، ونظام أكواد الحسابات البنكية وغيرها. فإذا لم تتم حماية تلك الملفات، فقد يقوم شخص ما بعمل تعديلات غير معتمدة عليها، أو حتى يقوم بحذف البيانات.

2- التطبيقات
يؤدي الوصول غير المحدود إلى زيادة مخاطر تعرض التطبيقات المالية لتعديلات غير معتمدة قد تؤدي إلى حدوث الغش أو فقد البيانات أو تلفها. فقد يساعد الوصول غير المعتمد للكود المصدري للتطبيق إلى إجراء تعديلات في المنطق البرمجي له، مثل تقريب المدفوعات إلى أقرب وحدة (بنس ، أو سنت، وما إلى ذلك) وترحيل الكسر التقريبي إلى حساب الشخص الذي يقوم بالبرمجة.
وعندما يقوم النظام بعمليات حسابية معقدة، قد لا يكون من الممكن فحص العمليات الحسابية للتطبيقات بشكل منفصل، وقد لا يتم كشف التعديلات غير المعتمدة لمدة طويلة.

3- ملفات كلمات السر
إن لم تتم حماية تلك الملفات بشكل كافٍ وأتيحت القدرة لكل شخص على الوصول إليها، فليس في الإمكان الحيلولة دون حصول أي شخص على تعريف للدخول وكلمة سر لأحد المستخدمين ممن لديهم الامتيازات بالوصول.وقد يتمكن أي مستخدم غير معتمد ممن يحصلون على الأذون بالوصول الخاص بأحد مستخدمي النظام ممن تكون لديهم القدرة للوصول إلى التسبب في حدوث أضرار كبيرة.
حتى في حالة الحصول على كلمة سر ومعرف أي شخص عادي، يتم تجاوز المبدأ الذي يتم من خلاله محاسبة كل شخص عن الإجراءات التي يقومون بها. ويمكن أن يستخدم المستخدم غير المعتمد التعريف "المسروق" في إجراء تعديلات قد لا تساعد على التعرف على من ارتكبها، أو قد يستخدمه للحصول على امتيازات وصول أكبر. .لوحظ في الفحص الميداني لا يوجد سياسة وإجراءات لمرافق دائرة تكنولوجيا المعلومات يستطيع المستخدم فتح النظام علي أكثر من جهاز

بنفس كلمة المرور وكلمة السر الخاصة لا يتم الخروج الآلي المؤقت للنظام في حالة ترك الموظف للجهاز لا يوجد معايير مكتوبة من الإدارة بما يخص الرقابة على الفيروسات .

4- البرامج والأدوات المساعدة في النظام

تشمل هذه البرامج برامج التحرير والتجميع وحل المشكلات في البرامج. ويجب حظر الوصول إلى تلك البرامج حيث يمكن استخدام تلك الأدوات لإجراء تعديلات في ملفات البيانات وبرامج التطبيقات.

5- ملفات السجلات

تستخدم ملفات السجلات لتسجيل الإجراءات التي يقوم بها مستخدم ما، وبالتالي فهي توفر شكلاً من أشكال المحاسبة لمسئولي النظام والإدارة في شركة العميل. ويمكن أن يسجل سجل النظام من قام بالوصول إلى النظام وما هي التطبيقات وملفات البيانات والأدوات المساعدة التي استخدمها أثناء تواجده. ويمكن أن يتم استخدام سجل تطبيق لتسجيل التغييرات التي تتم في البيانات المالية (من قام بتغيير أي بيانات وماذا كان التغيير، ومتى). فإن لم تتم حماية ملفات السجلات بشكل كافٍ، يمكن أن يقوم الهكر أو شخص مخادع بحذفها أو تحريرها لإخفاء الإجراءات التي قام بها. .لوحظ في الفحص الميداني عدم الاهتمام بتثقيف المستخدمين بالمخاطر

6-الملفات المنتظرة أو الملفات المؤقتة

يمكن استخدام الملفات التجهيزية أو الملفات المؤقتة لتخزين المعلومات قبل العمل وفقًا لها.على سبيل المثال، عندما يقوم أحد المستخدمين بإجراء طباعة لشيك، يتم عمل ملف مؤقت يشمل على تفاصيل الشيك. ويستخدم هذا الملف لطباعة الشيكات عندما تكون الطابعة جاهزة.وبدون توفير الحماية اللازمة، يمكن أن يقوم أي شخص بتحرير الملف وتغيير تفاصيل الدفع قبل أن يتم إرسالها إلى الطابعة.

إطار عمل امن الوصول

تقع المسئولية على الإدارة لدى العميل فيما يتعلق بضمان وجود عناصر التحكم الكافية للتعامل مع أي مخاطر يتم التعرف عليها في الأنظمة. ويجب أن تعطي الإدارة التوجيهات حول ما هي عناصر التحكم في الوصول المنطقي التي يجب أن تتواجد من خلال وضع سياسة امن وصول في بادئ الأمر.

وأثناء وضع السياسة، يجب أن تحدد الإدارة متطلبات الأعمال فيما يتعلق بالتحكم في الوصول كما يجب أن تحدد متطلبات الوصول لكل نظام.

وغالبًا ما تكون سياسات الأمن في الشركات عبارة عن مستندات قصيرة بشكل نسبي.وقد تحتوي تلك السياسات على ما يلي:

التعريفات: مثل ما هو المقصود بالأمان، وما هو المقصود على وجه الخصوص بالسرية والتكامل والإتاحة،

بيانات السرية مثل:

- ضرورة توافر مالك لكل تطبيق والملفات المتعلقة به، ويجب أن يتم تصنيف تلك المعلومات من ناحية السرية والتكامل والإتاحة،
- إمكانية الوصول إلى المعلومات الموجودة في الأنظمة فقط عند الحاجة إليها. تتوقف تلك الحاجة على الوظيفة (الأدوار، والمسئوليات والمهام) لكل مستخدم من مستخدمي الأنظمة

ووظيفة مستخدم نظام الكمبيوتر، وتتناسب درجة الحماية مع مستوى الخطورة وقيمة الأصول،

المسئوليات:يجب تحديد مسئوليات كل المستخدمين.ويتم ذلك بشكل عام من خلال تجميع المستخدمين في ملفات تعريفية معينة مثل "المستخدمون العاديون" ومالكي الأنظمة وإدارة الأمن وتدقيق نظام المعلومات/تقنية المعلومات.

وتعتمد عناصر تحكم الوصول المنطقي المفصلة على بيانات المستوى العلوي في سياسة أمان تقنية المعلومات في الشركة.

عناصر تحكم أنظمة التشغيل والوصول إلى

قد تتواجد عناصر تحكم الوصول المنطقي، وغالبًا ما تتواجد في الأنظمة المالية، في مستويين، مستوى التثبيت ومستوى التطبيقات.وبالتالي، يمكن إنشاء عناصر التحكم في الوصول في:

نظام التشغيل .

كل تطبيق على حده.

يتم التحكم في عناصر تحكم الوصول المنطقي في كل مستوى من خلال مسئولين مختلفين. فقد يكون شخص ما في إدارة تقنيات المعلومات مسئولاً عن إدارة من يمكن له الوصول إلى الشبكة، وما هي ملفات البيانات التي يمكن الوصول إليها عند الدخول إلى الشبكة. فهذا الشخص يتحكم في الوصول على مستوى التثبيتات.

قد يكون هناك مسئول تطبيقات منفصل يتمثل دوره في المسئولية عن إدارة من يمكنه أن يفعل ماذا في كل تطبيق من التطبيقات.

قد يكون لدى مسئول النظام في قسم تقنيات المعلومات فهمًا أفضل لنظام التشغيل والموارد المتعلقة به، وقد يعرف ما هي التطبيقات وأدوات النظام الهامة التي يجب حمايتها. وقد يسمح ذلك بحماية موارد النظام من الأشخاص الخارجيين ومن العاملين في تقنية المعلومات غير المعتمدين.

قد يكون لدى مسئولي التطبيق معرفة أفضل بالتطبيقات ومن يستخدمونها.وقد يسمح هذا الفهم بالتطبيقات لمسئولي التطبيقات بتغيير امتيازات الوصول حسب احتياجات كل مستخدم. فقد يتمكن شخص لديه معرفة بالإدارة المالية من معرفة الأنشطة التي يقوم بها كل عضو في الفريق للقيام بأعمالهم بشكل يتسم بالكفاءة. وقد يضمن ذلك ألا يتم إعطاء المستخدمين الوصول إلا وظائف معينة في التطبيقات، تلك الوظائف التي يحتاجون إليها في أعمالهم، فمثلاً قد يعرف مسئول التطبيق أن موظف طلب الشراء قد لا يحتاج الوصول إلى نظام المبيعات، وبالتالي لا يسمح له بالوصول إلى هذا النظام. ويتم تغطية أمان التطبيقات أيضًا في الدورة التدريبية 2.4 والدورة التدريبية 2.5.

ويضيف هذا الأسلوب إلى القدرة على التحكم من خلال تقسيم المهام الأمنية بين مسئول النظام ومسئول التطبيق.

عناصر التحكم في الوصول المنطقي على مستوى

يتم دمج عناصر تحكم الوصول المنطقي كثيرًا في برامج نظم التشغيل من قبل الشركات المصنعة (مثل يونكس، ونوفيل، إن تي).وتختلف قوة القدرة على الوصول من منتج إلى آخر.وهناك بعض المؤسسات التي تقوم بإجراء اختبارات مستقلة على امتيازات الأمان في أنظمة التشغيل. وتعد

التقييمات الأكثر شهرة عالميًا هي التي تقوم بها وزارة الدفاع الأمريكية باستخدام "المعايير محل الثقة لتقييم الكمبيوتر" والتي تعرف بشكل أكثر شيوعًا باسم "الكتاب البرتقالي". ويقوم الكتاب البرتقالي بتقسيم الأنظمة إلى فئات تتراوح بين د و أ، حيث يتم اعتبار الفئة أ هي الفئة الأكثر أمنًا.
ويتم بناء معظم الأنظمة المالية بحيث تتوافق مع التصنيف ج2، ما لم تكن هناك أية دواعي أمنية إضافية. وللحصول على التصنيف ج2، يجب أن يمتلك نظام التشغيل حماية بالتحكم في الوصول مع تدقيق الأحداث الأمنية وتخصيص الموارد.
وبالتالي، إذا أخبر أحد العملاء المراجع أن نظامه يتطابق مع معايير ج2، فمن المحتمل أن يشمل النظام على وسيلة للتصديق على الهوية وعناصر تحكم للتسجيل.
وهناك هيئات أخرى تقوم بتقييم الأمان، مثل ITSEC (معايير تقييم أمان تقنية المعلومات)، والتي تقوم على معايير الأمان الأوروبية. وهناك أساليب تقييم أخرى تمت تغطيتها بعمق أكثر في الدورة التدريبية 4.2.
وفي حالة عدم احتواء أنظمة التشغيل على أمان وصول منطقي مدمج بها ، فقد يقوم العميل بتثبيت حزم منفصلة عليها لتوفير تلك الميزة. على سبيل المثال، إن الشائع لمستخدمي أجهزة كمبيوتر IBM الرئيسية القيام بتثبيت حزم التحكم في الوصول مثل RACF وACF2. كما توجد أيضًا حزم أمان مملوكة للشركات،ومتاحة لأجهزة الكمبيوتر الصغيرة.

1- إجراءات الدخول

يتم استخدام إجراءات الدخول الطرفية للحصول على البيانات والتطبيقات على أنظمة الكمبيوتر.وعندما يطلب المستخدم الوصول إلى النظام، يتم تنشيط عملية الدخول (مثلاً من خلال التشغيل العادي أو من خلال النقر على أيقونة أو كتابة أمر للدخول). ويساعد ذلك على تنشيط برنامج للدخول. وتوجه إجراءات الدخول المستخدمين من خلال الخطوات التي يجب اتخاذها لتعريف هويتهم للكمبيوتر والتصديق عليها. وغالبًا ما يتضمن ذلك إدخال المستخدمين لتعريفات الدخول الخاصة بهم يتبع ذلك إدخال كلمات السر.
ويجب أن تشتمل إجراءات الدخول على عناصر التحكم التالية:

ألا يتم عرض اسم المؤسسة إلا بعد أن يقوم المستخدم بتسجيل الدخول. فهذا يؤدي إلى التقليل من الأدلة التي قد يوفرها النظام لأي مستخدم غير معتمد.على سبيل المثال، إذا عرضت مؤسسة قومية تعمل في مجال أبحاث الفضاء بعرض رسالة تسجيل دخول تشتمل على اسم المؤسسة، فمن الممكن أن يستطيع أي مستخدم غير معتمد بتوقع الطريقة التي يمكنه بها تخمين كلمات السر.فمن الممكن أن يقوموا باستخدام كلمات السر مثل nebula وquasar وsolar وغيرها.

ألا يحتوي التسجيل على "ترحيب" بأي شخص. فتوجد حالة شهيرة تمكن فيها مخرب محترف من الوصول إلى نظام كمبيوتر كان يحتوي على شاشة ترحيب. ولقد نجا هذا المخرب من المقاضاة بسبب شاشة الترحيب، التي اعتبرت دعوة للوصول إلى النظام

يجب ألا يخبر برنامج الدخول بالنجاح أو الفشل إلى أن تتم عملية الدخول كاملة. وهذا يضمن عدم إخبار المستخدم غير المعتمد بموضع الخطأ الذي يجب إصلاحه للحصول على الوصول.

قطع الاتصال بشكل تلقائي بعد عدد محدد من محاولات الدخول

يجب تعطيل أي تسهيلات قد تظهر على الشاشة أثناء عملية تسجيل الدخول، حتى لا يتمكن الأشخاص غير المعتمدين من الحصول على الإرشادات حول كيفية الوصول إلى النظام.

وبمجرد تسجيل المستخدمين للدخول، يمكن أن يتمكن النظام من عرض وقت وتاريخ آخر مرة تم فيها تسجيل الدخول للمستخدم، وتفاصيل أية محاولات غير ناجحة للدخول. فمن شأن ذلك أن يساعد على وضع محاولات الوصول إلى النظام أمام أعين المستخدم. على سبيل المثال، إذا قام أحد المستخدمين بالدخول إلى النظام في الصباح، وظهرت رسالة لتعلمه أن آخر مرة قام فيها بالدخول إلى النظام كانت الساعة الرابعة والنصف في الصباح، فهذا يعني أن شيء ما خطأ قد حدث.

2-تعريف المستخدم

يتم تعريف المستخدم بشكل طبيعي من خلال إدخال المستخدم لمعرف الدخول الخاص به. ويجب أن تتوافر لدى العميل سياسة لتكوين أكواد تعريف الدخول، على سبيل المثال، من خلال استخدام الحروف الثلاثة الأخيرة من الاسم الأخير لهم، ثم الحرف الأول من الاسم الأول ثم رقم مكون من عددين، وبالتالي يكون معرف دخول السيد جيمس سميث هو SMIJ27.

إذا كانت السياسة التي يقرر العميل استخدامها، يجب أن تضمن تلك السياسة أن تكون معرفات الدخول لكل مستخدم هي معرفات فريدة. فالتفرد أمر هام حيث إنه يساعد على التعرف على كل شخص. وبالتالي، فهو يساعد على مسئولية كل مستخدم عن حسابه، خصوصًا في الحالات التي يتم تسجيل معرفات الدخول التي يتم التصديق عليها للمستخدمين والأنشطة التي يقوم بها الشخص للدخول لهذه المعرفات في النظام.

ويجب أن يحتفظ الكمبيوتر بقائمة بمعرفات الدخول لكل المستخدمين المعتمدين.

وقد تستخدم بعض الأنظمة رمزًا كنوع من التعريف، مثل البطاقات التي تحتوي على شريحة ممغنطة على الخلف. .لوحظ في الفحص الميداني عدم الاهتمام بتثقيف المستخدمين بالمخاطر

3- التحقق

بعد أن يعرف المستخدم نفسه لنظام الكمبيوتر، يجب أن يقوم الكمبيوتر بالتأكد من أن هذا المستخدم هو من يدعي ذات الشخص. وهذه العملية تعرف باسم التصديق.

وهو أمر يمكن تحقيقه من خلال توفير المستخدم لبيانات تخصه، أو من خلال مقارنة السمات الشخصية الفعلية.وتقوم معظم أنظمة التحكم في الوصول بالتصديق على المستخدم من خلال طلب كلمة سر.

فإذا كانت كلمة السر صحيحة، يتم السماح للمستخدم بالدخول إلى النظام. أما إذا لم تكن كلمة السر صحيحة، يتم رفض طلبه للدخول إلى النظام.

وحتى تكون كلمات السر مؤثرة، يجب أن تفي كلمات السر بالمتطلبات التالية:

<u>تكوين كلمات السر.</u> يجب أن تحظر سياسة العميل كلمات السر التي تعتمد على ما يلي:

* أسماء العائلة، أو العناوين أو الحروف الأولى من الأسماء (بما في ذلك أسماء الحيوانات الأليفة)
* أرقام تسجيل السيارات
* أرقام الهواتف
* تكوينات الحروف التي يسهل توقعها، مثل qwerty
* الحروف أو الأرقام المفردة (فكلما زادت الخيارات، صعب تخمين كلمة السر)

* كلمات القاموس (تكون الكلمات التي تظهر في برامج الخيال العلمي شائعة)
* ما يمكن للمستخدمين أن يروه من النافذة (من الشائع منطقيًا استخدام المستخدمين لكلمات السر بناءً على شيء يمكن أن يرونه من مكتبهم، مثل Compaq 486، أو اسم محطة البنزين الموجودة على الجانب الآخر من الطريق).

الحد الأدنى من طول الكلمة: كلما زاد عدد الحروف، صعب تخمين كلمة السر.إلا أنه كلما توجب زيادة طول كلمات السر، تزداد احتمالية أن ينسى المستخدمون كلمات السر الخاصة بهم. ومن الشائع استخدام حد أدنى لا يقل عن 6 حروف في الأنظمة المالية؛

عمر كلمات السر: أي أن كلمات السر يجب أن تنتهي صلاحيتها بعد عدد محدد من الأيام (30-60 يومًا هو الشائع) وبالإضافة إلى ذلك، بعض الأنظمة لا تتيح للمستخدمين تغيير كلمة السر بعد عمل تغيير مباشرة. فعليهم في هذه الحالة الانتظار لفترة من الوقت، مثل 7 أيام، حتى يتسنى لهم تغيير كلمة السر مرة أخرى؛

تاريخ كلمات السر: تقوم بعض أنظمة كلمات السر بالاحتفاظ بسجل تاريخي لآخر كلمات السر وتمنع المستخدم من استخدام كلمة من الكلمات القديمة. وهذا الأمر يمنع على المستخدمين استخدام بعض كلمات السر المفضلة لديهم بشكل تتابعي دوري؛

سرية كلمات السر: أي اشتراط ألا تتم كتابة كلمات السر أبدًا أو مشاركتها مع شخص آخر. وبالإضافة إلى ذلك، يجب ألا تظهر كلمات السر على الشاشة أثناء إدخالها. بل يجب أن تعرض الشاشة مجموعة من النجوم.

التخصيص الأولي: يجب وضع إجراءات التخصيص الأولي لإضافة المستخدمين الجدد للنظام قيد التشغيل. يتم تخصص كلمات السر الأولية بشكل عام من خلال مسئولي النظام. وإذا كان النظام يتيح للمستخدمين تغيير كلمة السر، فيجب أن يقوموا بتغييرها في أقرب فرصة. ويمكن أن يكون النظام قادرًا على فرض تغيير كلمة السر على المستخدمين، فمثلاً عند إضافة مسئول النظام مستخدمًا جديدًا، يمكن ضبط فترة عمر كلمة السر على وقت تكون فيه كلمة السر قد انتهت بالفعل. وعندما يقوم المستخدم الجديد بالدخول لأول مرة، يخبره النظام أن كلمة السر قد انتهت صلاحيتها وأنه يجب أن يتم تغييرها قبل أن يتم السماح له بالدخول

تشفير كلمات السر : يجب أن تتم حماية كلمات السر للحيلولة دون كشفها للأشخاص غير المعتمدين. ويعد التشفير أسلوبًا شائعًا لحماية البيانات في ملف كلمات السر. فإذا رأيت كلمة سر غير مشفرة، يمكنك التعرف على كلمة السر الحقيقية , ويمكن في تلك الحالة نسخها واستخدامها في وقت لاحق؛

وتقوم بعض الأنظمة بتطبيق لوغاريتم على كلمات سر المستخدمين ثم تقوم بحفظ الناتج في ملف لكلمات السر.وعند تسجيل المستخدم للدخول، يتم تشفير كلمة السر التي يدخلها بنفس اللوغاريتم، وتتم مقارنتها بكلمة السر المشفرة المحفوظة في ملف كلمات السر. فإذا تطابقا، يتم السماح للمستخدم بالدخول إلى النظام.

وتقوم أنظمة أخرى بتخزين كلمات السر في ملف مخفي لا يمكن للمستخدمين رؤيته. ويحول ذلك دون حصول المخربين على نسخ من ملفات كلمات السر المشفرة، وتشغيل بعض البرامج مثل "فك الشفرات" عليها. وهو برنامج يونكس يقوم بتشفير الكلمات ومقارنتها بكلمات السر المشفرة. وعند العثور على حالات مطابقة، يتم إخبارك بكلمة السر؛

كلمات سر العاملين الذين يتركون المؤسسة: عندما يترك الموظفون العمل في المؤسسة، يجب أن يتم إيقاف تشغيل كلمات السر والمعرفات الخاصة بهم. فهذا يساعد على التقليل من احتمالية قيام موظف سابق، يشعر بالسخط، من الوصول إلى الأجهزة. ويتطلب ذلك من العميل وضع إجراءات يتم إخبار مسئول تقنيات المعلومات بالحالات التي يتم فيها إنهاء التعاقدات مع الموظفين. ومن الشائع أن تكون إدارة تقنية المعلومات هي آخر من يعلم عند انتهاء تعاقدات الموظفين، ويجب أن يتم تجنب عبارة "لم يخبرنا أحد لإيقاف معرفه!".

الموردون وكلمات السر الافتراضية: عندما يتم عمل أنظمة جديدة، تشتمل على حسابات مستخدمين لاستخدام مهندسي التثبيت والموردين والاستشاريين. ويكون لكلمات السر تلك قدرات عالية على الوصول ويكون لها امتيازات كبيرة. يجب التحكم في هذه الحسابات بشكل شديد، كما يجب تعطيلها إن لزم الأمر. على سبيل المثال، قد تحتوي حزم المحاسبات على حساب مستخدم افتراضي للقيام باختبار النظام. وقد يكون معرف هذا الحساب هو "test" وتكون كلمة السر "test" أيضًا.

إرشاد وإجراءات ووعي المستخدم: يجب أن يكون المستخدمون على علم بسياسات كلمات السر لدى العميل. مثلاً، يجب أن يكون لديهم العلم بأن كلمات السر يجب ألا يتم مشاركتها مع الغير أو كتابتها. وقد تفيد الإجراءات المكتوبة المستخدمين حيث إنها تقلل من ارتكاب المستخدمين للأخطاء عندما يقومون بتغيير كلمات السر (مثلاً ما هي الأزرار التي يتم الضغط عليها، وكيف تفكر في كلمة سر يصعب تخمينها).

4- حماية الموارد

إن القدرة على الوصول إلى الكمبيوتر والقدرة على تسجيل الدخول إليه لا تنطوي على أن المستخدم قد أصبح له القدرة على الوصول غير المحدود إلى كل التطبيقات وملفات البيانات. فهناك مستوى آخر من التحكم يتوجب توافره بحيث يتم قصر المستخدمين على استخدام التطبيقات وملفات البيانات وموارد النظام (مثل الفواتير والطابعات وطابعات الشيكات ومحركات الأشرطة الاحتياطية) التي تم منحهم القدرة على الوصول إليها بشكل خاص.

ويمكن استخدام **عناصر التحكم في القوائم** لقصر الاستخدام على مستخدمين بعينهم. ويمكن استخدام القيود التي تفرض على القوائم لضمان ألا يحصل أي أحد سوى المستخدمين المصرح لهم بالوصول على حق الوصول إلى تطبيق أو ملف بيانات محدد. ويمكن أن تتواجد عناصر التحكم في القوائم في نظام التشغيل، أو برامج الأدوات المساعدة أو في التطبيقات.

على سبيل المثال، عندما يقوم موظف طلب مبيعات بتسجيل الدخول، يتم عرض قائمة بالتطبيقات على النظام. ويمكن أن تكون الخيارات المتاحة هي:

- نظام المبيعات
- نظام المشتريات
- نظام المخزون
- نظام الموظفين

ويمكن أن يقوم مسئول النظام بضبط النظام بحيث لا يكون لموظف المبيعات إلا القدرة على رؤية نظام المبيعات، أما خيارات القائمة الأخرى مثل معالجة طلب الشراء وإدارة المخزون والموظفين فيمكن أن يتم تعطيلها و"تلوينها باللون الرمادي"، مما يعني أنها لا تكون متاحة له.

تأمين الملفات والبرامج: يجب أن يتم منح إمكانية الوصول إلى وظائف النظام وبياناته إلى المستخدمين المعتمدين فقط ممن يحتاجون إلى الوصول لتنفيذ مهام وظائفهم. ويجب أن يتم منح الترخيص بنوع الوصول واستخدامه من قبل الإدارة على وجه الخصوص، مع أخذ عوامل التكامل والسرية في الاعتبار. وقد يعتمد العميل على مالكي التطبيقات للموافقة على وصول الموظفين قبل منح الوصول. وغالبًا ما يكون مالكو التطبيقات هم المستخدمين الأكثر للتطبيق، ويتم إعطاؤهم مسئولية ضمان أن يفي التطبيق بأهداف العمل. على سبيل المثال، غالبًا ما يكون مالك تطبيق محاسبي مالي هو رئيس قسم الحسابات، بينما يكون مالك نظام الموظفين هو مدير الموارد البشرية. ويجب الحصول على موافقتهم قبل أن يتم منح المستخدمين الجدد القدرة على الوصول إلى تطبيقاتهم من خلال القوائم.

وقد تشتمل عناصر التحكم على ما يلي:

التأكيد على استخدام وظائف محددة (مثل الأدوات المساعدة، وعناصر القوائم، والبرامج الضمنية المرتبطة بها، وما إلى ذلك)

القدرة على "احتواء" المستخدمين داخل مجموعات الوظائف المعتمدة، بالإضافة إلى حظر الوظائف حسب المستخدم أو الوقت أو الموارد.ويمكن أن يتم حظر وصول المستخدمين إلى قوائم محددة بعينها. فعندما يقوم شخص ما بالدخول إلى النظام، يتم وضعهم بشكل تلقائي في بيئة خاضعة للسيطرة، ويتم عرض خيارات القوائم المتاحة لهم.وقد تؤدي أية محاولة للوصول إلى أقسام أخرى من النظام (مثل دخول باستخدام أوامر نظام التشغيل، على سبيل المثال، من خلال الضغط على زر الخروج Esc) إلى تسجيل خروج المستخدم.

رفض موجه نظام التشغيل، مثل رمز C:\ في نظام الدوس أو رمز $ أو # في نظام يونكس.

ويجب أن يحظر قصر الوصول مخاطرة قيام أحد المستخدمين بتحميل أو تشغيل تطبيقات أو برامج مساعدة للنظام غير مصرح بها.

السماح بالملفات: القدرة على قصر الوصول إلى البيانات بما في ذلك التفريق بين الاستعلام عن البيانات وتحديثها أو تغيير البيانات. ويمكن أن يتم تخصيص امتيازات وصول لكل مورد على النظام. وعند محاولة أحد المستخدمين الوصول إلى مورد ما، يتم التحقق من الامتيازات المتاحة ومقارنتها بالامتيازات المسموح بها على الملف. فإذا كان المستخدم لديه الامتياز المناسب، تتم إتاحة استخدام الملف أو المورد.

والسمات العامة للملفات/الموارد هي:

قراءة ,كتابة , تكوين , تحديث , حذف , تنفيذ , ونسخ.

وعند مراجعة عناصر التحكم المرتبطة بامتيازات الملفات، يجب أن يقوم المراجع بالتحقق من عمل العناصر التكميلية التالية:

التأكد أن امتيازات الوصول تتناسب مع المتطلبات المصرح بها، ومن أن الوصول إلى إحدى المناطق أو إحدى الوظائف لا يؤثر على القيود المفروضة على منطقة أو وظيفة أخرى. على سبيل المثال، قد يتجاوز امتياز القراءة على مجلد ما تلك الامتيازات الخاصة المتاحة على ملفات في هذه الدليل، و

القيود الخاصة على القدرة على إضافة أو حذف أو تعديل عناصر القائمة أو البرامج أو الأدوات المساعدة. يتم قصر الوصول إلى تلك القدرة على مسئولي النظام في أغلب الأحيان.

يجب مراجعة امتيازات الوصول وتحديثها بشكل مستمر.

5- عناصر تحكم الوصول المنطقي الأخرى

تحديد عدد جلسات العمل المتزامنة. وهذا يعني أنه عندما يقوم أحد المستخدمين بتسجيل الدخول إلى النظام، لا يمكن أن يقوموا بتسجيل الدخول من جهاز طرفي آخر. فهذا يساعد على التقليل من مخاطرة وصول مستخدم غير معتمد بالوصول إلى النظام.

فإذا كان المستخدم الشرعي قد قام بتسجيل الدخول، لا يمكن للمحتال تسجيل الدخول.وإذا كان الشخص المحتال قد قام بتسجيل الدخول، وحاول الشخص الشرعي تسجيل الدخول لكنه منع من ذلك، يتم إخبار المستخدم بالمشكلة، وبالتالي يمكن البدء في اتخاذ الإجراء التصحيحي.

وضع حدود على ساعات العمل: هناك بعض أنظمة التشغيل (مثل نوفيل ووينـدوز إن تي) بمقدورها قصر الوصول على فترات زمنية محددة مسبقًا. فمثلا، إذا رأت الإدارة أنه لا داعي لأن يحصل أي شخص من فريق الإدارة المالية على القدرة على الوصول إلى النظام خلال فترات الليل (من التاسعة مساءً، وحتى السادسة صباحًا)، يمكن أن يتم تعديل النظام بحيث لا يتم لهم المساح بالدخول خلال تلك الفترة.

حصر محاولات تسجيل الدخول: ينطوي هذا الأمر على وضع حد لمرات إدخال كلمة السر الفاشلة التي يمكن أن يقوم بها المستخدم قبل أن يتم قفل إمكانية الوصول. ويقلل تحديد عدد معين من محاولات الوصول غير الناجحة إلى النظام من مخاطرة قيام أحد الأشخاص بتخمين كلمات السر. وبمجرد الوصول إلى هذا العدد، يمكن أن يقوم النظام بقفل معرف المستخدم لفترة معينة من الوقت، مثل 30 دقيقة، أو الإبقاء على المعرف مقفولاً إلى أن يتم تحريره من قبل مسئول النظام.

انتهاء وقت الوحدات الطرفية بشكل تلقائي: قد يتم استغلال الوحدات الطرفية التي لا يستخدمها أحد للحصول على وصول غير معتمد إلى نظام الكمبيوتر. ويمكن إعداد بعض الأنظمة لتسجيل خروج المستخدمين بعد فترة معينة في حالة عدم قيام المستخدم بإجراء أية أنشطة. وبدلاً من ذلك، يمكن تنشيط كلمة سر تتطلب من المستخدم إدخال كلمة السر مرة أخرى لتحرير الشاشة (على سبيل المثال في ويندوز 98 وويندوز إن تي).

الوصول الخاص بالوحدات الطرفية: قد يرغب البعض في حظر الوصول على بعض التطبيقات لوحدات طرفية معينة. على سبيل المثال، قد يرغب العميل في إعداد النظام بحيث لا يتم الوصول إلى تطبيق المرتبات إلا من خلال وحدة طرفية موجودة في إدارة الموارد البشرية.

التسجيل

حتى هذه اللحظة، كل عناصر التحكم التي تم ذكرها هي عناصر ذات طبيعة وقائية، أي أنها مصممة لضمان منع الأشخاص غير المعتمدين من الحصول على القدرة للوصول إلى أنظمة الكمبيوتر.

أما الخط التالي من عناصر التحكم فهو يشتمل على القدرة على تحديد محاولات الوصول والأنشطة غير المعتمدة. ويمكن تحقيق ذلك بشكل طبيعي من خلال تسجيل الأحداث في سجل للتدقيق.

وهناك نوعان من سجلات التدقيق التي يشيع استخدامها في أنظمة الكمبيوتر، سجل تدقيق الأمان، وسجل تدقيق العمليات.

ويمكن استخدام سجل تدقيق الأمان لتسجيل معلومات مختلفة حول أنشطة المستخدمين.

وفيما يلي أمثلة لأحداث المستخدمين الأمنية التي يشيع تسجيلها:

الفشل في الوصول: عندما يفشل المستخدمون في الدخول، بعد المحاولة، إلى ملف أو دليل محمي، و
استخدام الأدوات المساعدة والتطبيقات في النظام. ويمكن أن تشتمل التفاصيل التي يتم تسجيلها على التطبيقات التي تم الوصول إليها ومن قام بالوصول ومتى.
ويجب أن يكون المراجع على علم أن تسجيل كل حدث أمني قد يحتاج إلى الكثير من موارد النظام، كما يؤدي إلى التقليل من قدرة النظام. وبالإضافة إلى ذلك، قد يكون قضاء العميل لساعات لمراجعة ملفات السجلات الضخمة أمرًا بعيد الحدوث. يجب أن يحافظ العميل على التوازن بين الأنشطة الهامة التي يتم تسجيلها وأهمية أو حساسية الأنظمة.
ويجب حماية سجلات التدقيق حتى لا يقوم أحد بالكتابة فيها أو حذفها من قبل أي شخص يحاول أن يغطي على ما فعله على النظام.
وعندما يتم كتابة كمية كبيرة من البيانات في ملف تسجيل، قد يستخدم العميل أدوات تقارير استثنائية، حيث تقوم تلك الأدوات بمسح ملفات التسجيل وتمييز تلك الأحداث التي يجب جذب الاهتمام إليها.
والنوع الآخر من سجلات التدقيق هو سجل تدقيق العمليات، وهو يستخدم لتسجيل سلسلة العمليات التي يتم عملها على النظام.

أنواع السياسات التي يجب توفرها لأمن

- سياسات كلمات المرور
- سياسات الدخول
- سياسات إنهاء خدمة موظفي تقنية المعلومات
- سياسات البريد الالكتروني
- سياسات إدارة البيانات
- سياسات الصلاحيات على الأنظمة والتطبيقات
- سياسات اتفاقيات مستوى الخدمة

وغيرها من السياسات العديدة لأمن مركز المعلومات وينبغي تحديث ومراجعة السياسات من فترة لأخرى بانتظام .

الملخ

في هذه الجلسة، قمنا بمناقشة أمن المعلومات والانترنت وعناصر التحكم المادية أو البيئية وعناصر التحكم المنطقية , ولكل نوع من عناصر التحكم ، قمنا بمناقشة أهداف عناصر التحكم ، والمخاطر الناجمة عن ضعف أو غياب تلك العناصر ، بالإضافة إلى إجراءات التحكم.

أساليب الرقابة باستخدام الحاسب

نظرة شاملة على المحاضرة

صممت هذه الجلسة كمقدمة لأساليب الرقابة المدعومة بالحاسب والغرض منها هو تقديم وفهم أدوات CAAT المتاحة للمراقبين في مجال الرقابة المدعومة بالحاسوب وأين ومتى يستخدمونها. سوف نركّز في أول الأمر على أساليب الرقابة المدعومة بالحاسوب (CAATs) المستخدمة في تحليل البيانات وفي نفس الوقت سيتم تقديم بعض المفاهيم المتعلقة بقواعد البيانات وسوف نستخدم برامج ACL لتحليل البيانات.

أهداف التعلم

سيتمكن المشاركون من وصف دور CAATs والأنواع المختلفة المتاحة لتأكيد صلاحية البرامج وتحليل البيانات.كما سيتعرفون أيضا على متى وأين يستخدمون CAATs وطرق النفوذ للبيانات وليكونوا على دراية أيضًا بمفاهيم قاعدة البيانات وقادرين على استخدام ACL لتحليل البيانات.

وظيفـــــــــــة

تمّ في البداية استخدام المعالجة الإلكترونية للبيانات من قبل الهيئات الخاضعة للرقابة ،عن طريق قيام المراقبون بمعالجة نظام تقنية المعلومات كآلة تسجل الأعمال بالكامل (مثل الصندوق الأسود في الطائرة)، ثم إجراء مراقبة بالحاسب. فيما بعد ومع مرور السنين، قام المراقبون (بما في ذلك الأجهزة العليا للرقابة) باستغلال فرصة توفر لدى الجهة الخاضعة للرقابة بيانات في صيغة إلكترونية لكي يقوموا "بالرقابة عن طريق الحاسب" باستخدام CAATs. لقد نتج عن هذا الاتجاه فوائد، ليست فقط على مستوى تنفيذ عمليات الرقابة ولكن أيضًا في مرحلة التخطيط. رغم أن التركيز الأولي لـ CAATs كان في الرقابة المالية ورقابة المطابقة، وتمشيًا مع الطبيعة المتغيرة واهتمام الأجهزة العليا للرقابة ، تزايد استخدام CAATs لتحقيق نتائج جيدة في رقابة الأداء والرقابة التفتيشية.

أنـــــــــــواع

يمكن تقسيم CAATs إلي مجالين منفصلين من العمليات:

- تأكيد صلاحية البرنامج
- تحليل البيانات

- الأساليب الموجهة للبرامج

تركّز CAATs الموجهة للبرامج، على التحقق من صحة مختلف العمليات في البرامج (التي يمكن القيام بها نظريا رغم ندرة ذلك عمليًا) ، ثم أمتد استخدام CAATs إلى الرقابة الكاملة للبرامج , من ناحية أخرى تتجاهل CAATs الموجهة للبيانات البرامج المستخدمة لإنتاج البيانات وتركز حصريًا على تحليل البيانات ولا يعني ذلك بالضرورة أن CAATs الموجه لتحليل البيانات هي تمكّن من إجراء الاختبارات الأساسية والفنية دون سواها مع CAATs الموجة لفحص البرامج الموجودة بالأنظمة بينما تكون رقابة البرنامج عمومًا مفيدة فقط في الرقابة على المطابقة أو في أفضل الظروف في التصديق على القوائم المالية. كما يمكن استخدام تحليل البيانات في رقابة الأداء وأيضًا الرقابة التفتيشية.

في الواقع يمكن أن يستخدم تحليل البيانات غالبًا على نحو فعال جدًا في تقييم الفعالية الحقيقية لعناصر التحكم، بدلاً من الاعتماد على تحليل البرامج (التي هي عنصر واحد فقط من عناصر التحكم بتقنية المعلومات).

- الأساليب الموجهة لتحليل البيانات

يستخدم لـ CAATs كذلك لتحليل بيانات الجهة الخاضعة للرقابة و هو الأسلوب السائد بسبب سهولة استخدامه. يتوفر لتحليل البيانات تشكيلة من برمجيات التدقيق وأدوات لغة SQL ، والتي صممت بصفة عامة للاستخدام في أنظمة الحاسب الشخصي.وتتلاءم هذه الأدوات مع رقابة المطابقة والأداء والرقابة القضائية / التفتيشية بالإضافة إلى الرّقابة المالية.

تشمل الطرق الشائعة لتحليل البيانات من قبل المراجعين ما يلي:

- منطقية البيانات
- كشف الثغرات
- التسلسل
- التجميع
- الترصيف (التقسيم إلى طبقات)
- منجم البيانات
- اختيار العينات
- التقارير الاستثنائية
- فحص السجلات المكررة
- التقادم

المسائل المتعلقة - بتحليل

هناك مخاطر محتملة تنشأ من اعتماد المراقب على نتائج تحليل البيانات لأجل قراراته الخاصة بالرقابة. يجب أن يكون المراقبون على دراية بالمخاطر إذا كانوا يعتمدون حصريًا على تحليل البيانات لنتائج الرقابة أو إضافة CAATs لفحوصات الرقابة غير المثبتة في الحاسب لتقديم سند أو دليل مؤيد. يجب أن يقوم المراقبون بالتحقق من نتائج تحليل البيانات كلها (أو على الأقل عينة منها) عن طريق الاستشهاد بالوثائق الورقية. من المهم جدًا إجراء مراجعة لعناصر التحكم بنظام تقنية المعلومات لتقييم درجة الموثوقية للبيانات التي أُدخلت أو عولجت بواسطة النظام ، كما يجب على المراقب التحقق من تكامل البيانات المنزلة عن طريق التوفيق مع عنصر تحكم أو ملخص التجميعات.

يجب أن يتفهم المراقبون نظام تقنية المعلومات للجهة الخاضعة للرقابة، والأكثر من ذلك أهمية هو فهم البيانات. و سوف يعتمد ذلك على مدى التدريب الذي تلقوه ومدى الخبرة في استخدام هذه الأدوات.

اعتبـــارات – اســـتخدام CAATs لتحليـــل

تعتبر أهمية وحساسية التطبيقات المستخدمة من قبل الجهة الخاضعة للرقابة ، والتي تعتمد عليها الأعمال التجارية الجوهرية، من أحد أسباب استخدام تحليل البرنامج. وقد يكون هناك سبب آخر

وهو أن تحليل البيانات بمفرده لا يمكّن الاعتماد عليه لتقديم تأكيد فيما يتعلق بكفاية وفعالية عناصر التحكم.

اعتبـــارات – اســـتخدام CAATs لتحليـــل

بالرغم من ان استخدام اساليب الرقابه المدعومه بالحاسب له فوائد عديدة للأجهزة العليا للرقابة، فإنه يحبذ إجراء تحليل التكلفة مقارنة بالعائد لاستخدام CAATs في بيئة رقابة محددة. غالبا ما قد يكون هذا التحليل في شكل تقييم نوعي، وبرغم ذلك فهو يساعد على خلق اتجاه لتوقعات أكثر واقعية للعوائد والتكاليف المستخدمة.

وفي ما يلي بعض العوامل الهامة، التي ترجح استخدام CAATs في العمل الرقابي :

- الاستخدام المتكرر لـ CAATs في المهمات الرقابية المستقبلية
- منح أولوية هامة للمجالات ذات مخاطر الرقابة العالية
- أساليب الرقابة المماثلة التي لا تعتمد على الحاسب تكون غير عملية أو عالية التكاليف.

خيـــارات – الوصـــول

بصفة عامة، يوجد طريقتين يمكن للمراقب أن يستخدم فيهما CAATs لتحليل بيانات العميل:

- تشغيل CAAT على نظام تقنية المعلومات الخاص بالجهة الخاضعة للرقابة، سواء مباشرة من حاسب شخصي أو شاشة طرفية أو عن طريق توصيل حاسب المراقب بشبكة الجهة الخاضعة للرقابة
- تنزيل البيانات على نظام تقنية المعلومات الخاص بالمراقب أو جهاز الرقابة وتشغيل CAAT من حاسبه.

المسائل المتعلقة – بتشغيل CAATs على نظام الجهة الخاضعة للرقابة

قد يكون تثبيت برنامج CAATs على نظام تقنية المعلومات الخاص بالجهة الخاضعة للرقابة غير عملي بسبب اختلافات البرامج الفنية الخ. عادة يستخدم المراقب الأدوات الموجودة في نظام الجهة الخاضعة للرقابة بدلاً من تثبيت برنامج CAATs الخاص بجهاز الرقابة ، في هذه الحالة سيحتاج المراقب للتعرّف على الأدوات المتاحة في تشكيلة متنوعة وكبيرة في محيط تقنية معلومات العميل. علاوة على ذلك، يحمل تشغيل CAATs على نظام الجهة الخاضعة للرقابة المخاطر المحتملة لاضطرابات أنظمة الجهة الخاضعة للرقابة، مع تبعات محتملة لكل من الأداء وتكامل البيانات (هناك احتمال أن تتغير أو تُحذف بيانات الجهة الخاضعة للرقابة بدون قصد) تظهر هذه المشكلة أيضًا في الطريقة التي يستخدم فيها ارتباطية البيانات بين حاسب المُراجع ونظام تقنية المعلومات الخاص بالجهة الخاضعة للرقابة.

المســائل المتعلقــة – بتنزيــل

العامل الهام في التنزيل الناجح للبيانات هو تأكيد تكامل البيانات المنزلة، والذي غيابه يجعل كامل عملية CAATs غير موثوقية. هناك عدة مسائل متصلة بتكامل البيانات مثل:

- يجب الحصول بلا استثناء على عدد سجلات البيانات في كل ملف من الجهة الخاضعة للرقابة ومن المستحسن أيضًا إما تجميع إجماليات التحكم لكل ملف من الجهة الخاضعة

للرقابة و/أو الحصول على وثائق مطبوعة تمثل أرقام إجمالية للبيانات التي تحتويها هذه الملفات (مثل ملخصات التقارير المالية).

- يتم حينئذ إجراء تأكيد تكامل البيانات المنزلة باستخدام أداة CAAT لإعادة حساب عدد التسجيلات وإجماليات البيانات التي تم جلبها إلى داخل برنامج CAAT، ومقارنتها بالأرقام التي قدمتها الجهة الخاضعة للرقابة.
- يجب الاحتفاظ بالبيانات المستلمة في صيغتها الأصلية من الجهة الخاضعة للرقابة سليمة ولا تُمس. في حالة الطلب من المراقب إعادة البيانات الأصلية إلى الجهة الخاضعة للرقابة، يجب أن يتم الاحتفاظ بنسخة من البيانات بدون مس على نظام تقنية معلومات المراقب.

اعتبـــارات – اختيـــار

يجب الربط بصفة واضحة بين أسلوب الرقابة المدعوم بالحاسوب وهدف (أهداف) الرقابة وتجنب إغواء الحصول على بيانات زائدة أو غير ذات صلة. لكن، قد يكون من الأسهل أحيانًا تنزيل جميع جداول أو حقول الجداول الموجودة في قواعد بيانات الجهة الخاضعة لرقابة حيث قد يتطلب الأسلوب الأفضل انتقاءًا وقت وموارد أكثر.

عمومًا، فإن المراقب مطالب بانتهاج أسلوب أكثر انتقائية في اختيار البيانات عند ما يتعلق الأمر بالرقابة المالية ورقابة المطابقة، حيث أن المراقب يتجه إلى "تعريف" البيانات من أجل إبراز النزعات أثناء القيام برقابة الأداء أو الرقابة التفتيشية..

يجب على المراقب، بقدر الإمكان، اختيار بيانات في الشكل الأقرب للمعاملات الأصلية (الصفقة أو الملفات الأولية / الجداول الرئيسية بدلاً من الملخصات أو الملفات / الجداول الثانوية) وذلك لكي تبقى معالجة البيانات في أقل حد.

لكي يتم اختيار البيانات المطلوبة، يحتاج المراقب للتفهم الكامل للبيانات المتاحة في نظام تقنية المعلومات الخاص بالجهة الخاضعة للرقابة والمتعلقة بالأعمال التجارية بدلا من منظور فني.

يمكن تحقيق هذا التفهم من مصدرين، وثائق النظام ذات الصلة بهيكل البيانات والمناقشة مع العاملين في الجهة الخاضعة للرقابة (وخاصة إدارة تقنية المعلومات و"صاحب النظام").

والمصدر الآخر هو مراجعات النظام السابق من قبل المراقبين.

مفاهيم قواعد

أدوات تحليل البيانات

يمكن تصنيف ذلك في فئات كالآتي:

- **برامج رقابة مخصصة:** وهذه عبارة عن حزم برامج جاهزة أنشئت خصيصًا للمراجعين لاستخدامها في تنوع كبير من البيئات الفنية. الحزمتان الرئيسيتان للأغراض العامة هما IDEA (استخراج وتحليل البيانات التفاعلي) وIDEA (لغة أمر الرقابة)
- **لغة الاستعلام المدمجة والأدوات المبنية على–لغة الاستعلام المدمجة**SQL هي لغة تستخدم على نطاق كبير لتحديد ومعالجة البيانات المخزنة في نظم الإدارة بقاعدة بيانات علائقية (RDBMS).
- **Microsoft Access:** Microsoft Access هو تطبيق قاعدة بيانات علائقية لسطح المكتب (desktop) يشكل جزء من مجموعة Microsoft's Office Professional لتطبيقات

الأتمتة المكتبية. إضافة لاستخدامه العادي لتطبيقات قاعدة البيانات الصغرى، يمكن لـ إمداد المراجع بأداة استعلام سهلة الاستعمال وفي المتناول.

- **أدوات أخرى:** تطبيقات Spreadsheets مثل إكسيل أو لوتس 123، يمكن أن تكون مفيدة بشكل غير متوقع لقواعد البيانات الصغيرة. يدعم ميكروسوفت إكسيل 2000 (MS Excel 2000) حتى 65 ألف تسجيل / صف ويمكن لإكسيل اكس بي (Excel XP) أن يتسع لأكثر من ذلك بكثير. رغم أن الاستعلام رئيسي نسبيًا، إلا أن إكسيل يقدم مزايا ممتازة للرسوم والمخططات. من الممكن في الغالب تلخيص البيانات المستخرجة باستخدام Access وتصديرها ككشف spreadsheet للعرض كجداول بيانية ومخططات.

مفهوم البيانات

البيانات هي المفردات أو المادة الخام المخزنة في نظام الحاسب في صيغة إلكترونية لا يمكن فهمها، في معظم الحالات، بمفردها. في حين المعلومات هي نفس البيانات في صيغة معالجة تكون ذات معنى للمستخدمين.

قواعـــــد البيانـــــات العلائقيـــــة

إن ملف قاعدة البيانات هو مجموعة من "الكائنات" objects– جداول tables،الاستعلام queries or views، تقاريرreports، إطارات forms. قاعدة البيانات العلائقية RDBMS هي مجموعة من الجداول المرتبطة ببعضها البعض عن طريق علاقات. تتضمن قواعد البيانات العلائقية على بيانات وتركيب هذه البيانات من حيث الأسماء، والأنواع والأحجام وهي مرتبطة ببعضها لتشكيل تكاملية للبيانات. ولها ميزة أخرى مثل الأمن والتحكم، ومدير قاعدة البيانات (DBA) يمكنه إعداد عناصر معينة للتحكم الأمني(الضوابط) على الجداول والسجلات والحقول.
أغلب قواعد البيانات العلائقية إن لم يكن كلها، تستخدم لغة الاستعلام المسماة SQL (Structred Quercy language) لغة الاستعلام المدمجة والتي تستخدم في نطاق واسع لتحديد ومعالجة البيانات المخزنة في قاعدة البيانات العلائقية. إن تعريف البيانات هام بالنسبة لمطوري الأنظمة، ومعالجة البيانات ضرورية للمستخدمين الذين يمكنهم أداء وظائف مثل: العرض / الإدخال / التحديث / الحذف. المثال البسيط على بيان لغة الاستعلام المدمجة هو " **اختر SELECT** اسم NAME ، تاريخ الميلاد DOB، تاريخ الالتحاق DOJ، المكتب Office_ المكانLocation **من FROM الموظف** EMP_ الصفحة الرئيسية MASTER **أينما WHERE تكون الإدارة** Management **صحيحة TRUE".** بعض المنتجات الشائعة لقاعدة البيانات العلائقية هي OrIDEAe، IBM DB2، Microsoft SQL Server، Sybase SQL، Informix، Ingressولكن أكثر المنتجات استخداما على نطاق واسع هي OrIDEAe وMS-SQL Server

المفاهيم العلائقية

المفتاح الرئيسي Primary Key : هو عبارة عن حقل وحيد في الجدول ولا يمكن أن يتكرر أو تكون قيمته null .(فراغ)

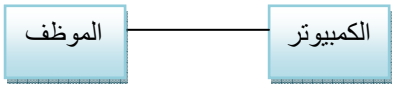
العلاقاتRelationships: هناك أربع أنواع من العلاقات هي :

. One to one , One to many , many to one , many to many

One to one :

تعرف هذه العلاقة بعلاقة واحد إلى واحد ويرمز لها بالرمز 1 1 .

ومثال على هذه العلاقة الموظف بالكمبيوتر ←



الموظف الواحد يصرف له كمبيوتر واحد

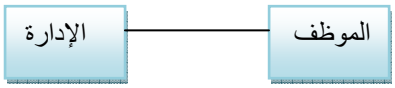
الكمبيوتر الواحد يصرف لموظف واحد

ويتم وضع المفتاح الثانوي في الجدول المناسب.

One to many :

تعرف هذه العلاقة بعلاقة واحد إلى أكثر ويرمز لها بالرمز 1 M

ومثال على هذه العلاقة علاقة الموظف وعمله في الإدارة ←



الإدارة الواحدة يعمل فيها أكثر من موظف

أكثر من موظف يعمل في إدارة واحدة

ويكون المفتاح الثانوي موجود في جهة M

many to one :

تعرف هذه العلاقة بعلاقة أكثر إلى واحد ويرمز لها

بالرمز M 1 ←

مثال على هذه العلاقة : علاقة المريض وعلاجه مع الدكتور في عيادة فرديّة

M 1

أكثر من مريض يتعالج عند دكتور واحد

الدكتور الواحد يعالج أكثر من مريض

ويكون المفتاح الثانوي موجود في جهة M.

many to many :

وتعرف هذه العلاقة أكثر إلى أكثر ويرمز لها بالرمز M M

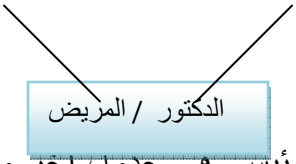
وهذه العلاقة تكون جدول ثالث يربط الجدولين المراد ربطهما. ←

ومثال على ذلك علاقة المريض مع الدكتور في حالة المستشفى

M M

أكثر من مريض يتعالج عند أكثر من دكتور

أكثر من دكتور يعالج أكثر من مريض



ويحتوي جدول الدكتور / المريض على مفتاحين ثانويين.

المفتاح الثانوي Foreign Key: هو عبارة عن مفتاح رئيسي في جدول آخر ولكنه ليس مفتاح رئيسي بمفرده في هذا الجدول بالذات.

تركيب (بنية) قاعدة البيانات Data

يجب عند محاولة المُراجع تنزيل بيانات أن يسأل عن تركيب قاعدة البيانات التي تحتوي على قائمة بجميع الجداول (الكائنات) وتخطيط السجل لكل جدول. يحتوي مخطط السجل على قائمة بجميع الحقول وخصائصها مثل أسمائها، وأوصافها وأنواعها وأحجامها. يجب أن تحتوي أيضًا على المفاتيح الرئيسية والعلاقات.

جلب ملف إلى لغة أوامر الرقابة IDEA**:**

قبل تحليل البيانات باستخدام برنامج لغة أوامر الرقابة IDEA، هناك أمور معينة يجب أن يعيها المراجع.

تنزيل الملف Downloading file : هناك وسائل عديدة يمكن تنزيل الملف بها، هذه الوسائل تشمل القرص المرن والقرص المدمج والشرائط والبريد الإلكتروني ووسائل الاتصال أو ارتباط بالشبكة. ارتباط الشبكة يكون أصعب في الإعداد للمرة الأولى. لكن، لاستخدام علائقية قاعدة البيانات المفتوحة (ODBC) في الشبكة المحلية، يحتاج المراجعين إلى صلاحية لاستخدام قاعدة البيانات من الجهات الخاضعة للرقابة التي في معظم الوقت ستعارض إعطاء هذه الصلاحيات. إن هذه الطريقة أثبتت أنها فعالة وسريعة وخاصة لتنزيل البيانات الكبيرة جدًا.

هيئة الملف File Format: هناك عدة هيئات للملفات كالآتي: **ملفات ذات طول ثابت** : الملفات ذات الطول الثابت تحتوي على سجلات لها نفس الطول ولا يوجد فواصل تعريفيّة أو تعريف ذاتي لطول البيانات التي سوف تكون في السجل ويجب أن يعرف طول السجل في هذه الحالة. **وملفات محددة** : الملفات المحددة هي طريقة من طرق استيراد البيانات ووضع البيانات على شكل صفوف وأعمدة كالجدول وتعتبر ملف نصي ويفصل بين السجلات بالطرق التالية (فراغ ، فاصلة، نقطة، وكوما) **ملفات تقرير، ملفات ذات طول متغير**: الملفات ذات الطول المتغير تستخدم طول ملف معروف مسبقا تحتوي على طول السجل في الملف وكل سجل يحتوي على حقل يحدد طول السجل والملفات المتغيرة تستخدم فاصل أو محدد لتعريف نهايات كل سجل. ويمكن أن تكون MS-Excel أو MS-Access. بينما عند استخدام علائقية قاعدة البيانات المفتوحة لا يهم تنسيق الملف.

تعديل الملف File Modification: عند تنزيل البيانات قد تتغير أو يحصل لها تلف أو إضافات رموز أخرى. ولذا، على المراجعين أن يكونوا على علم بهذه المواقف ويجهزوا أنفسهم بالأدوات القادرة على تعديل البيانات إلى حالتها الأصلية وحذف الرموز التي أضيفت.

الوثائق Documentation : هذا هو أهم جزء من عملية تنزيل وتحليل البيانات. يجب أن يتضمن التوثيق نوع الاستفسارات المستخدمة، ومتى وأية بيانات تم تنزيلها وماذا كانت نتائج الاستعلامات والتقارير التي نتجت. يجب تخزين الوثائق في صيغة إلكترونية وورقية.

الملـــخ

تناقشنا في هذه الجلسة التدريبية حول أساليب الرقابة المدعومة بالحاسب (CAATs) وكذلك وظائف وأنماط (CAATs) المستخدمة بواسطة المراجعين. وتناولت هذه الجلسة أيضًا استخدام CAATs لتحليل البيانات والأمور والاعتبارات التي صادفت المراجعين. تداولت الجلسة طرق الوصول للبيانات وانتقائها وتنزيلها. وأدوات تحليل البيانات المتاحة للمراجعين لاستخدامها مثل برامج الرقابة المعممة.

لقد ذكرت مفاهيم قاعدة البيانات وكذا قاعدة البيانات العلائقية على نطاق واسع في هذه الجلسة التدريبية. ناقشت الجلسة خصائص قاعدة البيانات العلائقية وتفرد علاقاتها ما بين الجداول والحقول.

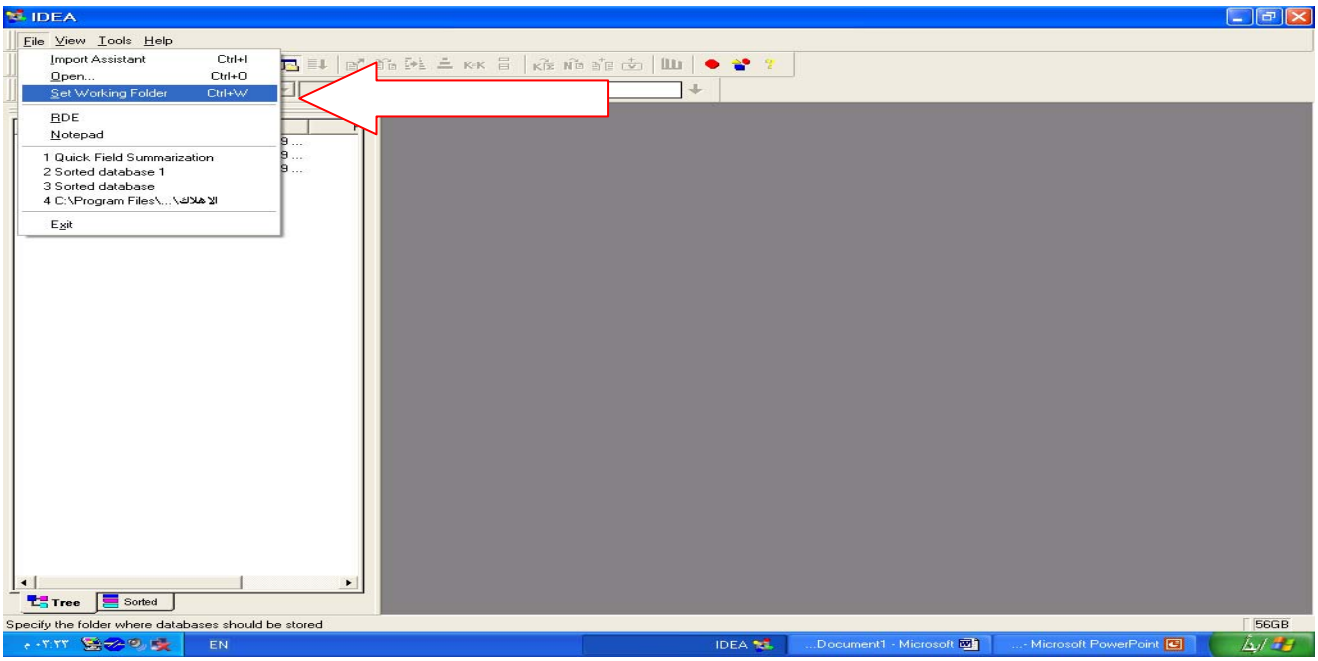
تحليل البيانات هو أحد الأجزاء الرئيسية في عمل أي مراجع في بيئة مجهزة بالحاسبات. ولذلك يجب أن يكون المراجع على علم بتنسيق الملفات وبنية البيانات لكي يجري التحليل باستخدام لغة أوامر الرقابة IDEA. بعد عمل كل ما ذُكر بعاليه ، يجب أن يوثق المراجعين جميع أعمالهم من أجل الاستخدام في المستقبل.

الأوامر المهمة المستخدمة في برنامج

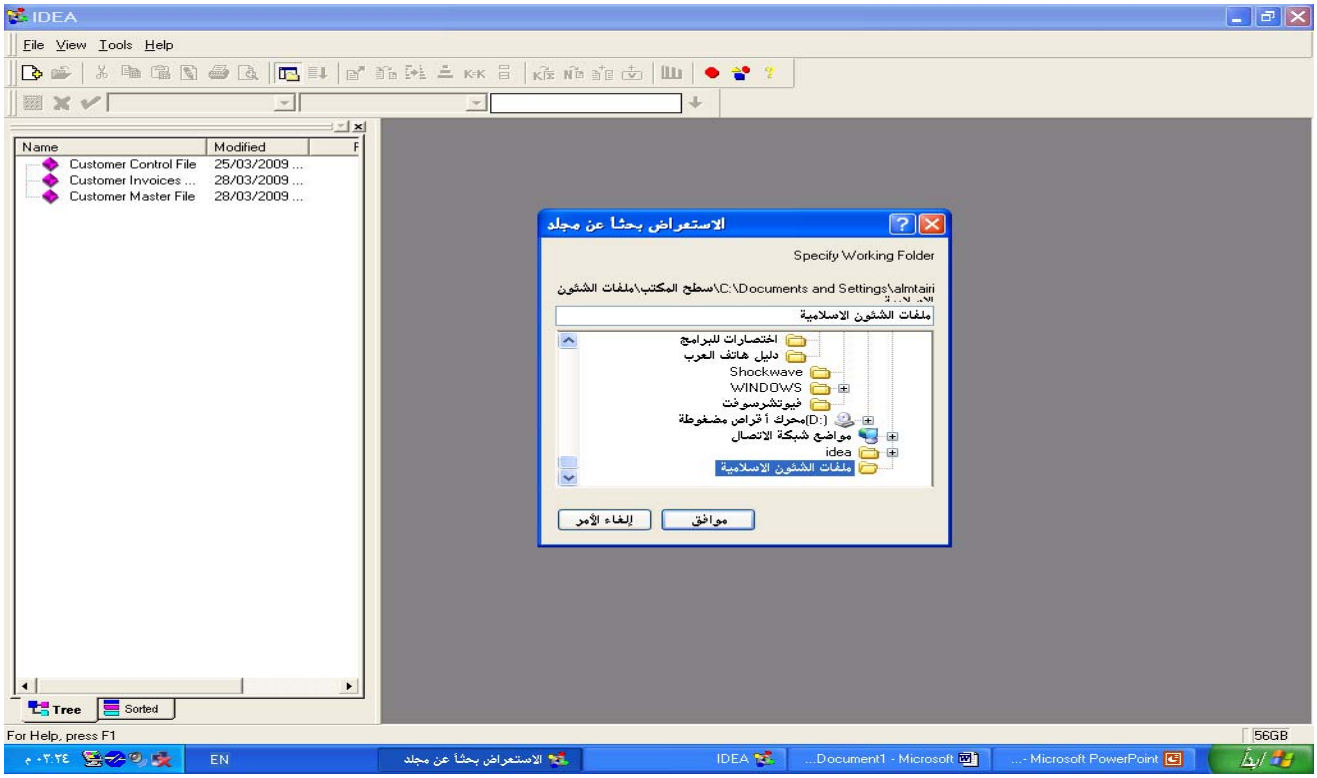
اسم الأمر	*استخداماته*
Set working folder	لتحديد الملف الذي سيحفظ عليه المشروع
Import Assistant	لاستيراد الملفات لبرنامج التحليل
Gap Detection	فحص الثغرات
Numeric Stratification	التصنيف الرقمي
Character Stratification	التصنيف الحرفي
Date Stratification	التصنيف التاريخي
Key Field Stratification	التصنيف بالحقول الرئيسية
Random Numbers	العينات العشوائية للأرقام
MUS	العينات النقدية
Charts	الرسوم البيانية
Control Total	إجراء عملية الجمع للحقول
SORT	إجراء عملية الفرز من الأكبر إلى الأصغر
FIELD STATISTICS	معرفة أعلى واقل قيمة والمتوسط الحسابي
Extractions	استخلاص البيانات
Sampling, Random	العينات الإحصائية العشوائية
join database	ربط الملفات ببعضها البعض
append database	إضافة ملفات متشابهة مع بعضها
GAP	اكتشاف الفجوات
Age	مقارنة بين تاريخين
Val(fieldname)	تحويل الرقم الحرفي إلى رقم حقيقي
Export	تصدير البيانات إلى صيغ أخرى مثل الإكسل

تطبيق رقم

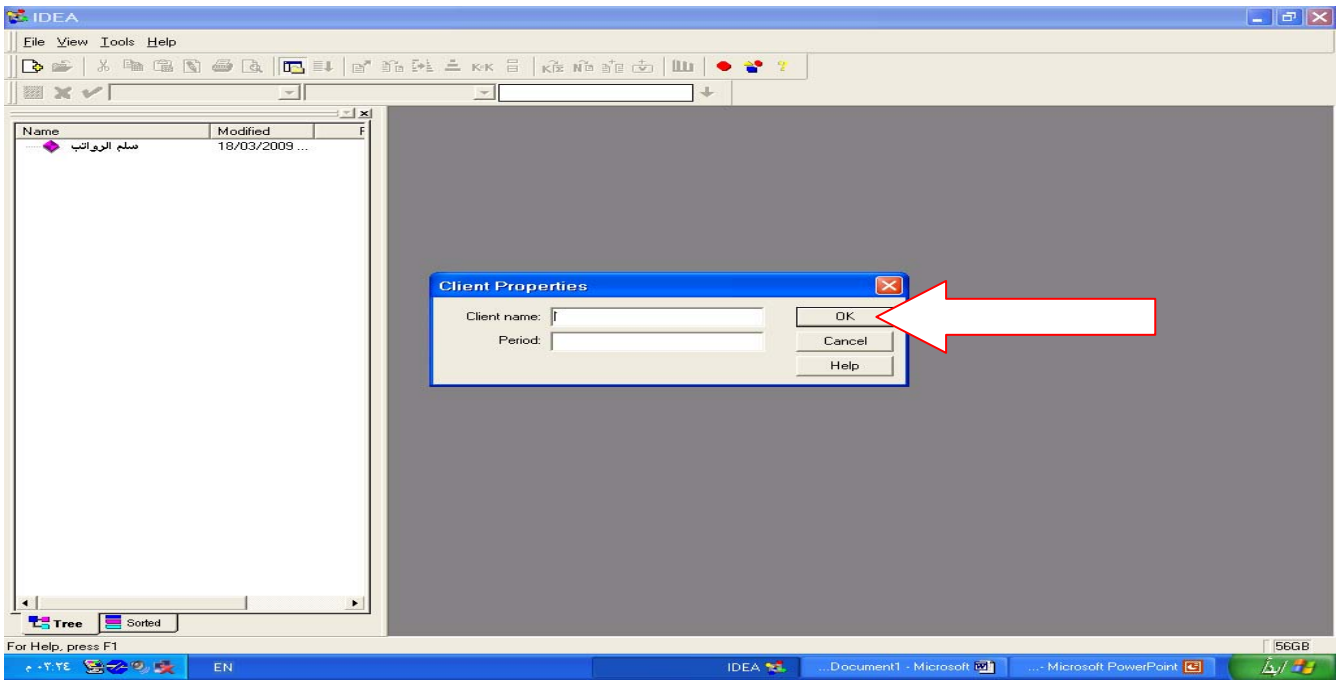
في البداية نقوم بفتح مجلد جديد على سطح المكتب أو المستندات ونسميه بـأي اسم ثم نفتح برنـامج آيديا ونقوم باختيار File – ثم الأمر Set Working Folder



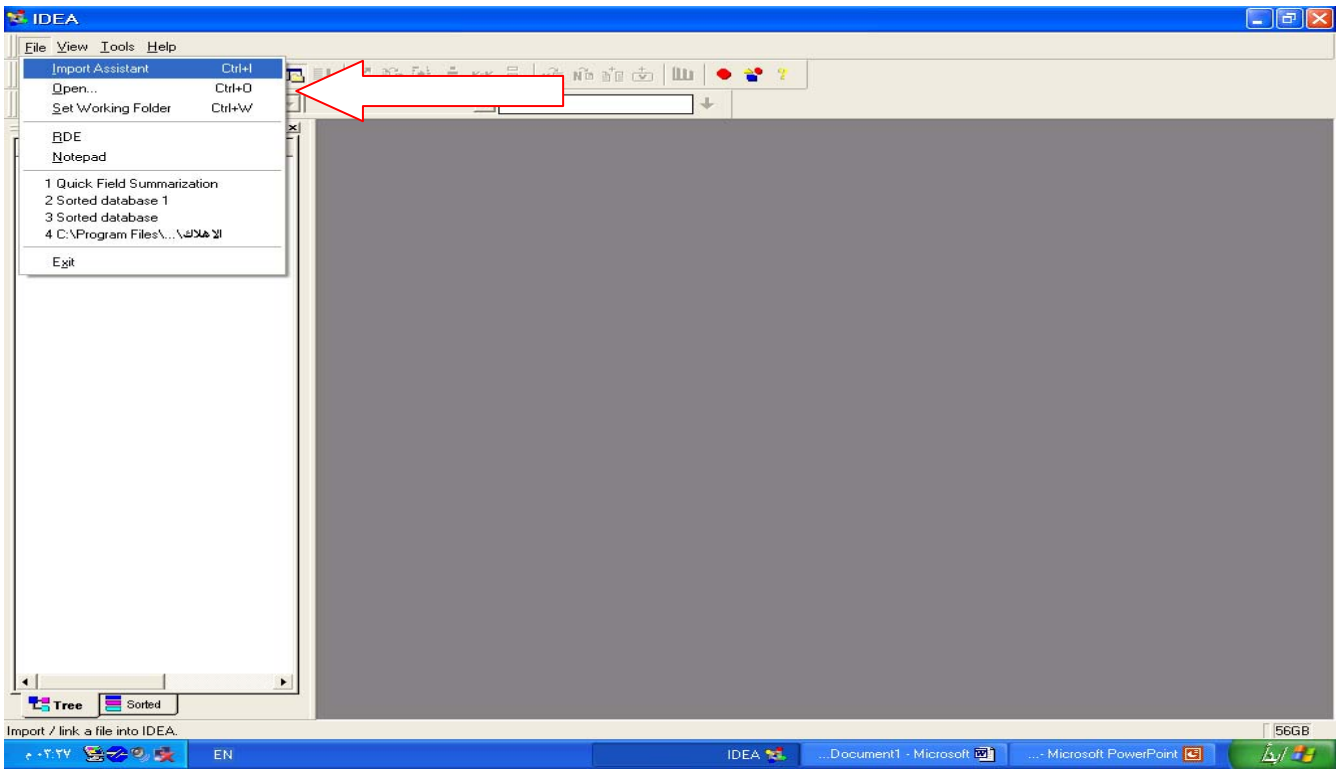
ثم نقوم باختيار الملف الذي تم إنشاءه مسبقا على سطح المكتب ونضغط موافق



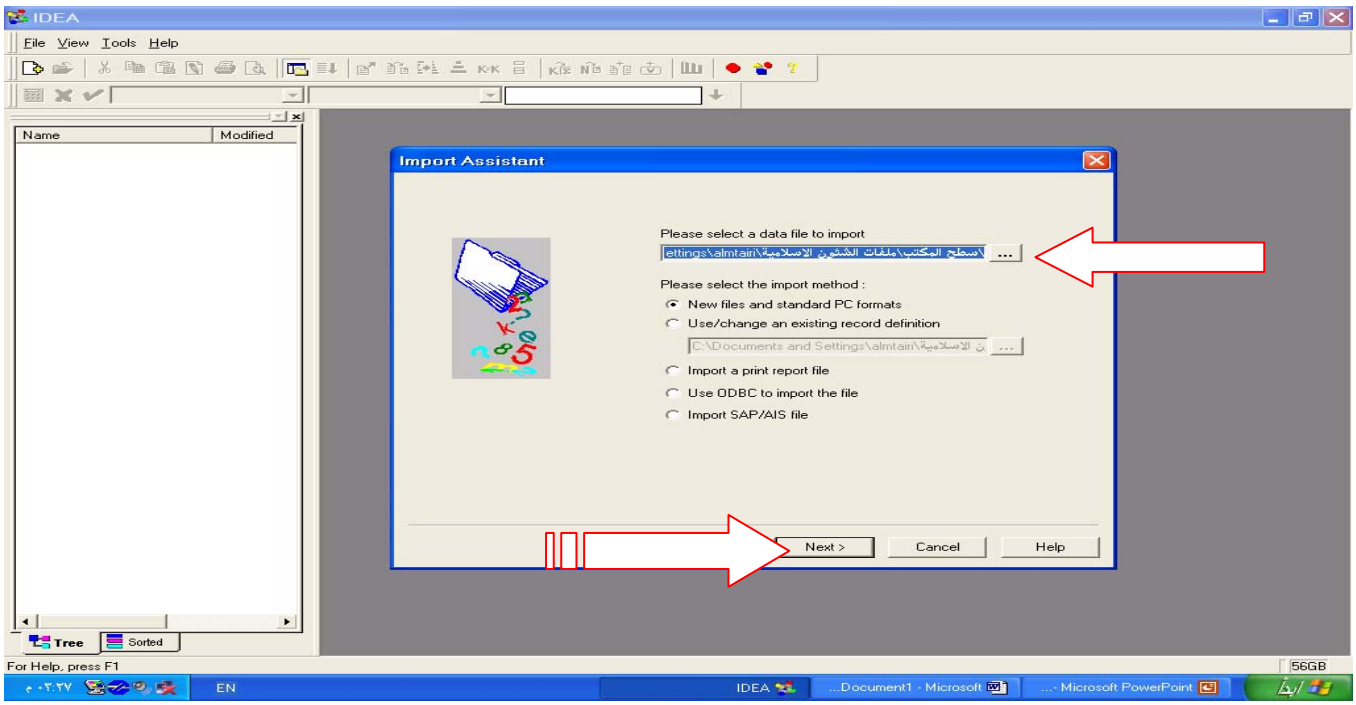
بعد ذلك نقوم بكتابة اسم المشروع والفترة الزمنية ... وهذه الخطوة اختيارية يمكن تجاهلها بالضغط على OK



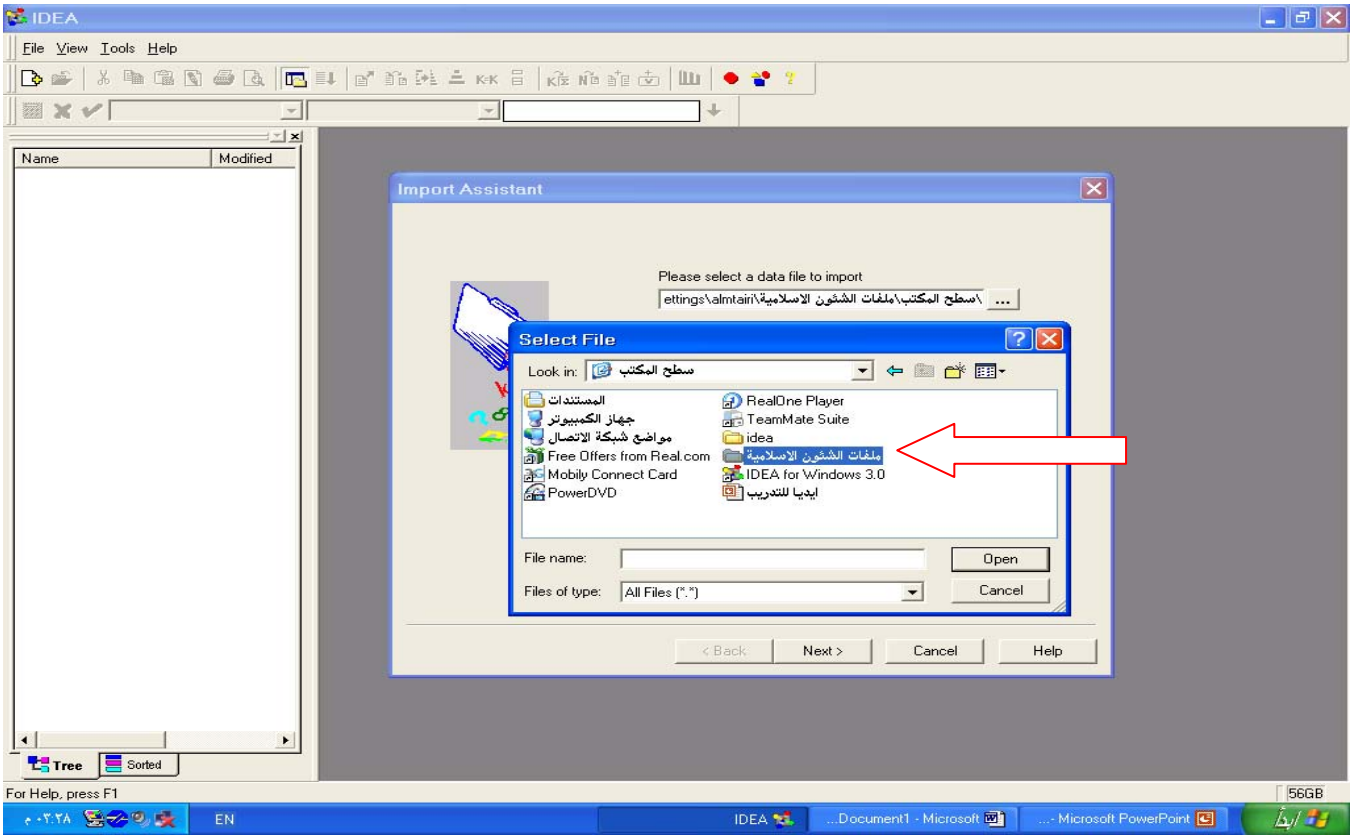
بعد ذلك يتم اختيار الأمر Import Assistant من القائمة File لاستيراد الملف المطلوب



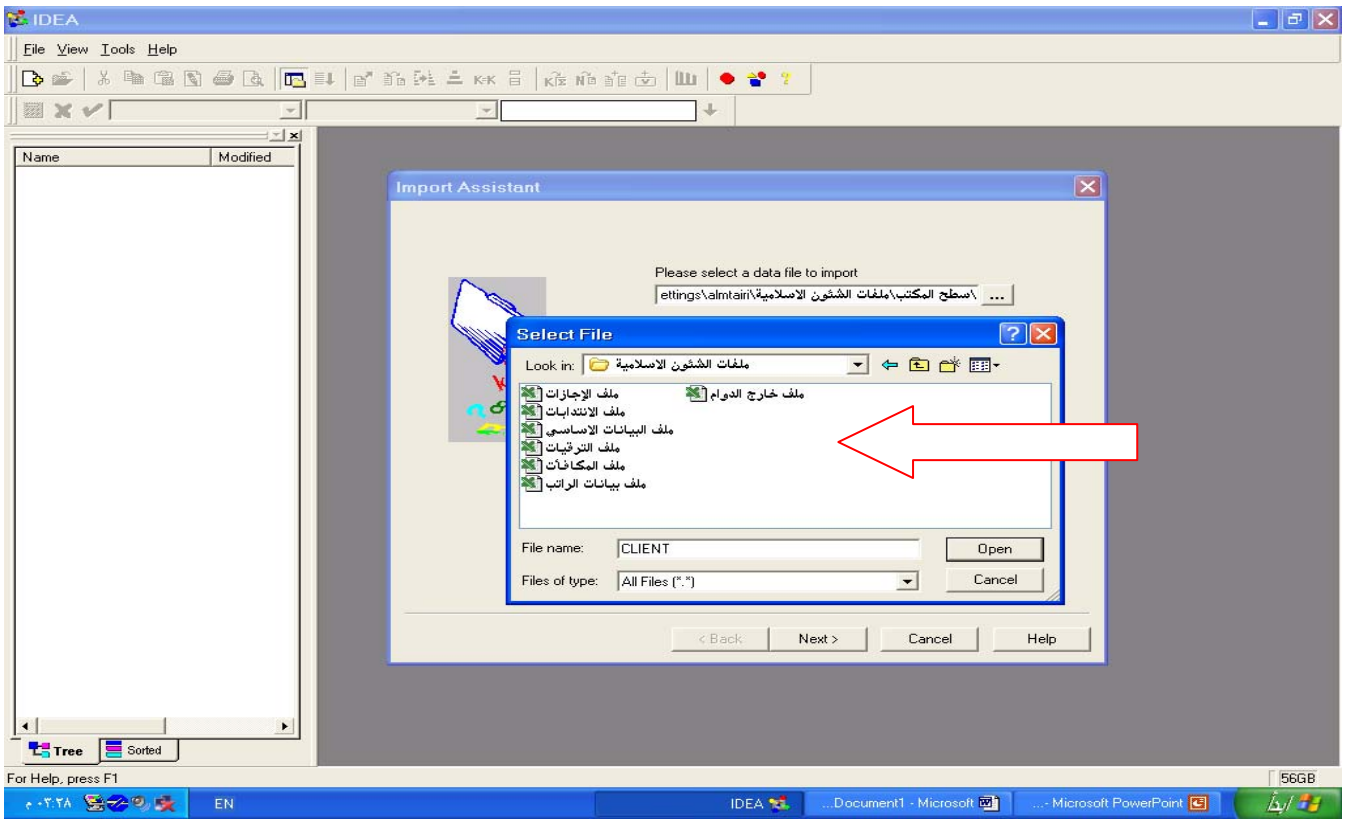
بعد ذلك نقوم بالضغط على المربع الموضح أدناه لتحديد مكان وجود الملف المطلوب ثم نضغط التالي .



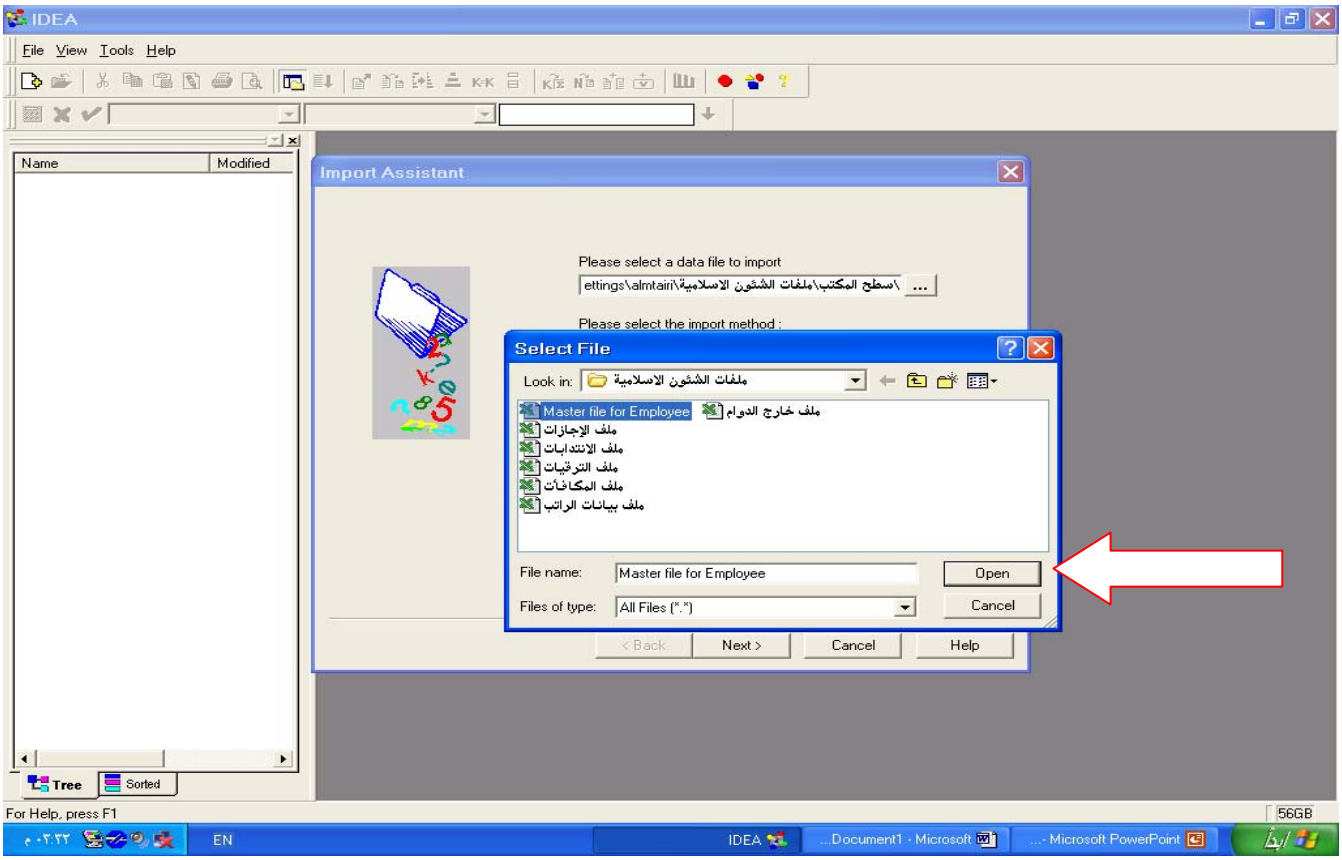
بعد ذلك يتم اختيار الملف كما هو موضح سواء كان في سطح المكتب أو المستندات



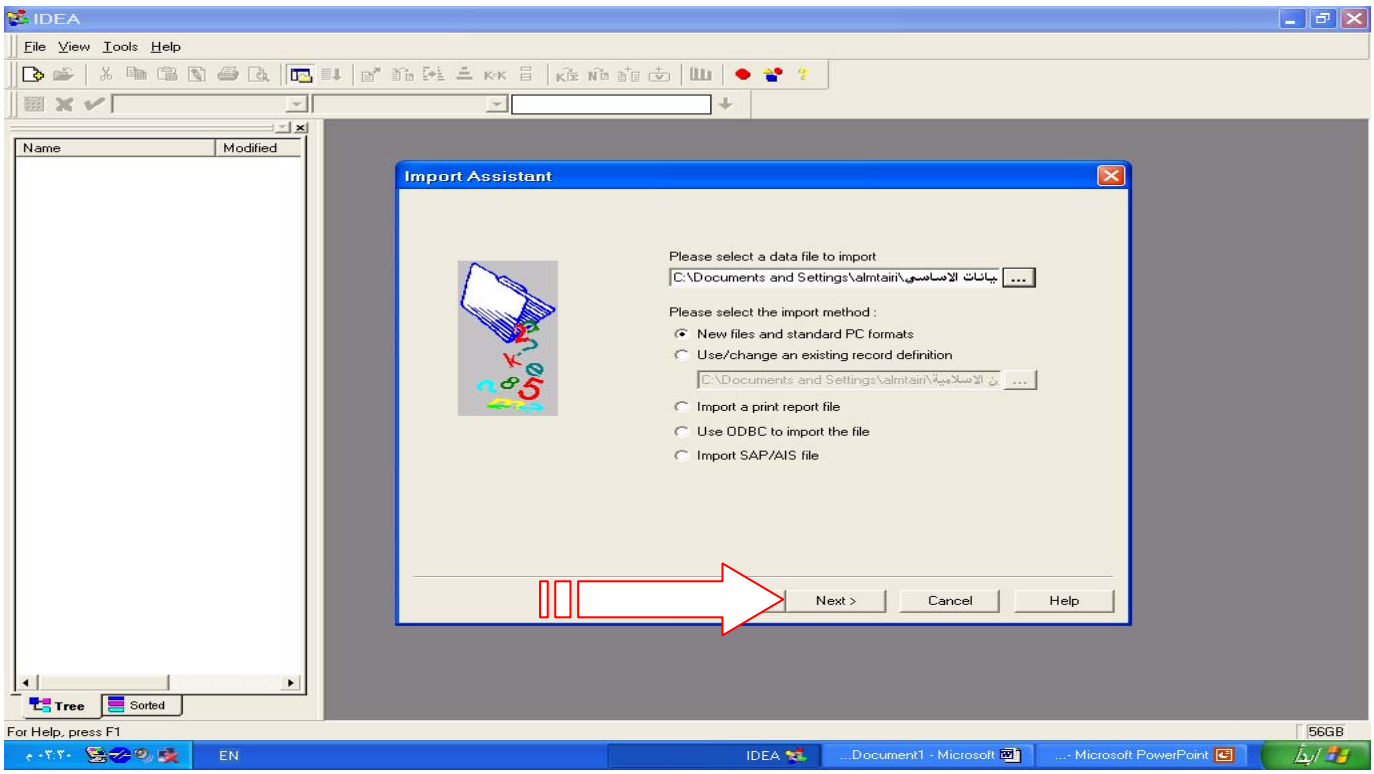
بعد ذلك يتم اختيار الملف المطلوب استيراده .



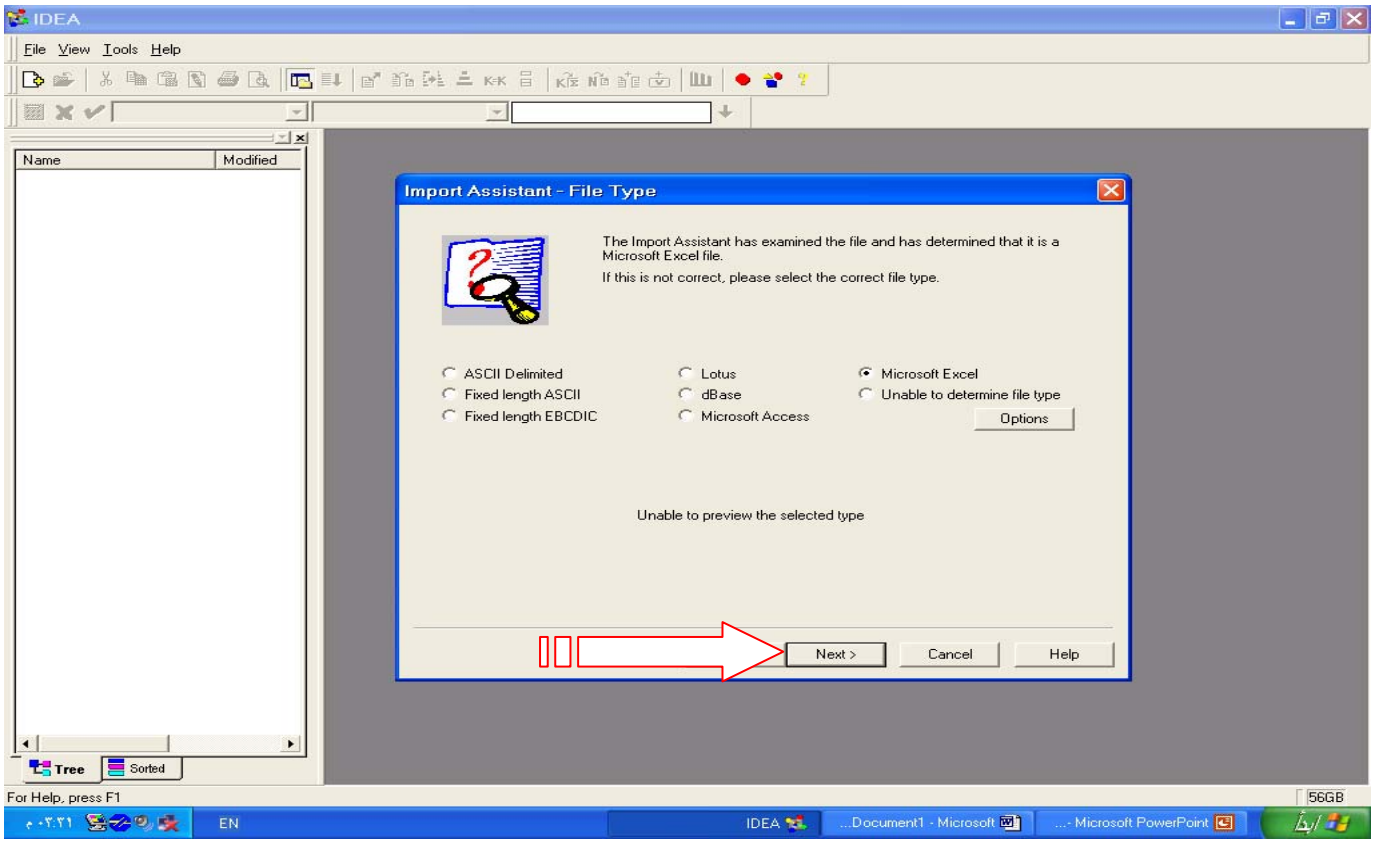
بعد ذلك يتم اختيار الملف ونضغط على الأمر Open



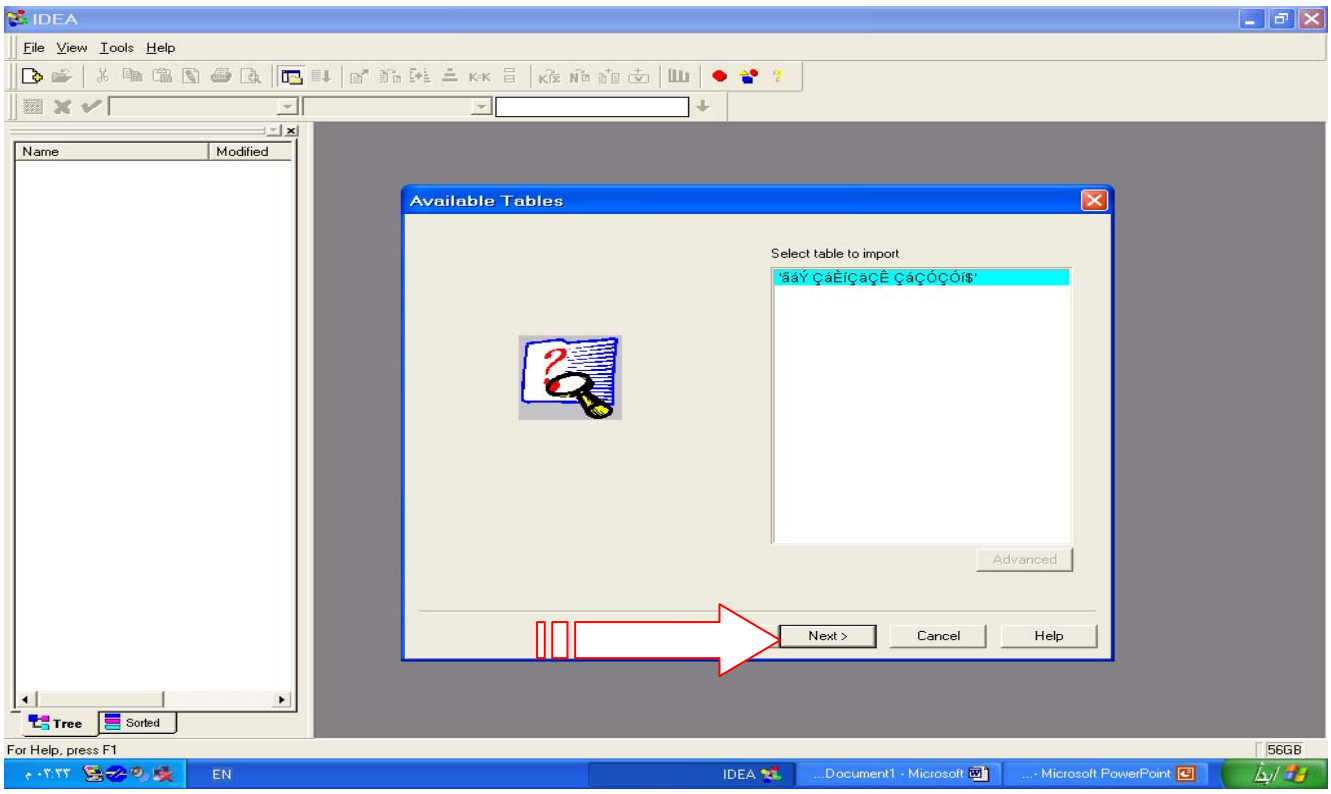
ثم نضغط التالي كما هو موضح أدناه .



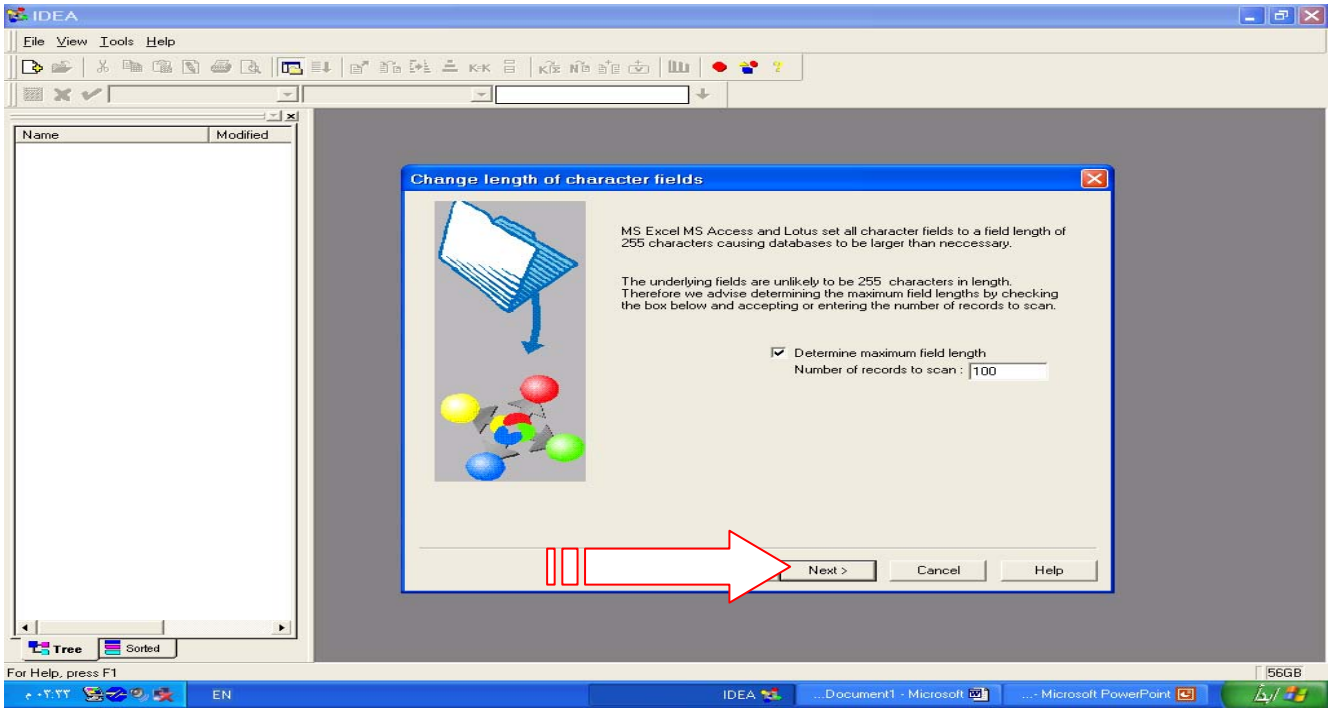
بعد ذلك سوف تظهر الشاشة التالية ومحدد بها نوع الملف الذي سيتم استيراده ونضغط التالي .



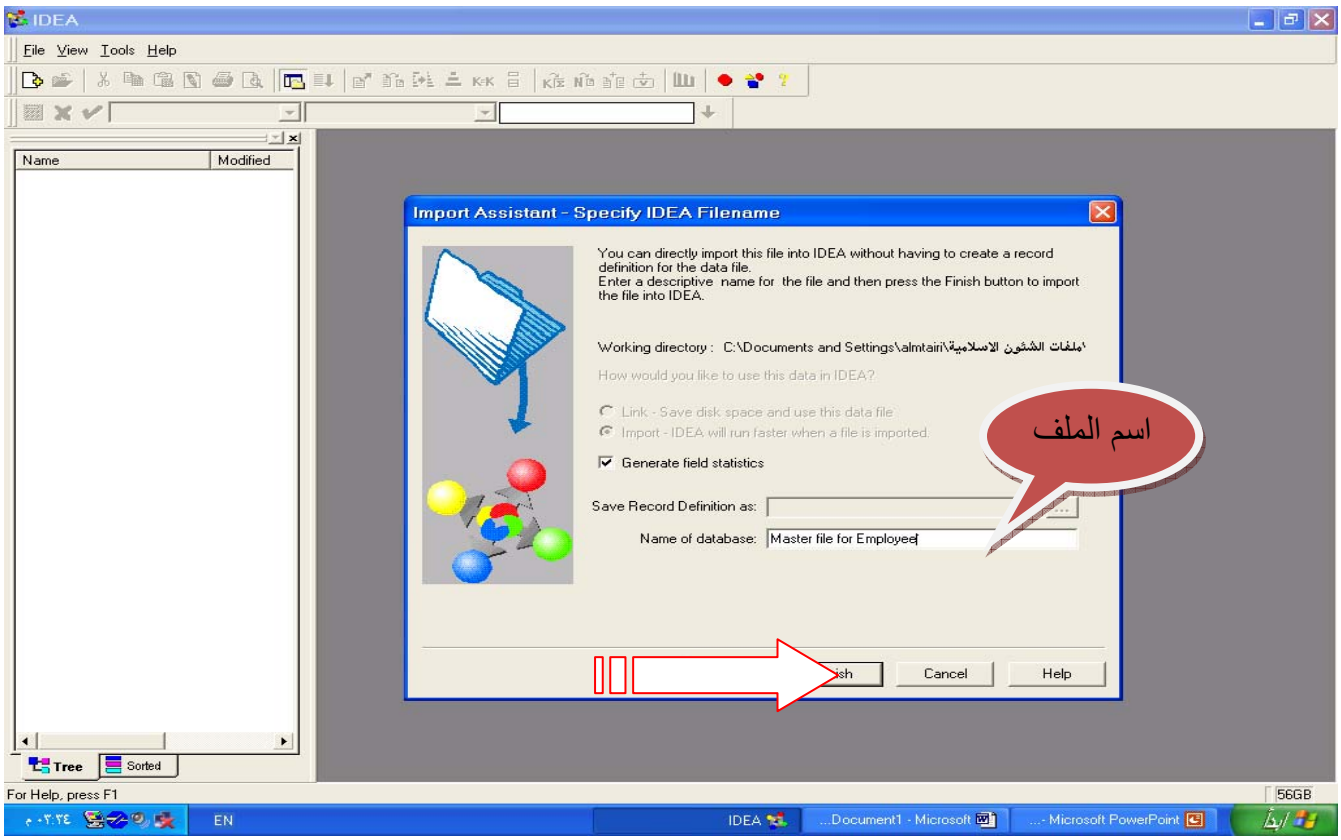
ثم نضغط التالي كما هو موضح .



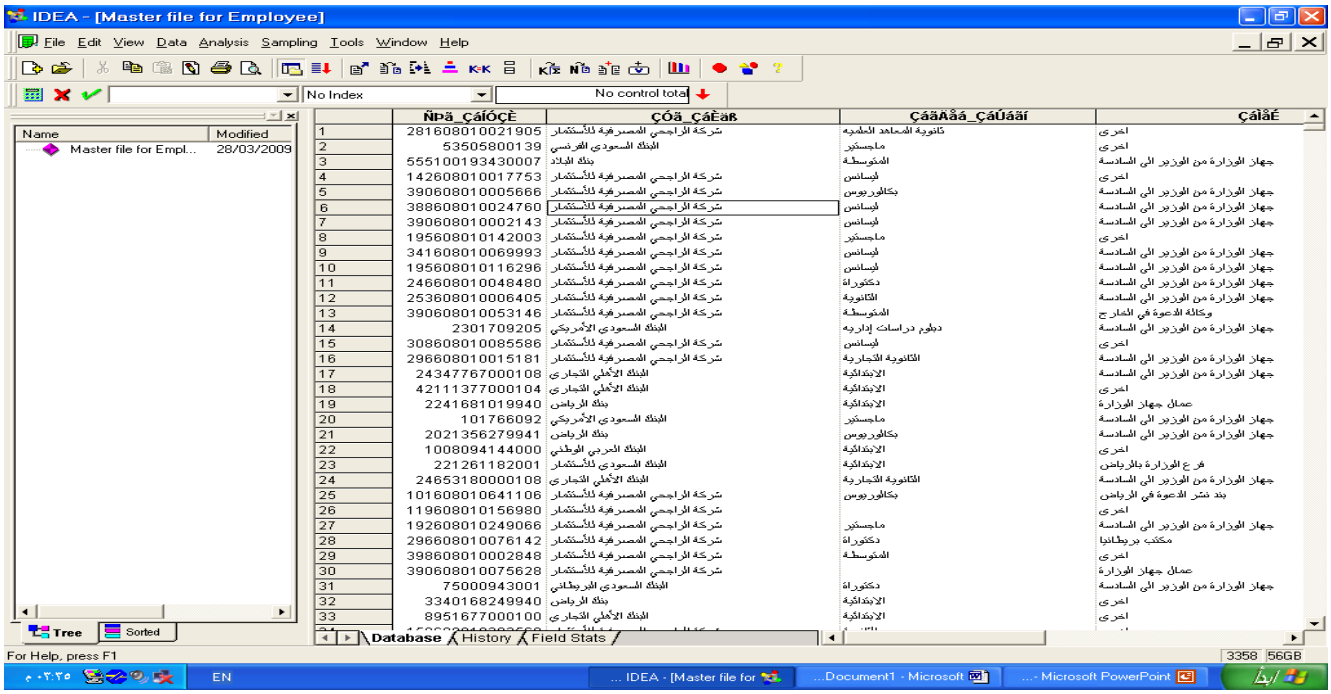
ثم نضغط التالي ...



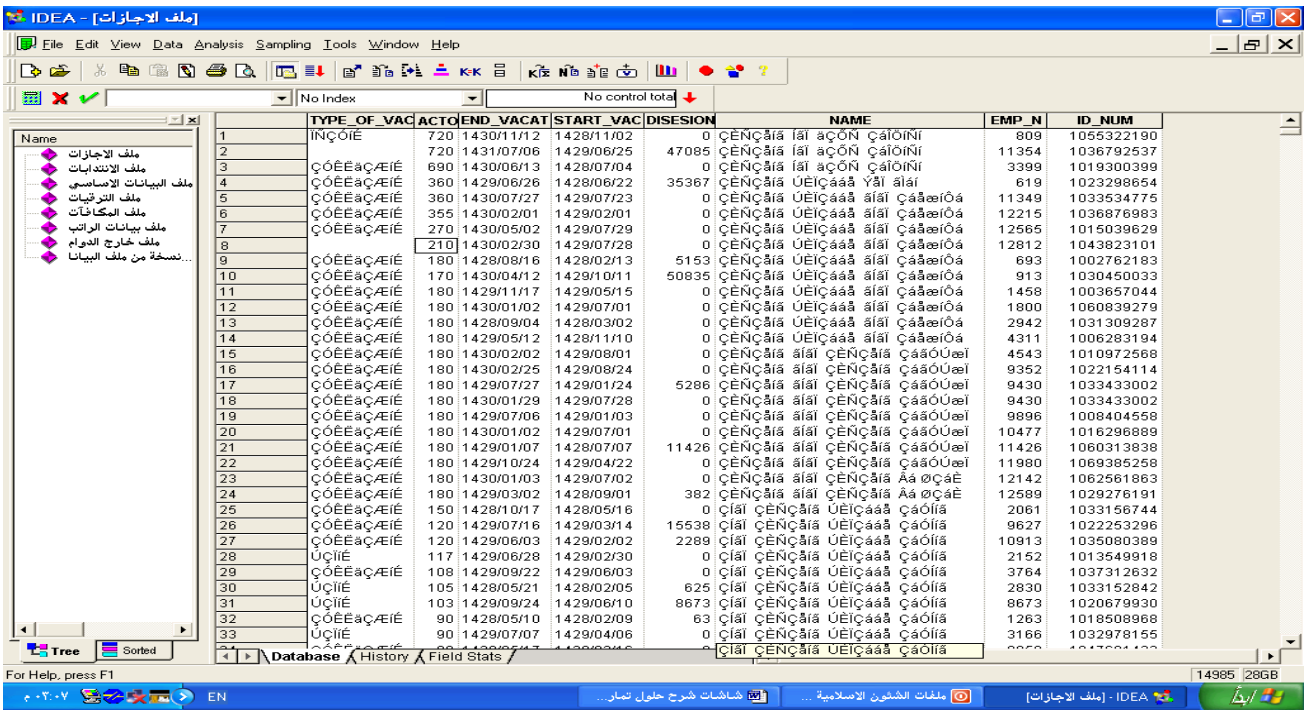
بعد ذلك يتم إدخال اسم الملف الذي سيتم استيراده ومن ثم إنهاء .



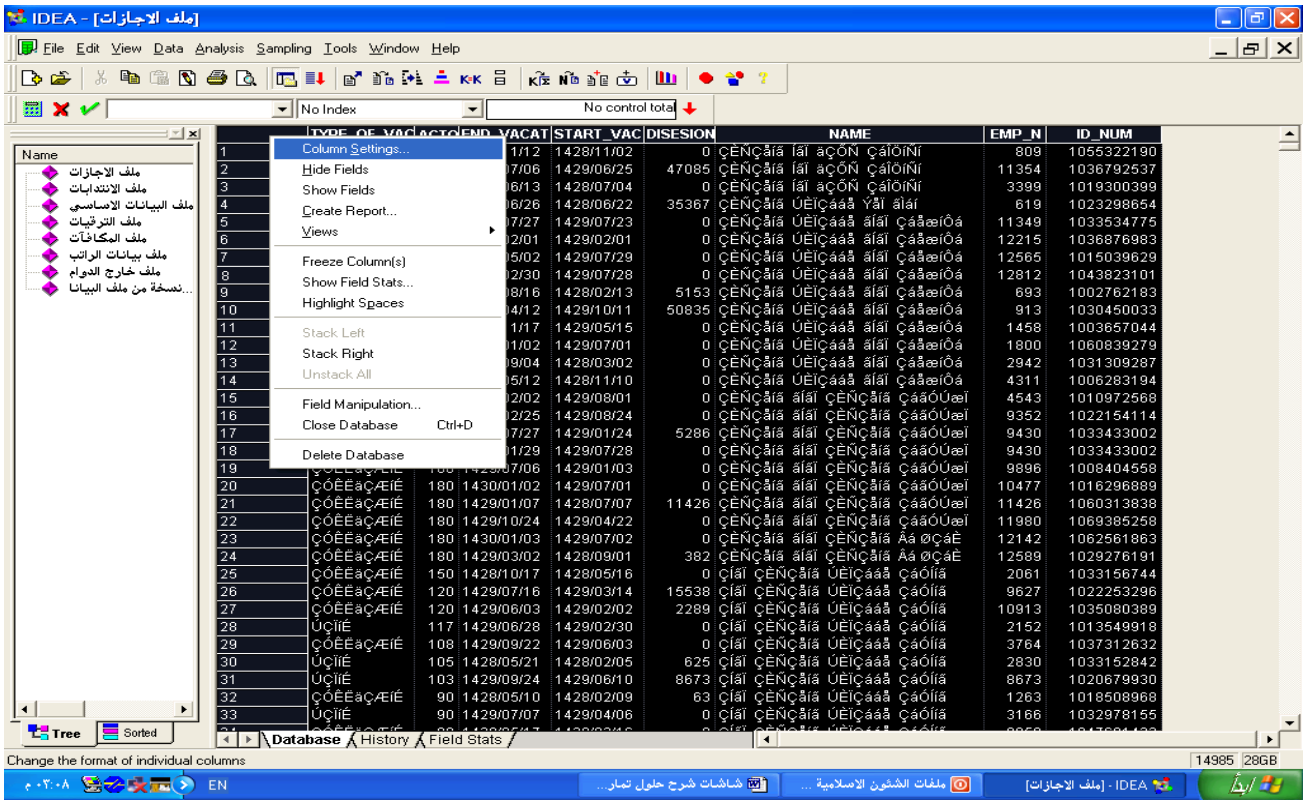
بعد ذلك ستظهر البيانات بهذا الشكل ... ومن هنا تبدأ عملية التحليل ...



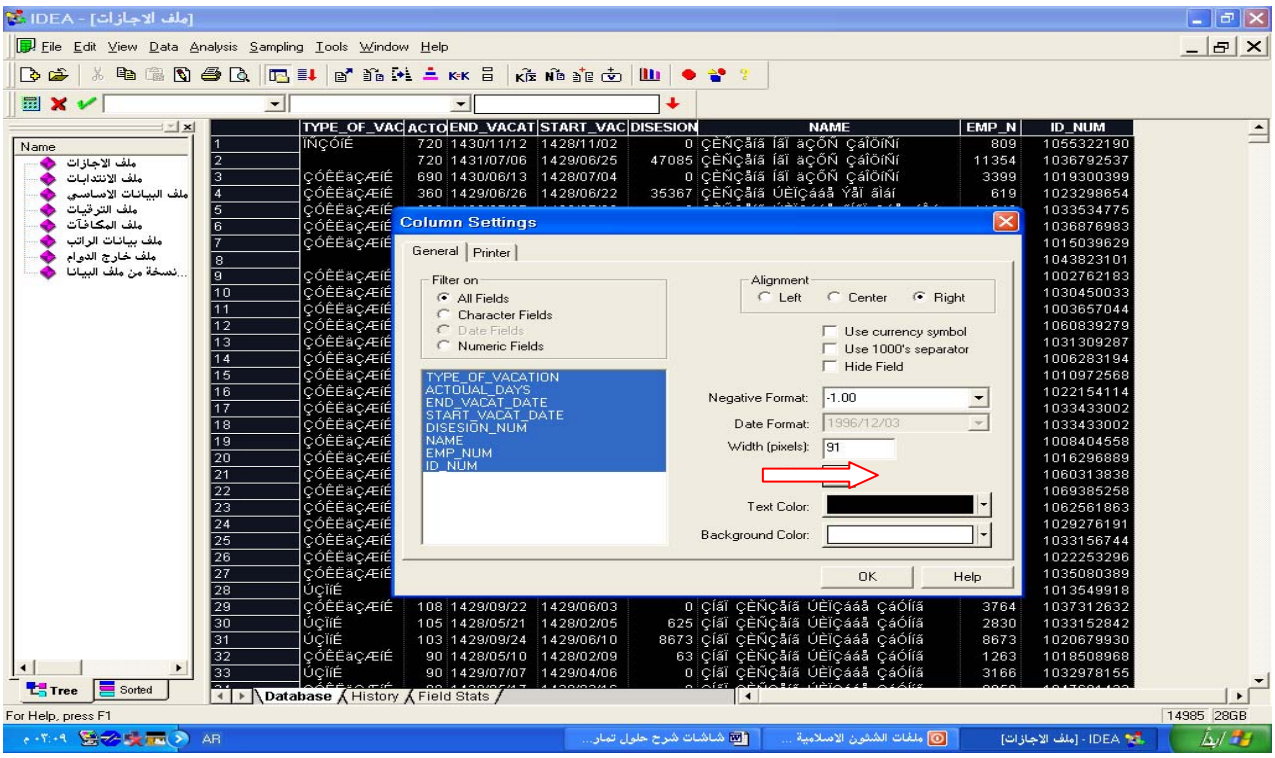
في حالة ظهور البيانات بالشكل التالي ... بيانات غير مفهومة نقوم بتغير الخط واللغة حسب ما هو موضح في الشاشات المرفقة :



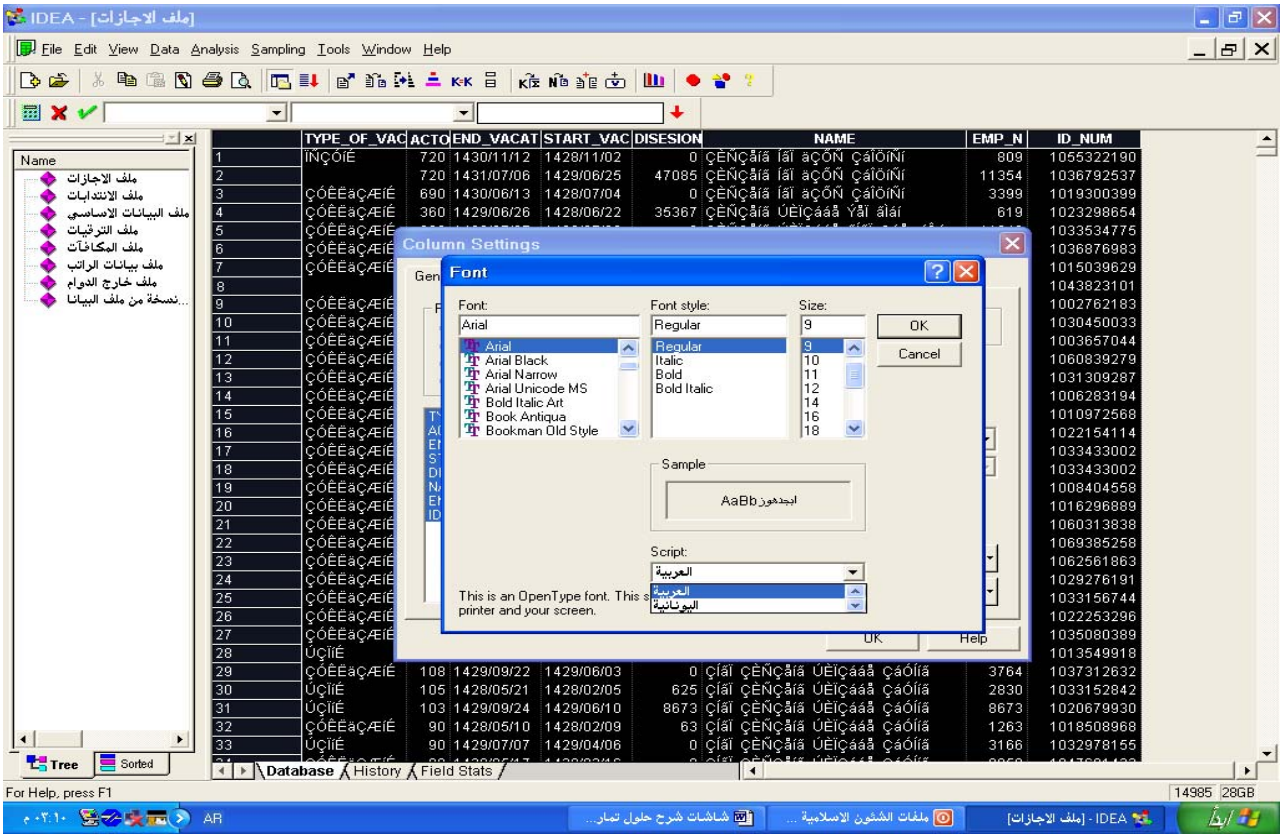
نظلل كامل الجدول بالضغط على أول المربع من اليسار في الجدول ومن ثم نضغط على الماوس الأيسر وتظهر القائمة التالية :



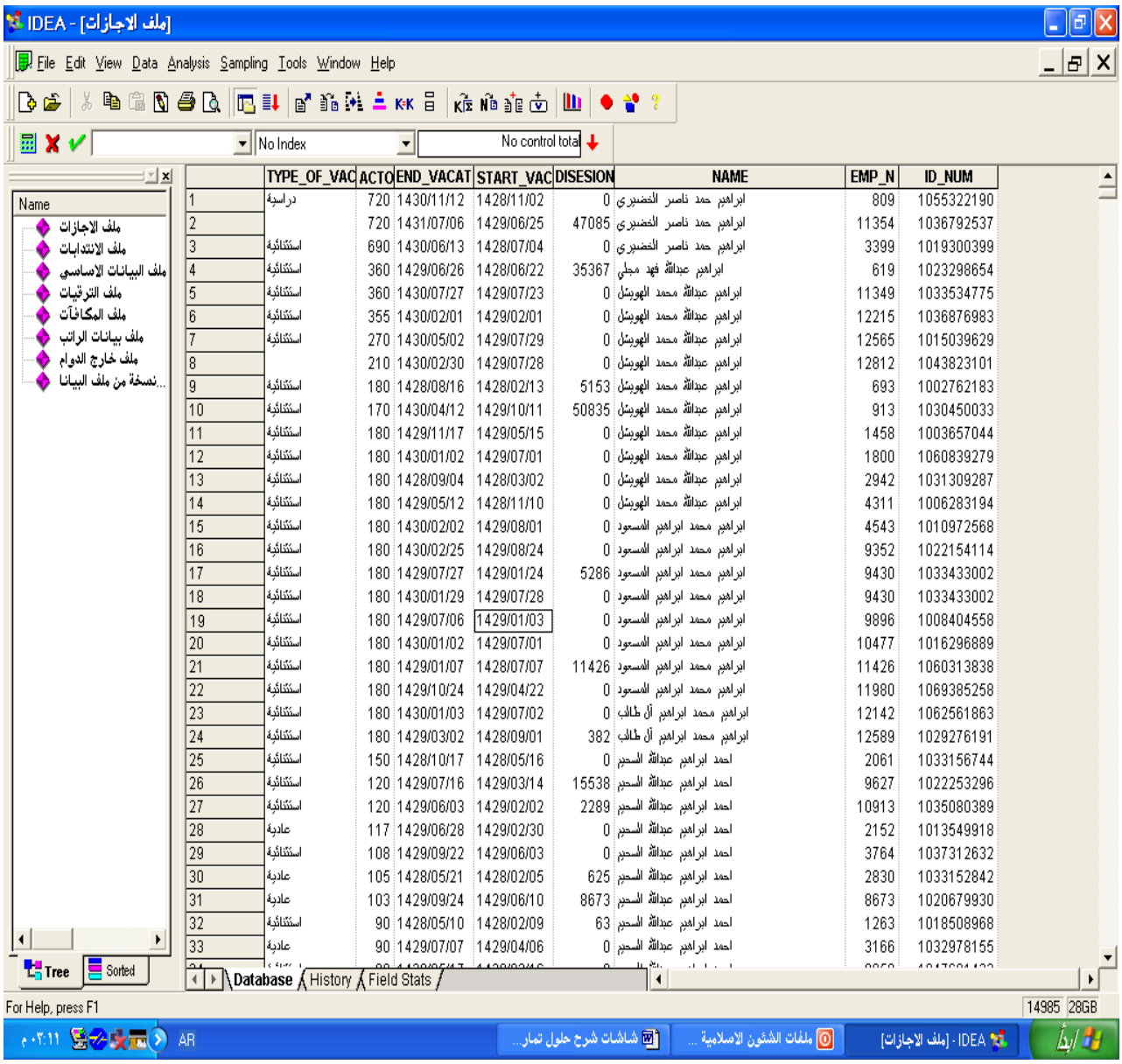
بعد ذلك نقوم بالضغط على الأيقونة Column sitting



يظهر مربع حوار لاختيار الخط ونختار Font وتظهر الشاشة التالية



بعد ذلك ستظهر البيانات بالشكل التالي :

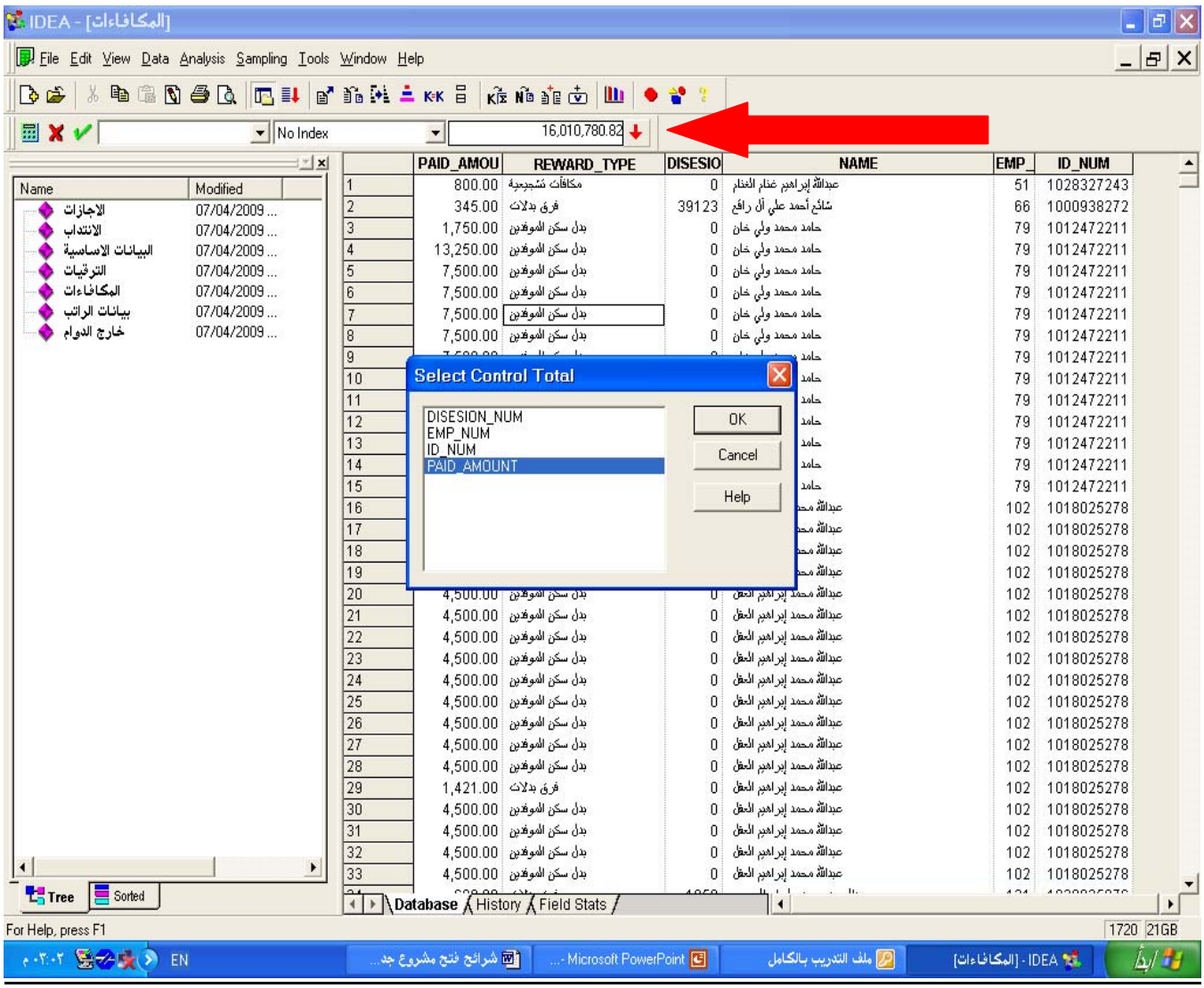


	TYPE_OF_VAC	ACTO	END_VACAT	START_VAC	DISESION	NAME	EMP_N	ID_NUM
1	دراسية	720	1430/11/12	1428/11/02	0	ابراهيم حمد ناصر الخضيري	809	1055322190
2		720	1431/07/06	1429/06/25	47085	ابراهيم حمد ناصر الخضيري	11354	1036792537
3	استثنائية	690	1430/06/13	1428/07/04	0	ابراهيم حمد ناصر الخضيري	3399	1019300399
4	استثنائية	360	1429/06/26	1428/06/22	35367	ابراهيم عبدالله فهد مجلي	619	1023298654
5	استثنائية	360	1430/07/27	1429/07/23	0	ابراهيم عبدالله محمد الهويشل	11349	1033534775
6	استثنائية	355	1430/02/01	1429/02/01	0	ابراهيم عبدالله محمد الهويشل	12215	1036876983
7	استثنائية	270	1430/05/02	1429/07/29	0	ابراهيم عبدالله محمد الهويشل	12565	1015039629
8		210	1430/02/30	1429/07/28	0	ابراهيم عبدالله محمد الهويشل	12812	1043823101
9	استثنائية	180	1428/08/16	1428/02/13	5153	ابراهيم عبدالله محمد الهويشل	693	1002762183
10	استثنائية	170	1430/04/12	1429/10/11	50835	ابراهيم عبدالله محمد الهويشل	913	1030450033
11	استثنائية	180	1429/11/17	1429/05/15	0	ابراهيم عبدالله محمد الهويشل	1458	1003657044
12	استثنائية	180	1430/01/02	1429/07/01	0	ابراهيم عبدالله محمد الهويشل	1800	1060839279
13	استثنائية	180	1428/09/04	1428/03/02	0	ابراهيم عبدالله محمد الهويشل	2942	1031309287
14	استثنائية	180	1429/05/12	1428/11/10	0	ابراهيم عبدالله محمد الهويشل	4311	1006283194
15	استثنائية	180	1430/02/02	1429/08/01	0	ابراهيم محمد ابراهيم المسعود	4543	1010972568
16	استثنائية	180	1430/02/25	1429/08/24	0	ابراهيم محمد ابراهيم المسعود	9352	1022154114
17	استثنائية	180	1429/07/27	1429/01/24	5286	ابراهيم محمد ابراهيم المسعود	9430	1033433002
18	استثنائية	180	1430/01/29	1429/07/28	0	ابراهيم محمد ابراهيم المسعود	9430	1033433002
19	استثنائية	180	1429/07/06	1429/01/03	0	ابراهيم محمد ابراهيم المسعود	9896	1008404558
20	استثنائية	180	1430/01/02	1429/07/01	0	ابراهيم محمد ابراهيم المسعود	10477	1016296889
21	استثنائية	180	1429/01/07	1428/07/07	11426	ابراهيم محمد ابراهيم المسعود	11426	1060313838
22	استثنائية	180	1429/10/24	1429/04/22	0	ابراهيم محمد ابراهيم المسعود	11980	1069385258
23	استثنائية	180	1430/01/03	1429/07/02	0	ابراهيم محمد ابراهيم آل طالب	12142	1062561863
24	استثنائية	180	1429/03/02	1428/09/01	382	ابراهيم محمد ابراهيم آل طالب	12589	1029276191
25	استثنائية	150	1428/10/17	1428/05/16	0	احمد ابراهيم عبدالله السحيم	2061	1033156744
26	استثنائية	120	1429/07/16	1429/03/14	15538	احمد ابراهيم عبدالله السحيم	9627	1022253296
27	استثنائية	120	1429/06/03	1429/02/02	2289	احمد ابراهيم عبدالله السحيم	10913	1035080389
28	عادية	117	1429/06/28	1429/02/30	0	احمد ابراهيم عبدالله السحيم	2152	1013549918
29	استثنائية	108	1429/09/22	1429/06/03	0	احمد ابراهيم عبدالله السحيم	3764	1037312632
30	عادية	105	1428/05/21	1428/02/05	625	احمد ابراهيم عبدالله السحيم	2830	1033152842
31	عادية	103	1429/09/24	1429/06/10	8673	احمد ابراهيم عبدالله السحيم	8673	1020679930
32	استثنائية	90	1428/05/10	1428/02/09	63	احمد ابراهيم عبدالله السحيم	1263	1018508968
33	عادية	90	1429/07/07	1429/04/06	0	احمد ابراهيم عبدالله السحيم	3166	1032978155

تطبيق رقم

تحديد حقل تجميعي Control Total

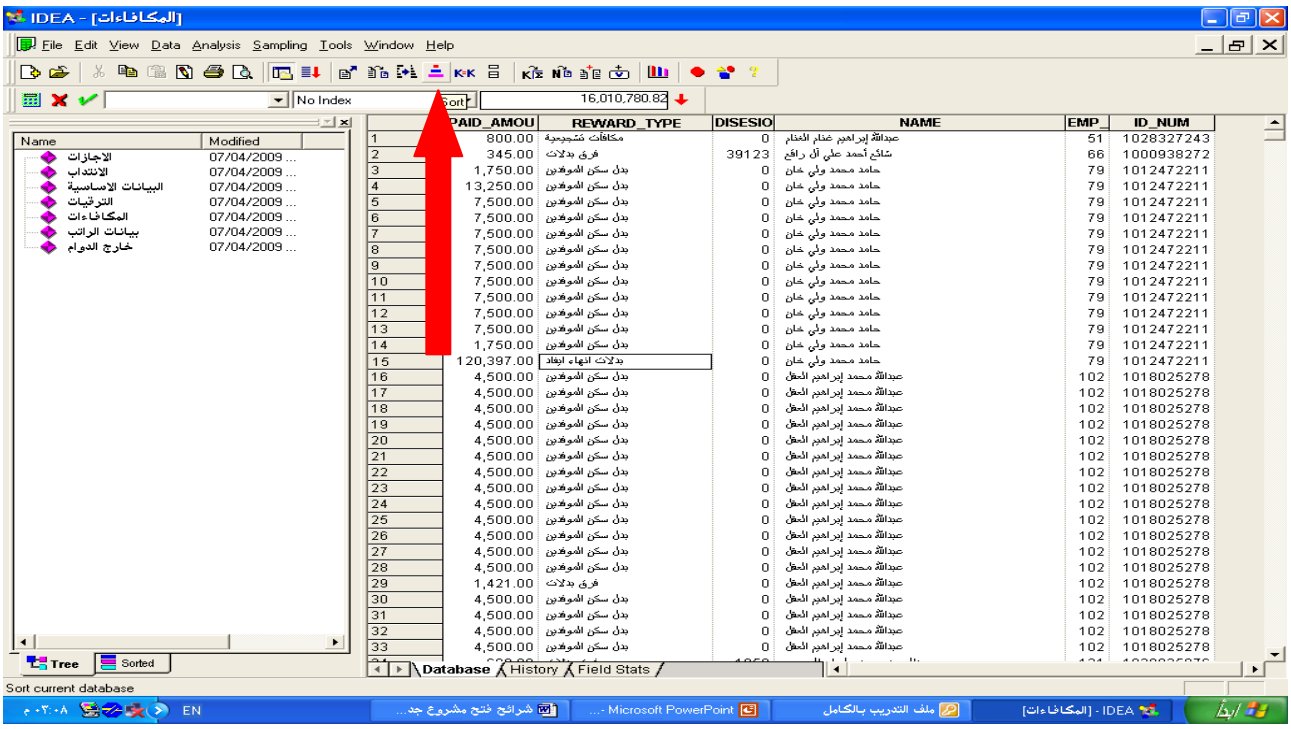
لتحديد المجاميع نضغط على السهم الموضح أدناه وبعده سوف تظهر القائمة التالية نضغط



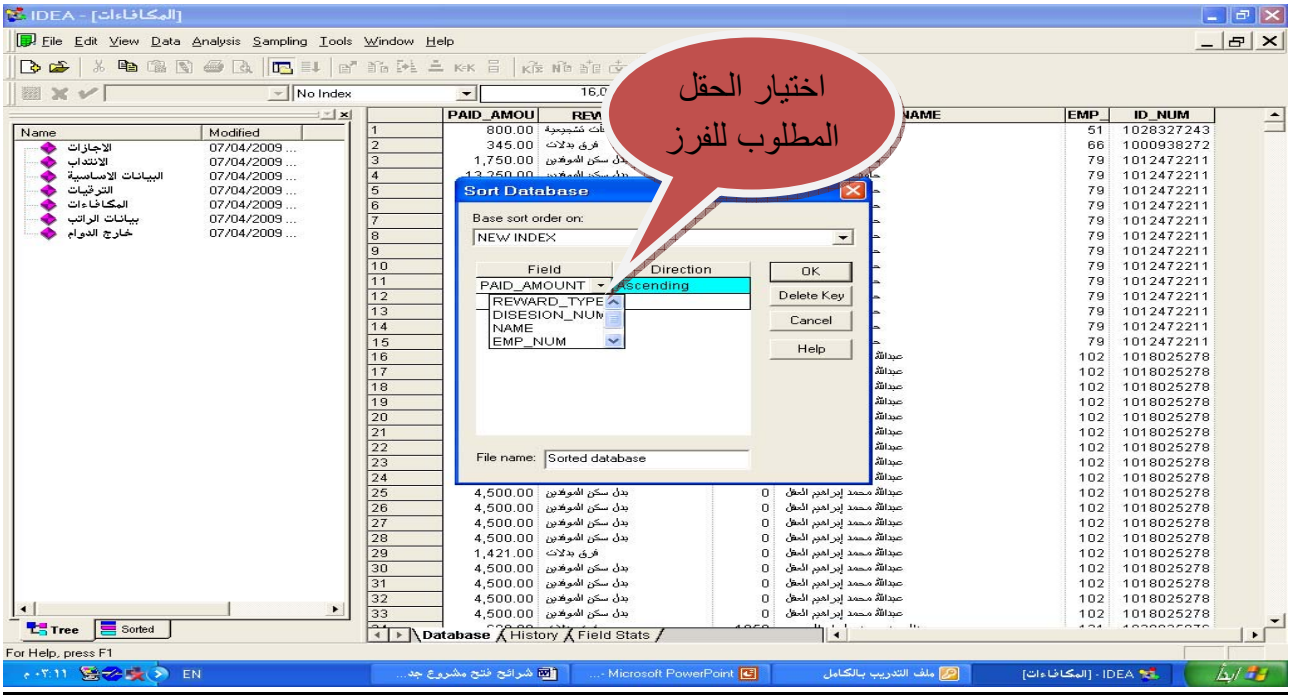
بعد ذلك سوف تظهر الحقول الرقمية فقط والتي يمكن جمعها ونختار ما نريد أن نجمعه كما هو موضح حيث قمنا باختيار حقل Paid Amount وظهر المجموع في المستطيل في الأعلى ... ونقوم بنفس الطريقة السابقة لإجراء عمليات جمع أخرى لأي حقول .

تطبيق رقم

نقوم باختيار الأيقونة الموضحة أدناه لفرز البيانات من الأكبر إلى الأصغر والعكس أو من خلال الذهاب للقائمة Data – Sort

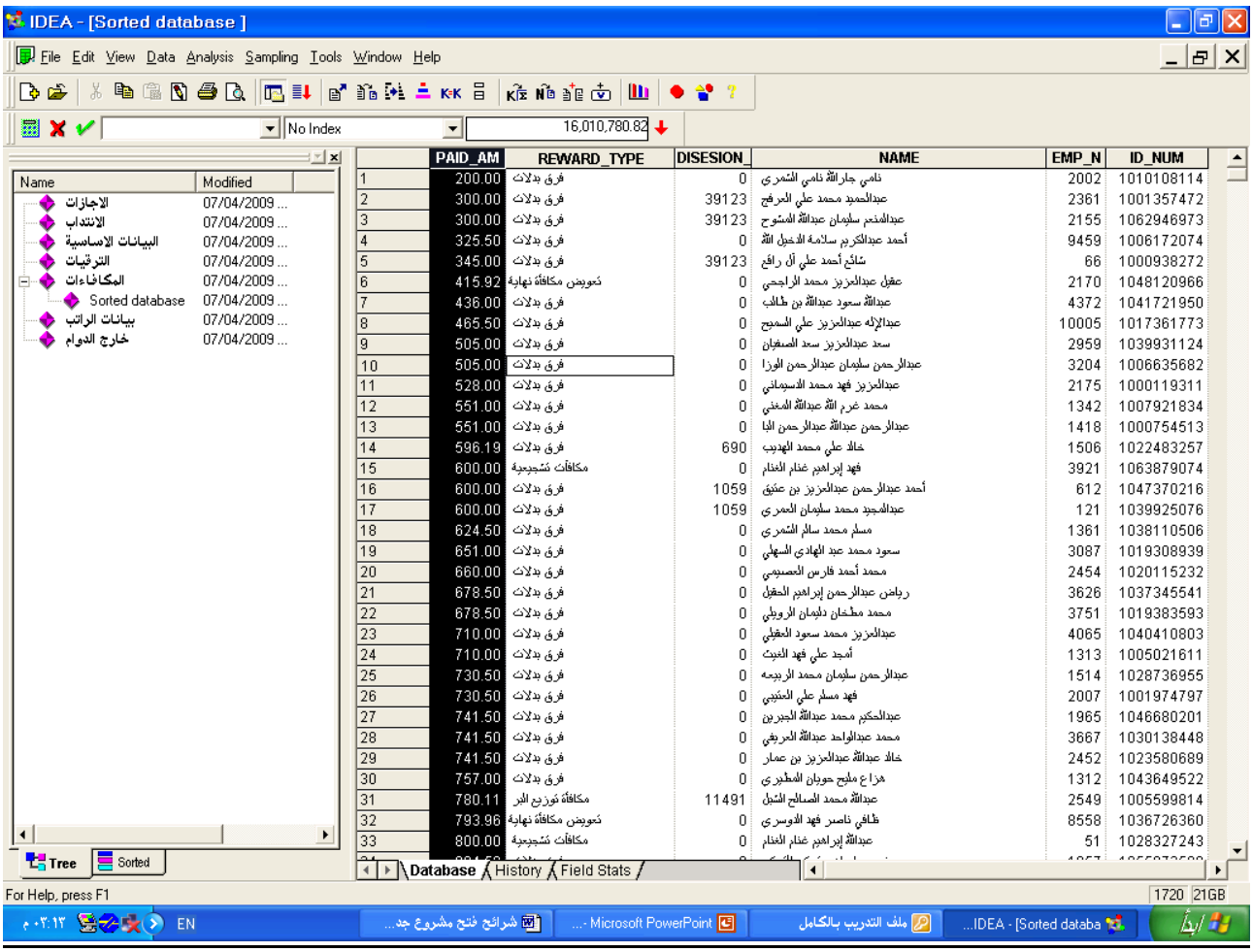


بعد ذلك يظهر المربع التالي :



نقوم باختيار الحقل الذي نرغب بفرزه ونضغط موافق ,

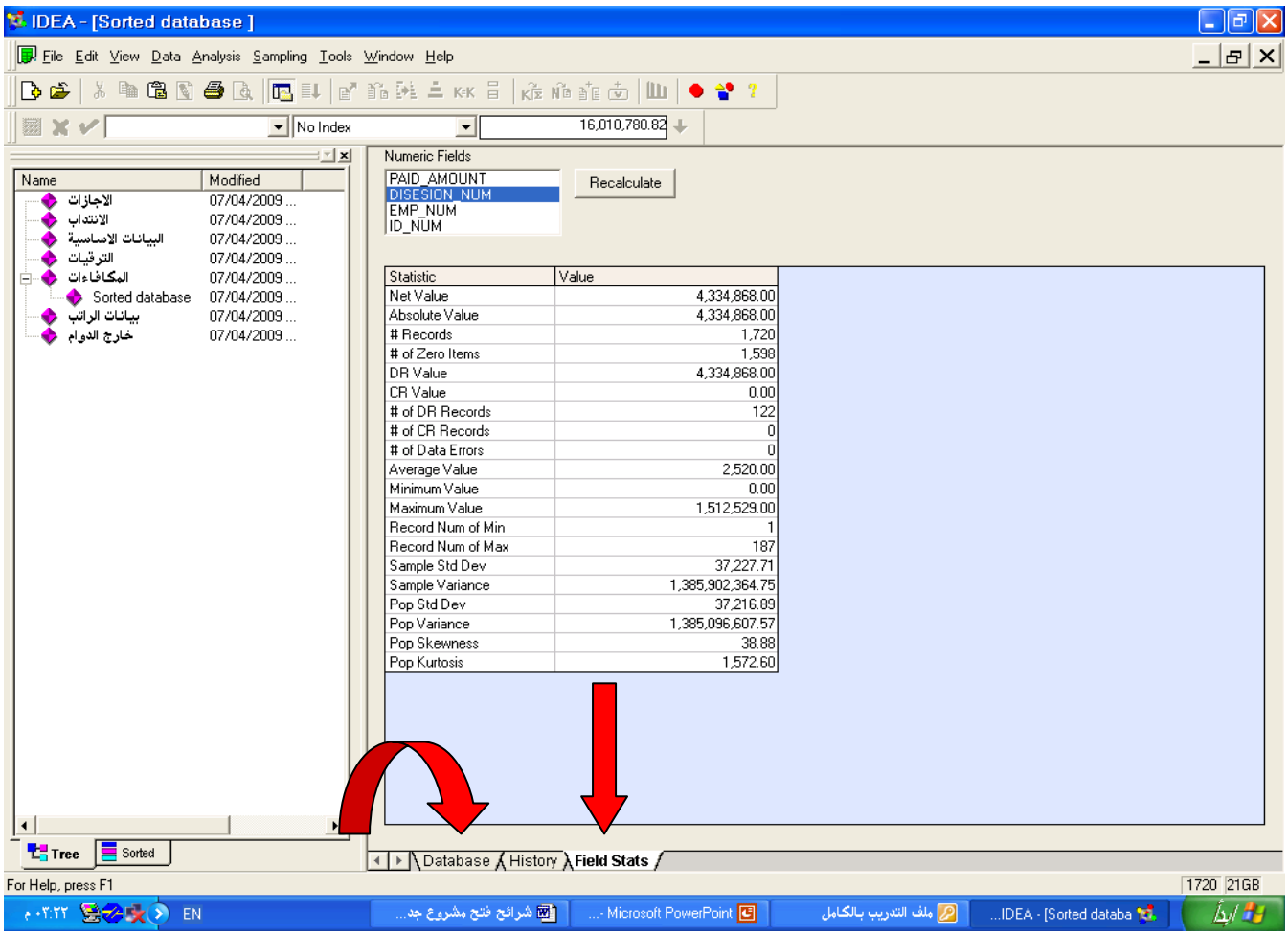
وسوف تظهر البيانات كالتالي على اعتبار انه قمنا باختيار حقل Paid Amount وسوف نلاحظ أنها مرتبة من الأصغر إلى الأكبر ونطبق ذلك على الحالات المماثلة



تطبيق رقم

لمعرفة أعلى قيمة وأدنى قيمة والمتوسط الحسابي ومعلومات أخرى إحصائية في الملف المراد تحليله

من خلال الأمر FIELD STATISTICS كما هو موضح أدناه .

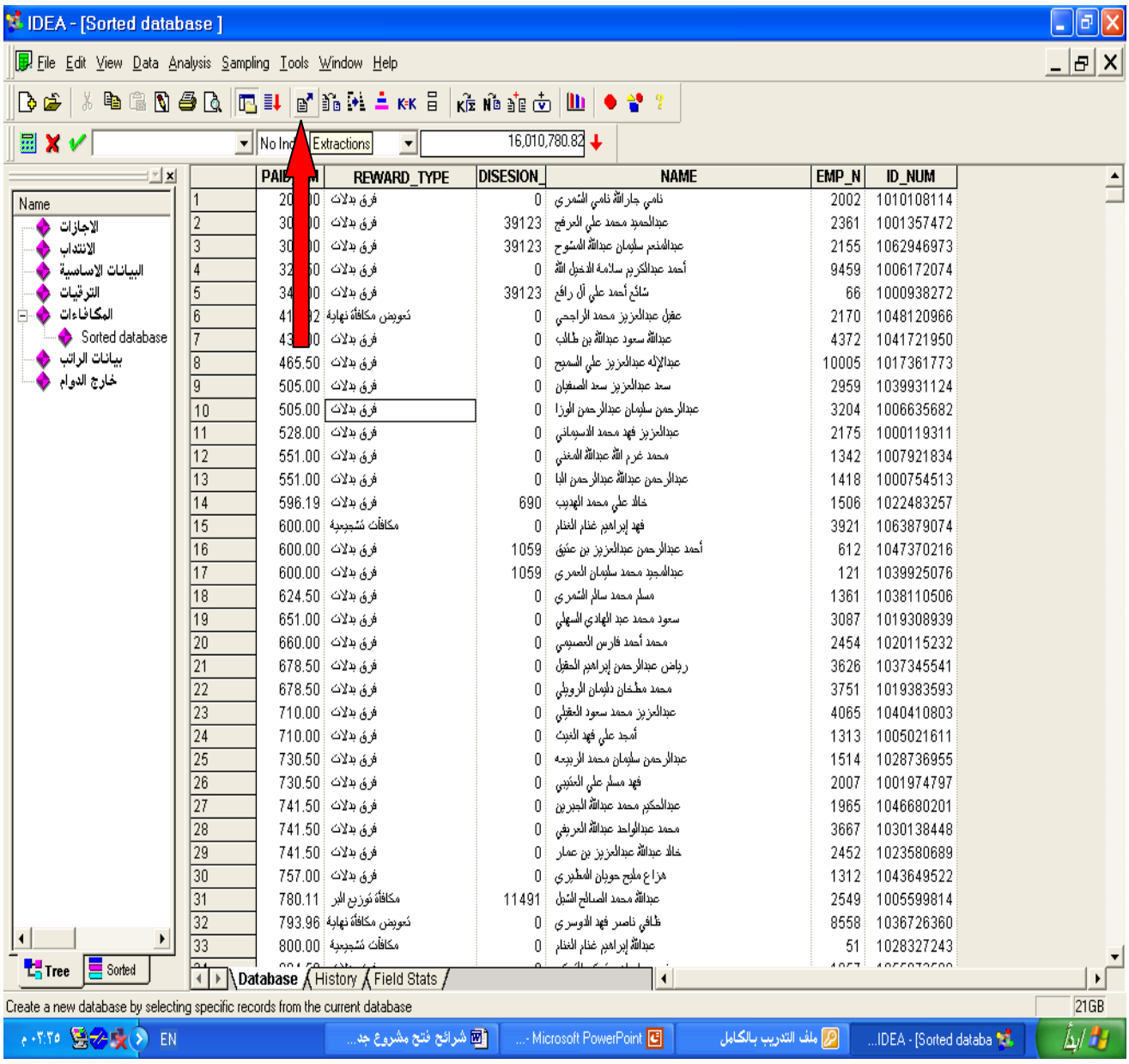


وعند الرغبة للعودة للبيانات نقوم بالضغط على الأيقونة التي بجانبها وتسمى Database كما هو موضح في السهم السابق .

تطبيق رقم

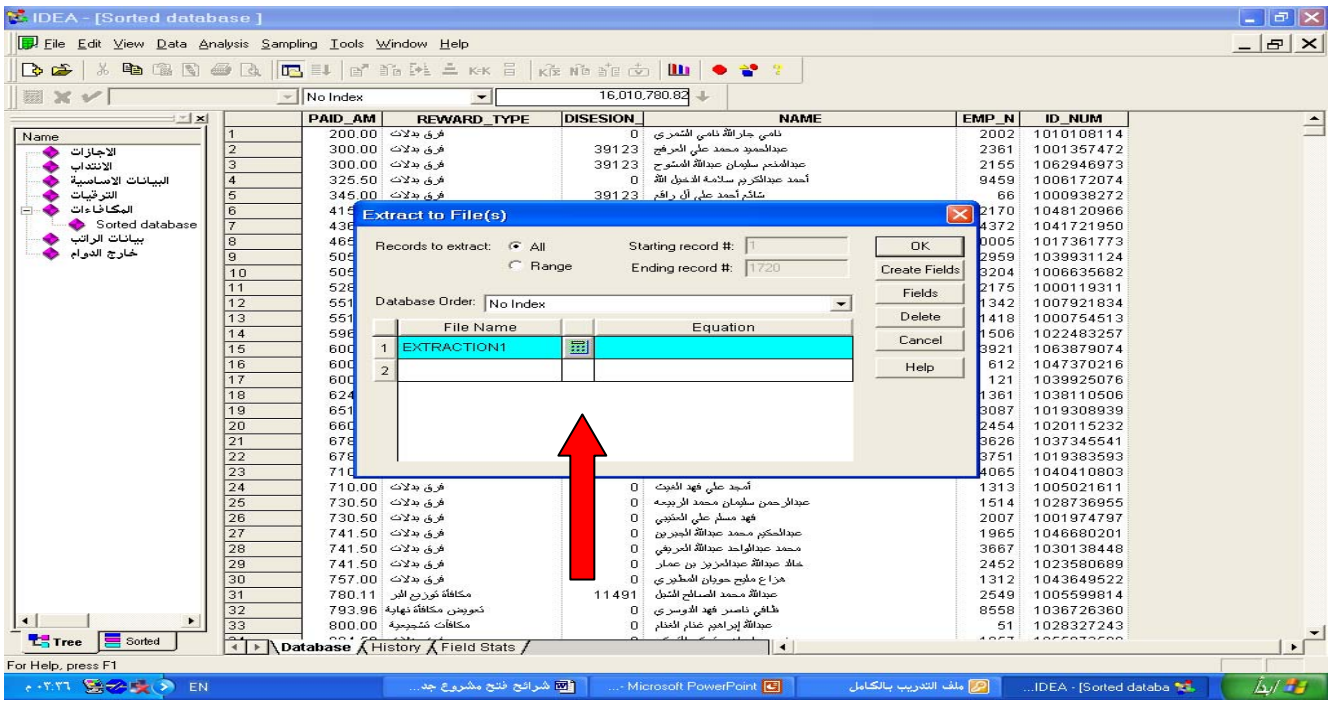
الأمر Extractions ويفيد في استخلاص التقارير التي يحتاجها المراجع من البيانات المتوفرة وذلك من خلال وضع المعادلات المطلوبة لعمليات المراجعة ومثال ذلك :

نقوم باختيار الأيقونة كما هو موضح أدناه , أو من خلال الذهاب إلى القائمة Data- Extraction أو من خلال الضغط على الأمر الموضح بالسهم .



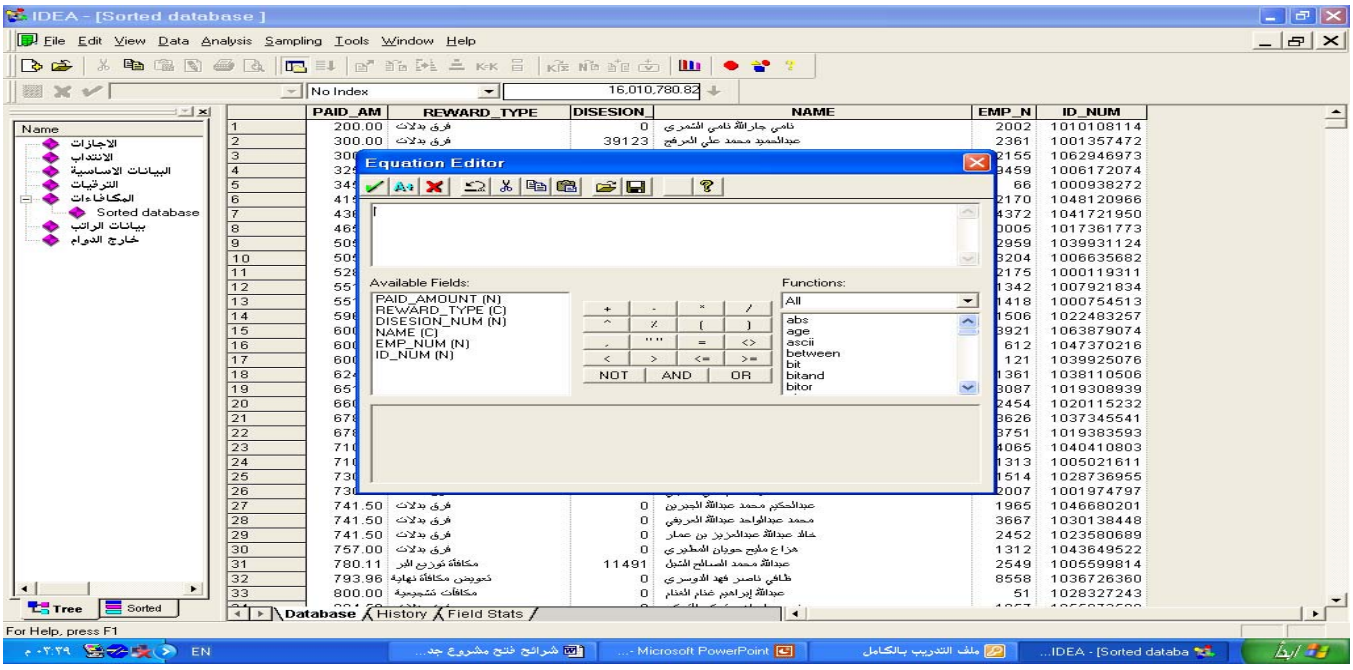
	PAID_AM	REWARD_TYPE	DISESION_	NAME	EMP_N	ID_NUM
1	20 00	فرق بدلات	0	ناصي جارالله ناصي الشمري	2002	1010108114
2	30 00	فرق بدلات	39123	عبدالحميد محمد علي المرفج	2361	1001357472
3	30 00	فرق بدلات	39123	عبدالمنعم سليمان عبدالله المسوح	2155	1062946973
4	32 50	فرق بدلات	0	أحمد عبدالكريم سلامة الدخيل الله	9459	1006172074
5	34 00	فرق بدلات	39123	شائع أحمد علي آل رافع	66	1000938272
6	41 92	تعويض مكافأة نهاية	0	عقيل عبدالعزيز محمد الراجحي	2170	1048120966
7	43 00	فرق بدلات	0	عبدالله سعود عبدالله بن طالب	4372	1041721950
8	465.50	فرق بدلات	0	عبدالإله عبدالعزيز علي السميح	10005	1017361773
9	505.00	فرق بدلات	0	سعد عبدالعزيز سعد الصفيان	2959	1039931124
10	505.00	فرق بدلات	0	عبدالرحمن سليمان عبدالرحمن الوزا	3204	1006635682
11	528.00	فرق بدلات	0	عبدالعزيز فهد محمد الاسيماني	2175	1000119311
12	551.00	فرق بدلات	0	محمد غرم الله عبدالله المغني	1342	1007921834
13	551.00	فرق بدلات	0	عبدالرحمن عبدالله عبدالرحمن البا	1418	1000754513
14	596.19	فرق بدلات	690	خالد علي محمد الهديب	1506	1022483257
15	600.00	مكافأت تشجيعية	0	فهد إبراهيم غنام الغنام	3921	1063879074
16	600.00	فرق بدلات	1059	أحمد عبدالرحمن عبدالعزيز بن عتيق	612	1047370216
17	600.00	فرق بدلات	1059	عبدالمجيد محمد سليمان العمري	121	1039925076
18	624.50	فرق بدلات	0	مسلم محمد سالم الشمري	1361	1038110506
19	651.00	فرق بدلات	0	سعود محمد عبد الهادي السهلي	3087	1019308939
20	660.00	فرق بدلات	0	محمد أحمد فارس العصيمي	2454	1020115232
21	678.50	فرق بدلات	0	رياض عبدالرحمن إبراهيم الحقيل	3626	1037345541
22	678.50	فرق بدلات	0	محمد مطخان دليمان الرويلي	3751	1019383593
23	710.00	فرق بدلات	0	عبدالعزيز محمد سعود العقيلي	4065	1040410803
24	710.00	فرق بدلات	0	أسجد علي فهد الغبيث	1313	1005021611
25	730.50	فرق بدلات	0	عبدالرحمن سليمان محمد الربيعه	1514	1028736955
26	730.50	فرق بدلات	0	فهد مسلم علي العتيبي	2007	1001974797
27	741.50	فرق بدلات	0	عبدالحكيم محمد عبدالله الجبرين	1965	1046680201
28	741.50	فرق بدلات	0	محمد عبدالواحد عبدالله العريفي	3667	1030138448
29	741.50	فرق بدلات	0	خالد عبدالله عبدالعزيز بن عمار	2452	1023580689
30	757.00	فرق بدلات	0	هزاع مليح حويان المطيري	1312	1043649522
31	780.11	مكافأة توزيع البر	11491	عبدالله محمد الصالح الشبل	2549	1005599814
32	793.96	تعويض مكافأة نهاية	0	طافي ناصر فهد الدوسري	8558	1036726360
33	800.00	مكافأت تشجيعية	0	عبدالله إبراهيم غنام الغنام	51	1028327243

بعد ذلك سوف يظهر المربع التالي , ونقوم بالضغط على الحاسبة التي في وسط المربع كما هو موضح في الصورة المرفقة .



بعد ذلك سوف يظهر المربع التالي :

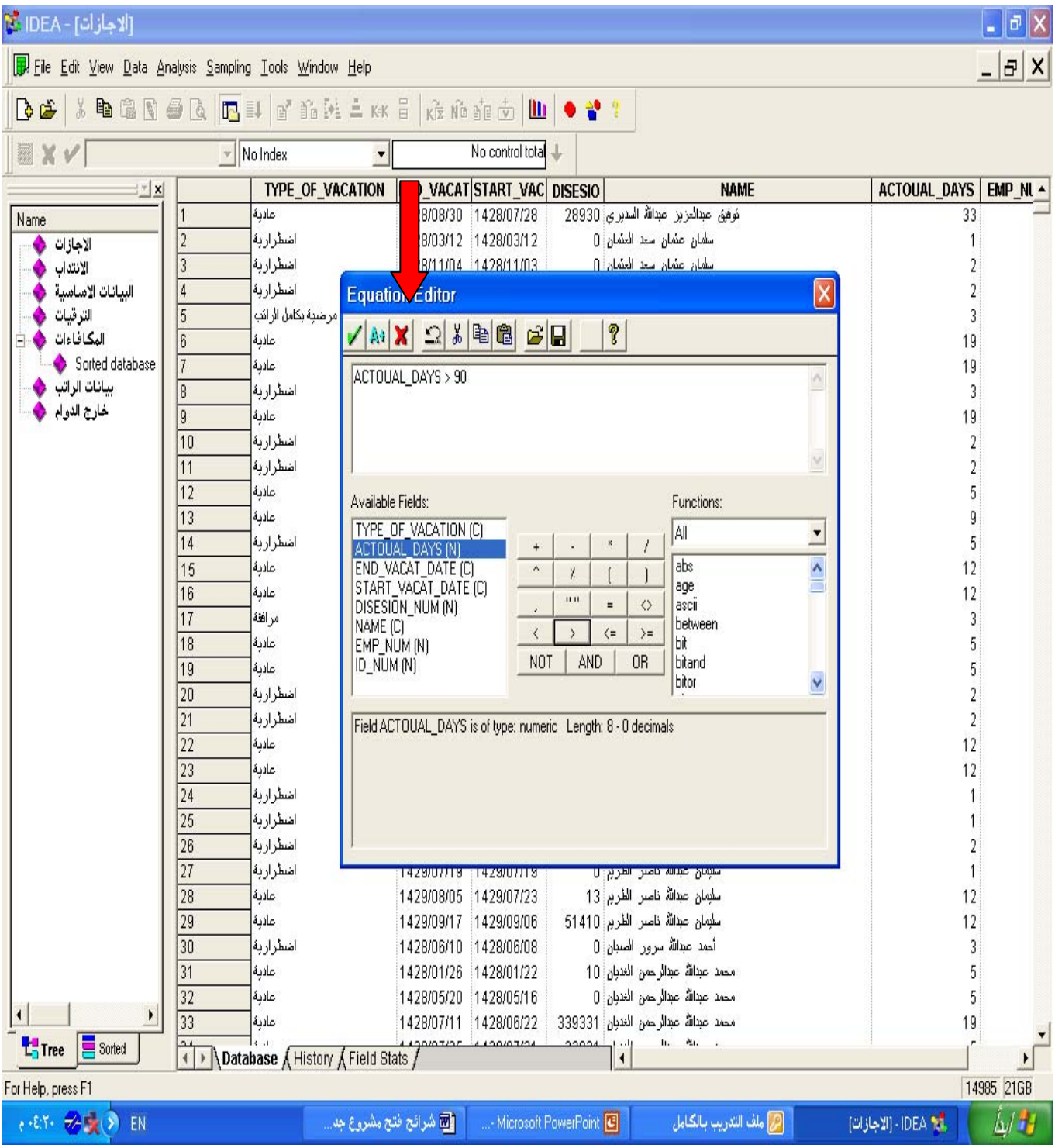
والتي يقوم المراجع بكتابة المعادلة المطلوبة لإجراء الاختبار الذي سيتم تنفيذه .



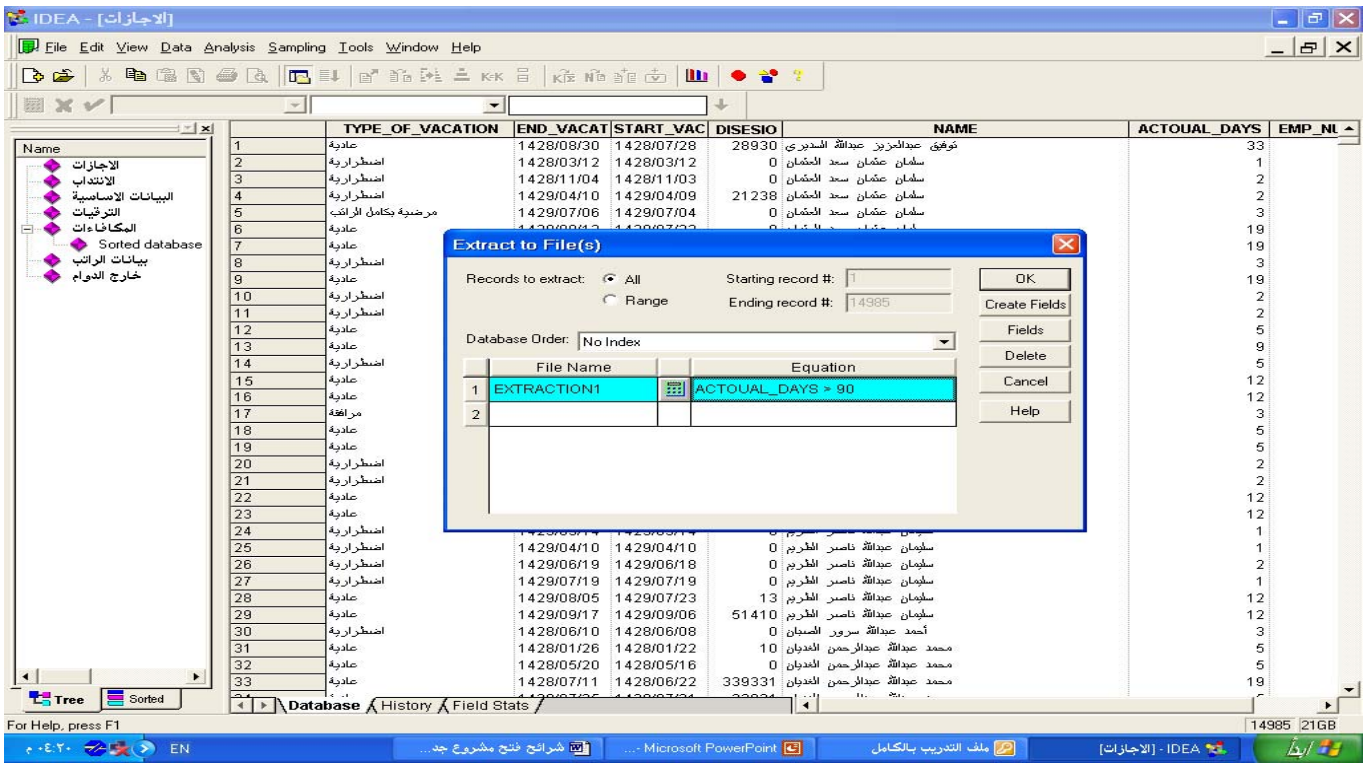
بعد ذلك نضع المعادلة كما هو موضح أدناه , والتي وضعنا فيها المثال التالي :

معرفة عدد أيام الإجازة التي تتجاوز المدة النظامية المسموح بها وهي 90 يوماً إلا باستثناء خاص

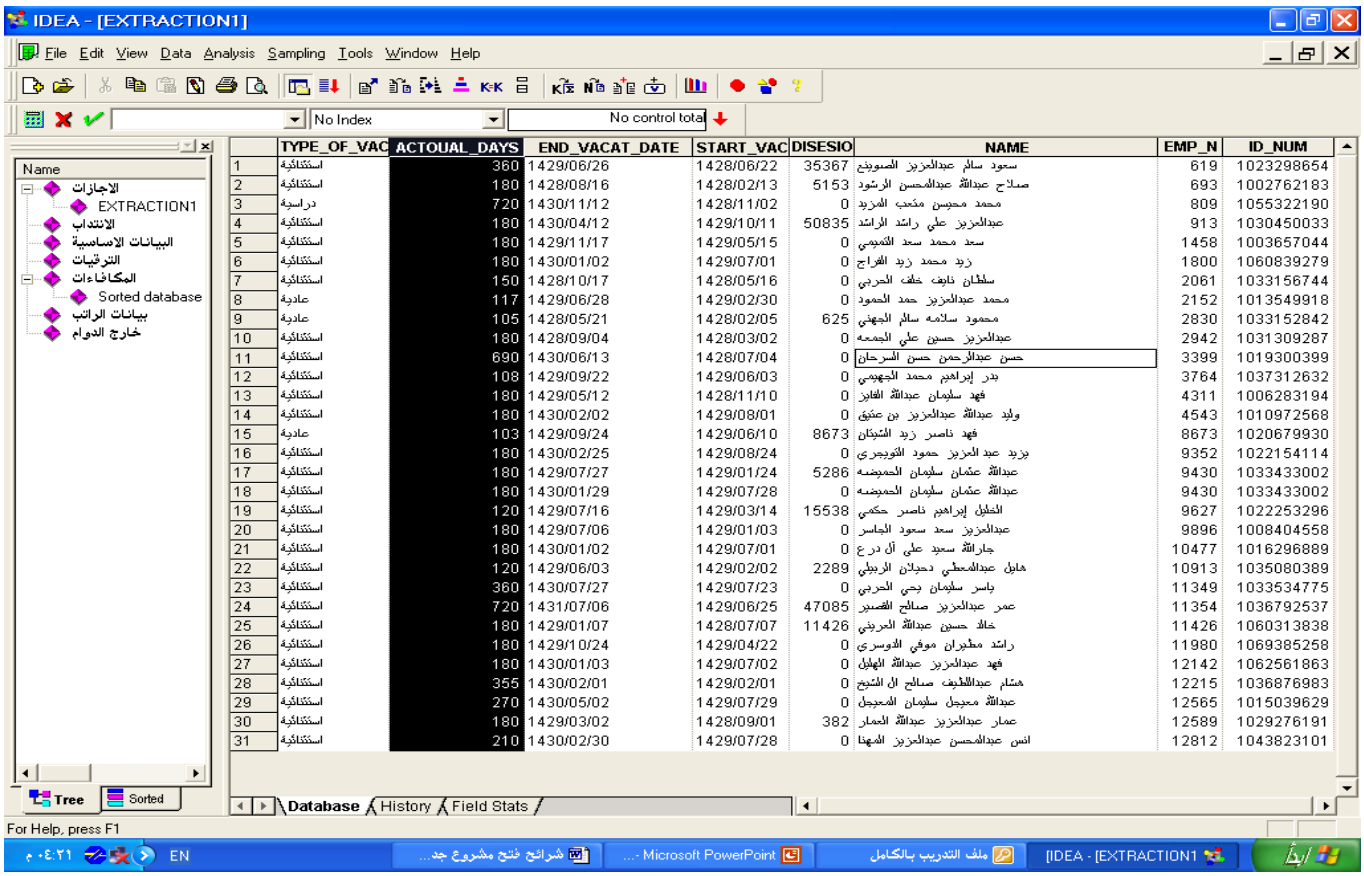
وبعد كتابة المعادلة من الممكن التحقق من صحتها وذلك بالضغط على الأيقونة الموضحة أدناه وهي A+ , وإذا كانت المعادلة مقبولة تظهر رسالة أسفل المربع Valid Equation وبعد ذلك يتم تنفيذ المعادلة بالضغط على علامة الصح .



وبعد تنفيذ المعادلة سوف يظهر المربع التالي :



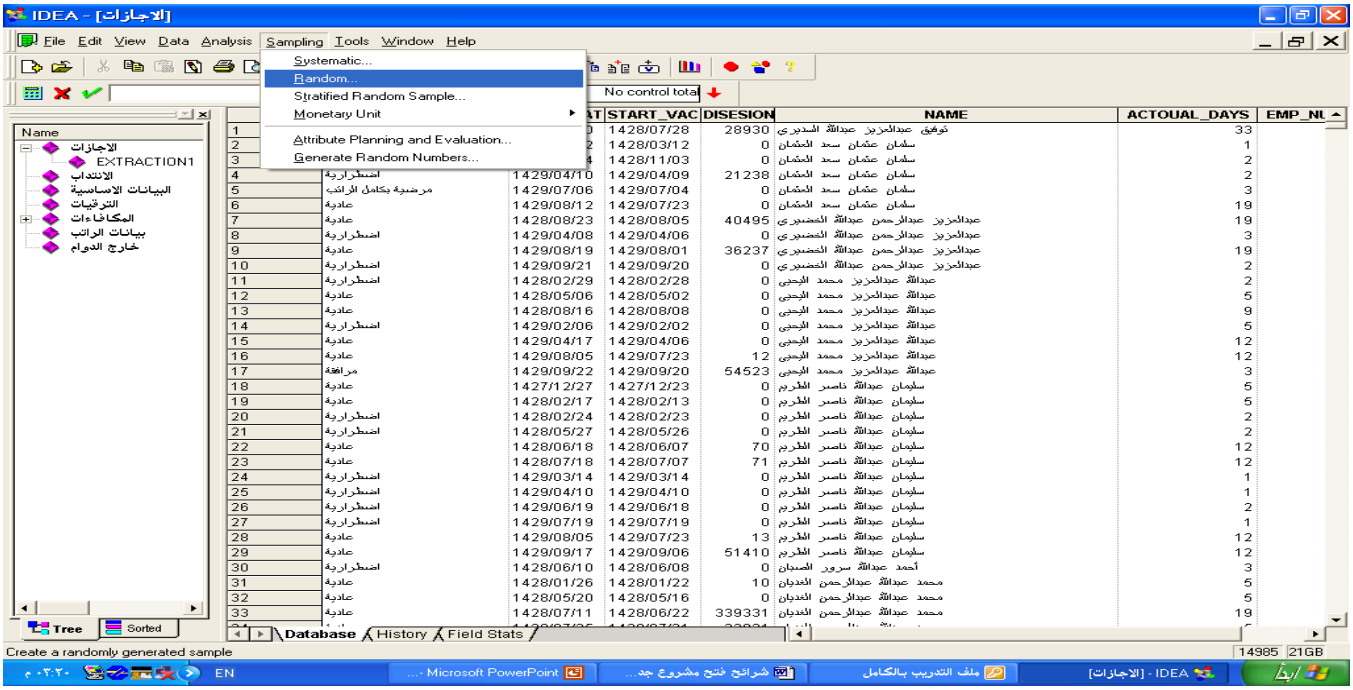
ثم نضغط OK وبعد ذلك ستظهر النتيجة التالية :



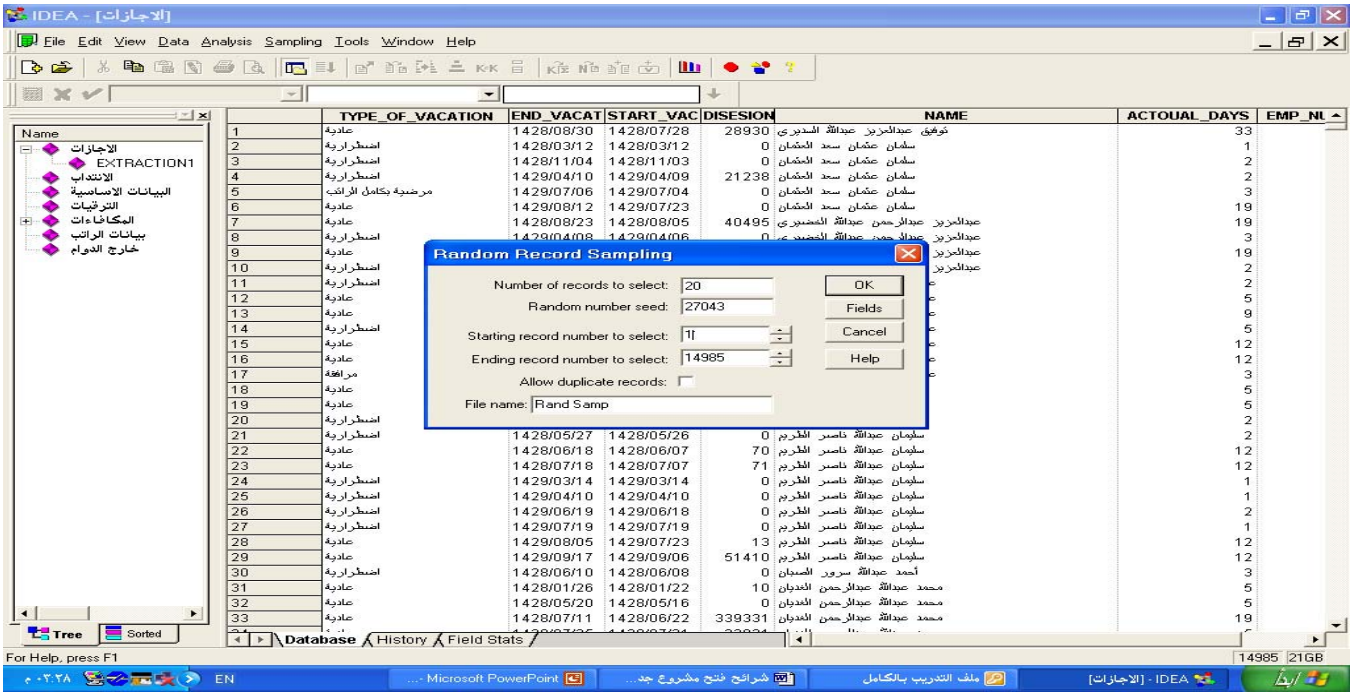
تطبيق رقم

الأمر Sampling, Random العينات الإحصائية العشوائية استخلاص عينة إحصائية من الملف وتحديد بداية العينة وتحديد نهاية العينة ومثال ذلك :

نقوم باختيار sampling من القائمة ثم اختيار Random كما في الشكل التالي :



بعد ذلك ستظهر الشاشة التالية :

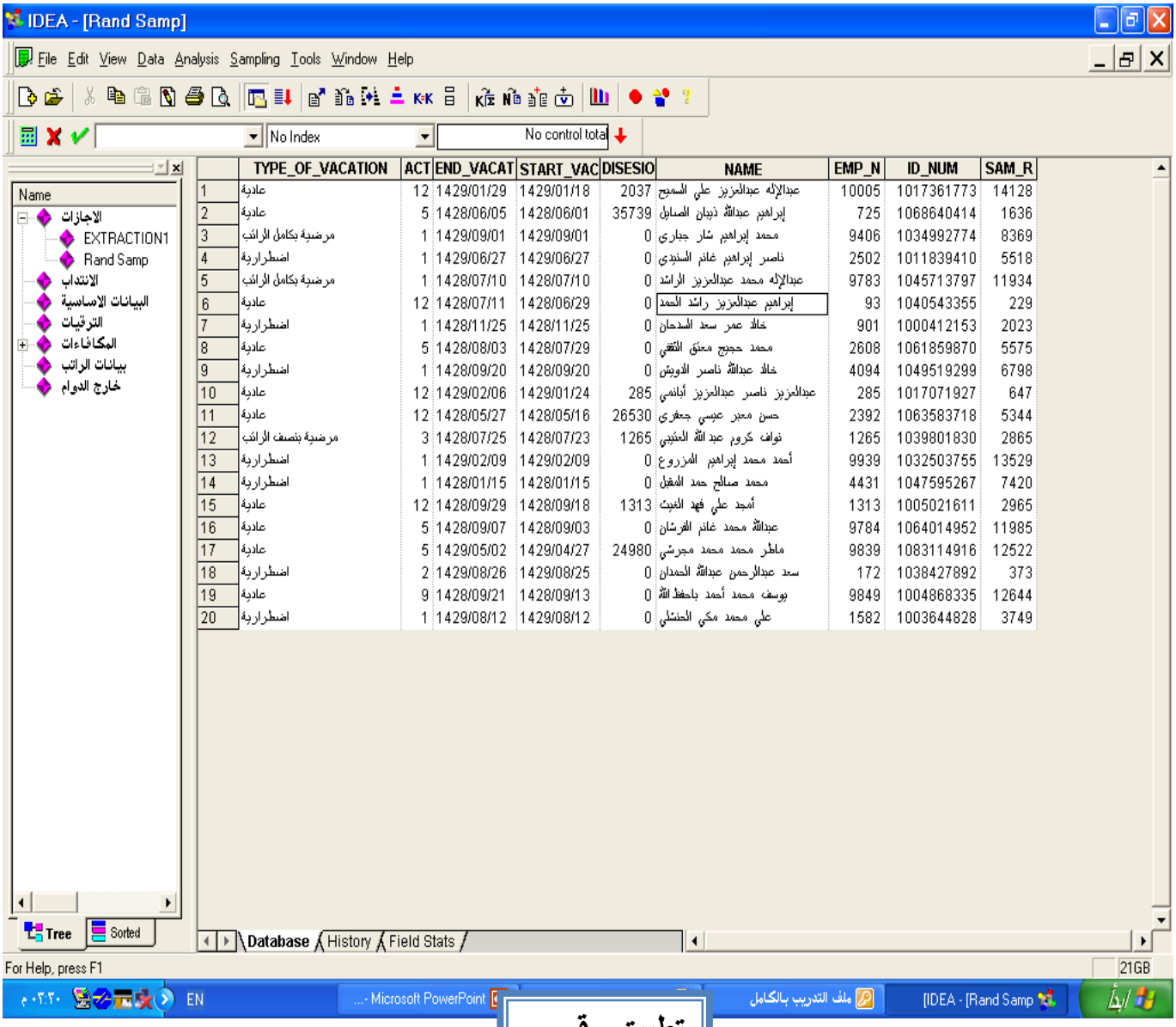


نقوم بتعبئة البيانات التالية كما هو موضح أدناه :

في الخانة الأولى نحدد عدد السجلات المطلوب اختيارها كعينة .

في الخانة الثانية نحدد عدد السجلات التي يتم اختيارها مثلا سجلين من كل عشرة سجلات .

في الخانة الثالثة نحدد نقطة البداية من جميع السجلات .
في الخانة الرابعة نحدد نقطة نهاية عدد السجلات من جميع السجلات .
في الخانة الخامسة وهو السماح بتكرار السجلات عند اختياره .
في الخانة السادسة نحدد اسم الملف الذي سوف يظهر كنتيجة ضمن ملفات البرنامج .
بعد ذلك نضغط OK وسوف تظهر النتيجة التالية , حيث تم اختيار 20 سجل كعينة عشوائية .

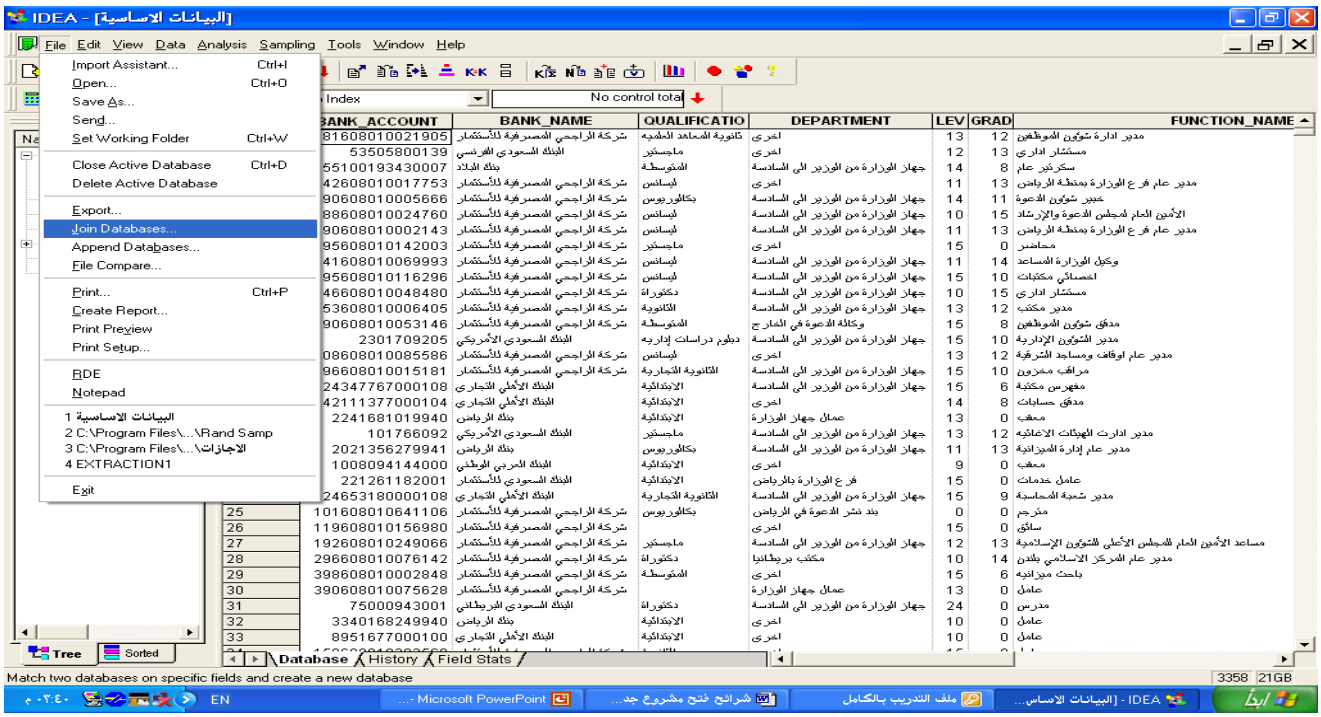


	TYPE_OF_VACATION	ACT	END_VACAT	START_VAC	DISESIO	NAME	EMP_N	ID_NUM	SAM_R
1	عادية	12	1429/01/29	1429/01/18	2037	عبدالإله عبدالعزيز علي السميح	10005	1017361773	14128
2	عادية	5	1428/06/05	1428/06/01	35739	إبراهيم عبدالله ذيبان الصابل	725	1068640414	1636
3	مرضية بكامل الراتب	1	1429/09/01	1429/09/01	0	محمد إبراهيم شار جباري	9406	1034992774	8369
4	اضطرارية	1	1429/06/27	1429/06/27	0	ناصر إبراهيم غانم السنيدي	2502	1011839410	5518
5	مرضية بكامل الراتب	1	1428/07/10	1428/07/10	0	عبدالإله محمد عبدالعزيز الراشد	9783	1045713797	11934
6	عادية	12	1428/07/11	1428/06/29	0	إبراهيم عبدالعزيز راشد الحمد	93	1040543355	229
7	اضطرارية	1	1428/11/25	1428/11/25	0	خالد عمر سعد السدحان	901	1000412153	2023
8	عادية	5	1428/08/03	1428/07/29	0	محمد حجيج معتق الثقفي	2608	1061859870	5575
9	اضطرارية	1	1428/09/20	1428/09/20	0	خالد عبدالله ناصر الدوبش	4094	1049519299	6798
10	عادية	12	1429/02/06	1429/01/24	285	عبدالعزيز ناصر عبدالعزيز أبانمي	285	1017071927	647
11	عادية	12	1428/05/27	1428/05/16	26530	حسن معبر عيسى جعفري	2392	1063583718	5344
12	مرضية بنصف الراتب	3	1428/07/25	1428/07/23	1265	نواف كروم عبد الله العتيبي	1265	1039801830	2865
13	اضطرارية	1	1429/02/09	1429/02/09	0	أحمد محمد إبراهيم المزروع	9939	1032503755	13529
14	اضطرارية	1	1428/01/15	1428/01/15	0	محمد صالح حمد الشقيل	4431	1047595267	7420
15	عادية	12	1428/09/29	1428/09/18	1313	أسجد علي فهد الغبيت	1313	1005021611	2965
16	عادية	5	1428/09/07	1428/09/03	0	عبدالله محمد غانم القرشان	9784	1064014952	11985
17	عادية	5	1429/05/02	1429/04/27	24980	ماطر محمد محمد مجرشي	9839	1083114916	12522
18	اضطرارية	2	1429/08/26	1429/08/25	0	سعد عبدالرحمن عبدالله الحمدان	172	1038427892	373
19	عادية	9	1428/09/21	1428/09/13	0	يوسف محمد أحمد باحفظ الله	9849	1004868335	12644
20	اضطرارية	1	1429/08/12	1429/08/12	0	علي محمد مكي الحنشلي	1582	1003644828	3749

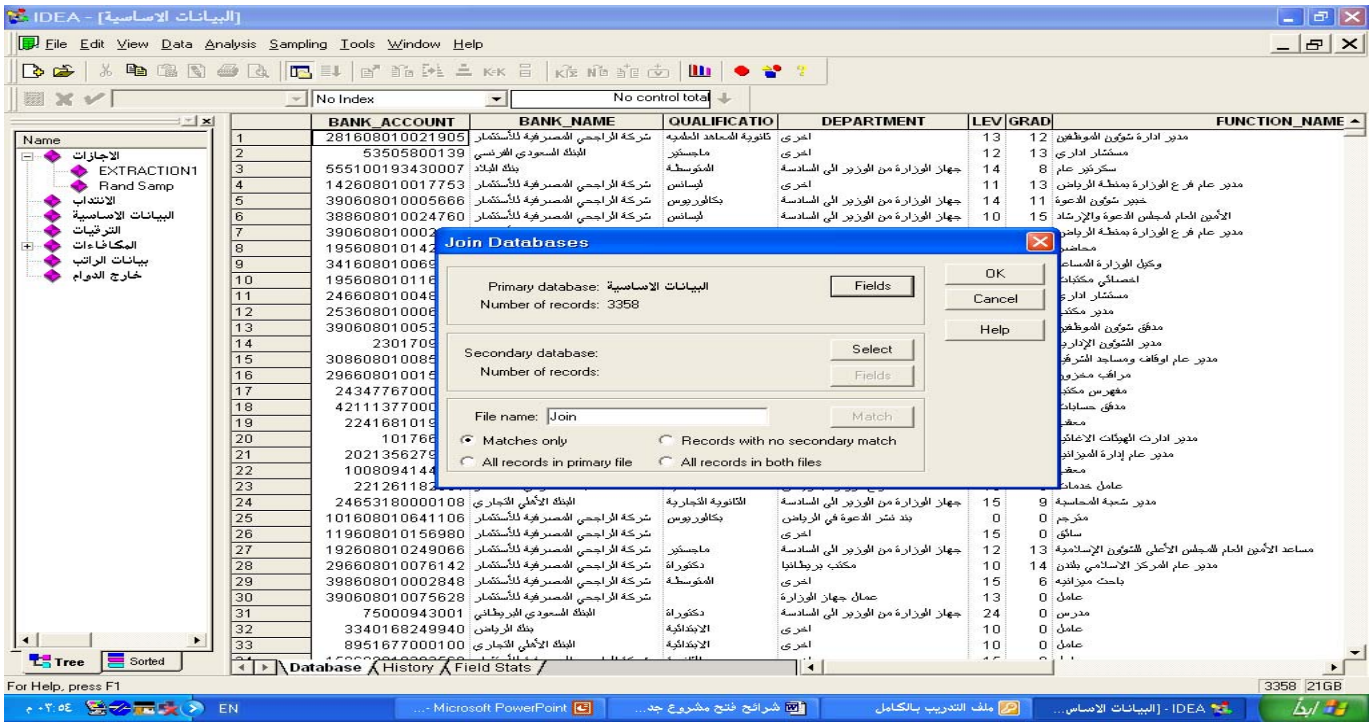
تطبيق رقم

الأمر join database والذي يفيد في ربط الملفات مع بعضها البعض بشرط توفر رابط بين الملفات

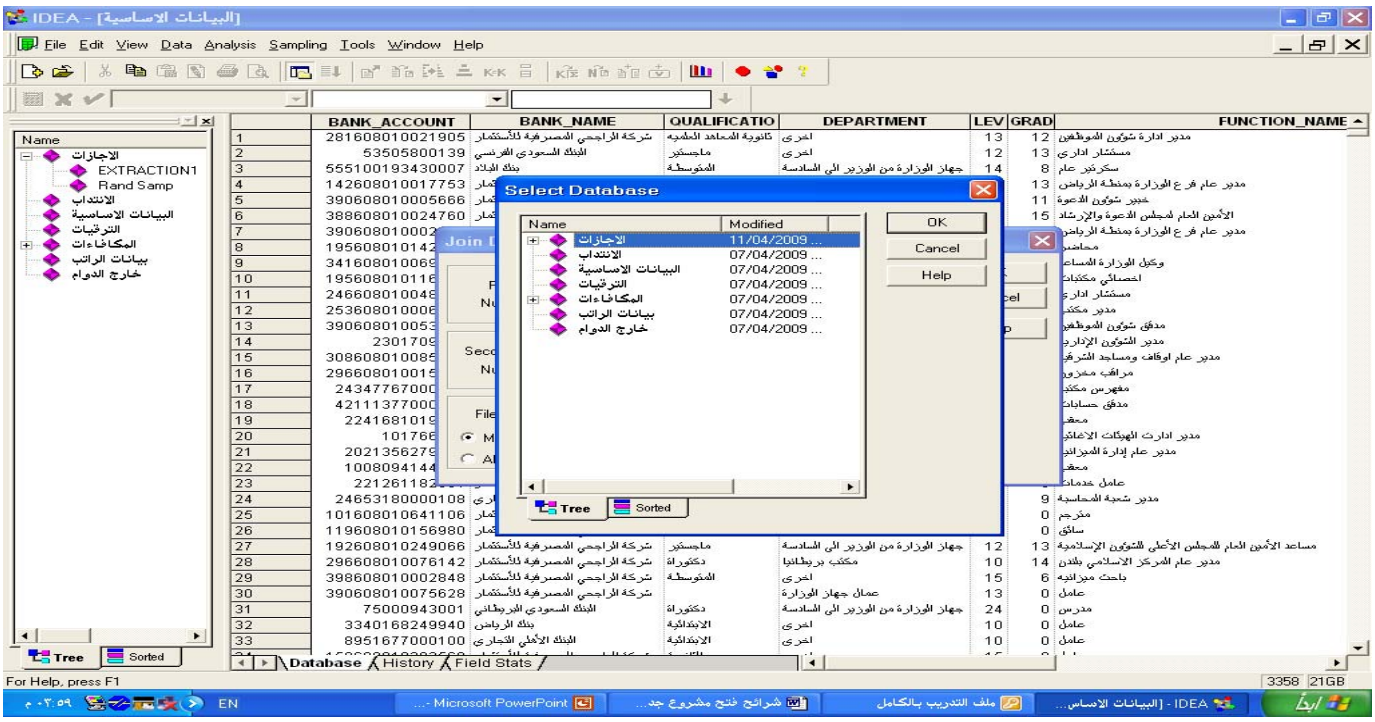
1- فتح الملف الرئيسي
2- اختر الأمر Join Database من القائمة File كما هو موضح في الشكل التالي



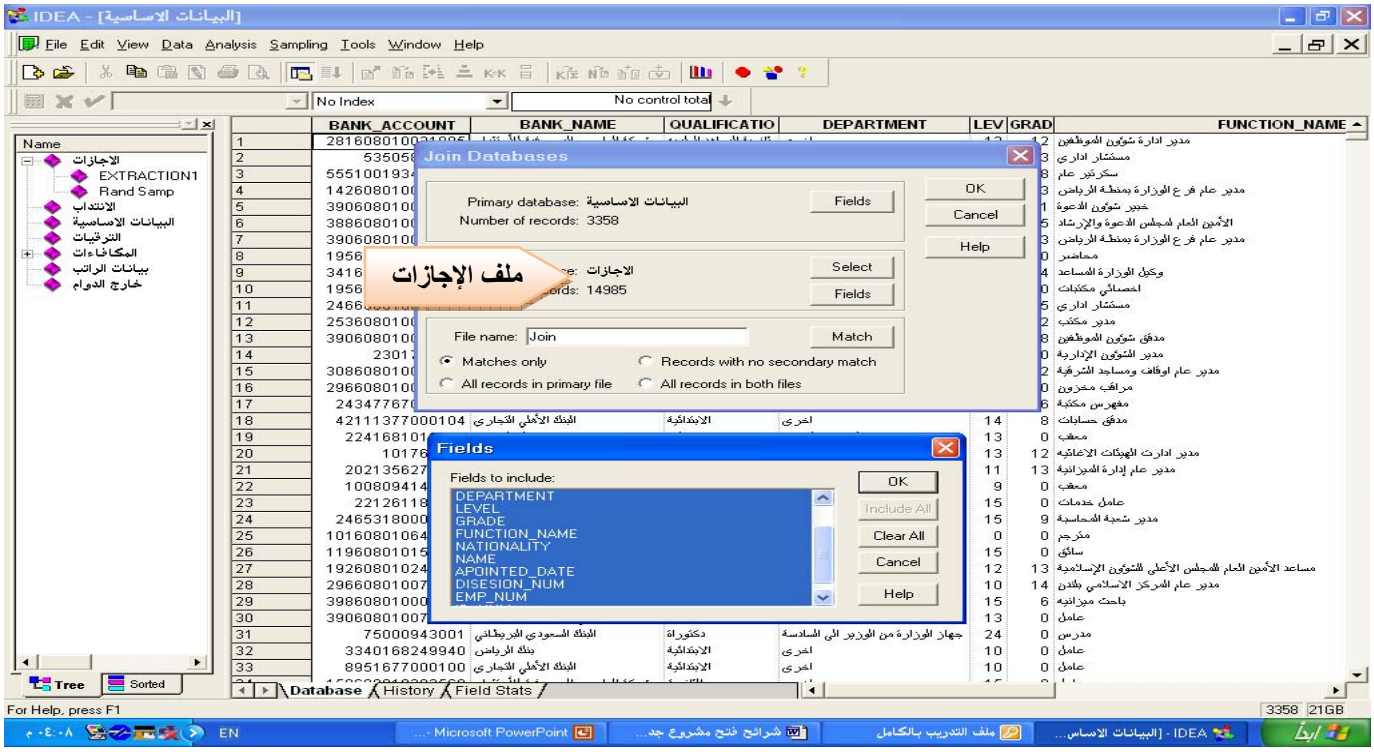
بعد ذلك تظهر الشاشة التالية :



بعد ذلك يتم اختيار الملف الأول (الرئيسي) كما هو موضح في ملف البيانات الأساسية , وبعد ذلك يتم تحديد الحقول المراد اختيارها من الملف عن طريق Field من المربع الموضح أعلاه , وبعد ذلك يتم الضغط على Select لتحديد الملف الثاني المراد ربطه بالملف الرئيسي كما هو موضح في الشكل التالي :

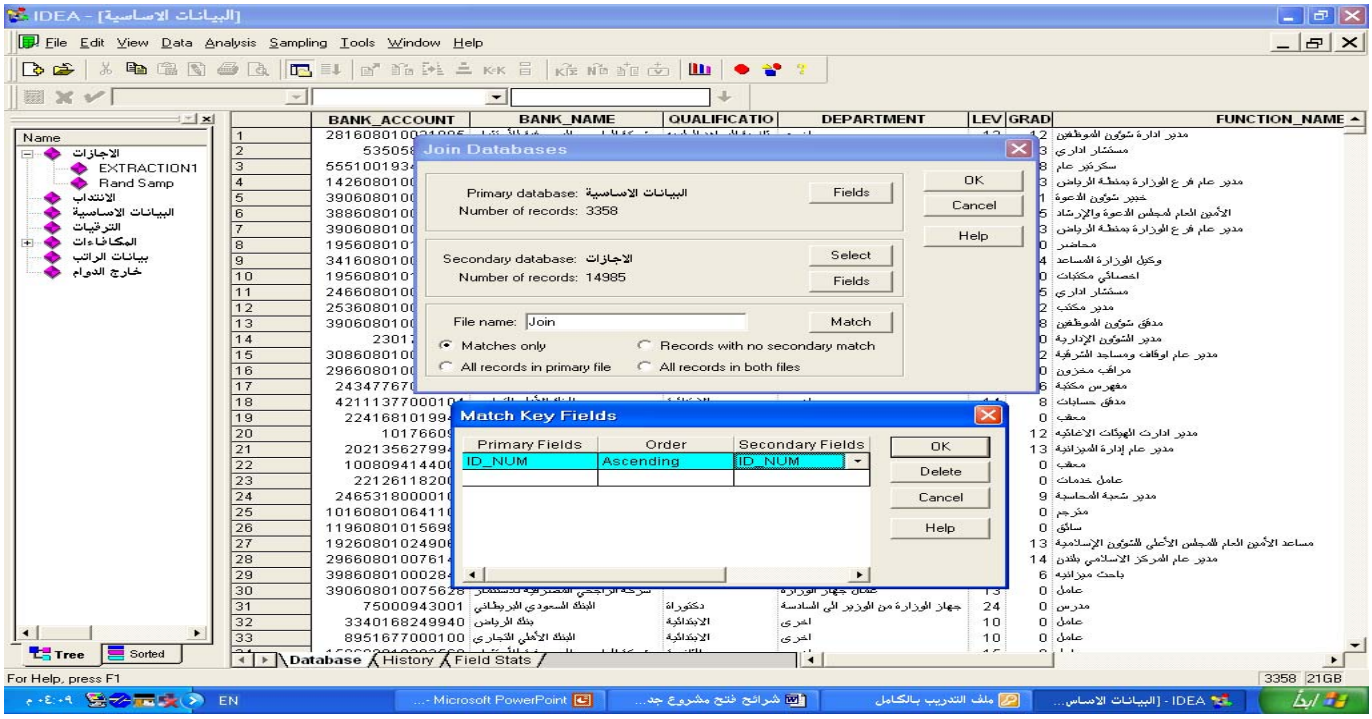


وبعد ذلك تم اختيار ملف الإجازات كملف ثاني لربطه بالملف الرئيسي ونضغط OK وستظهر الشاشة التالية :

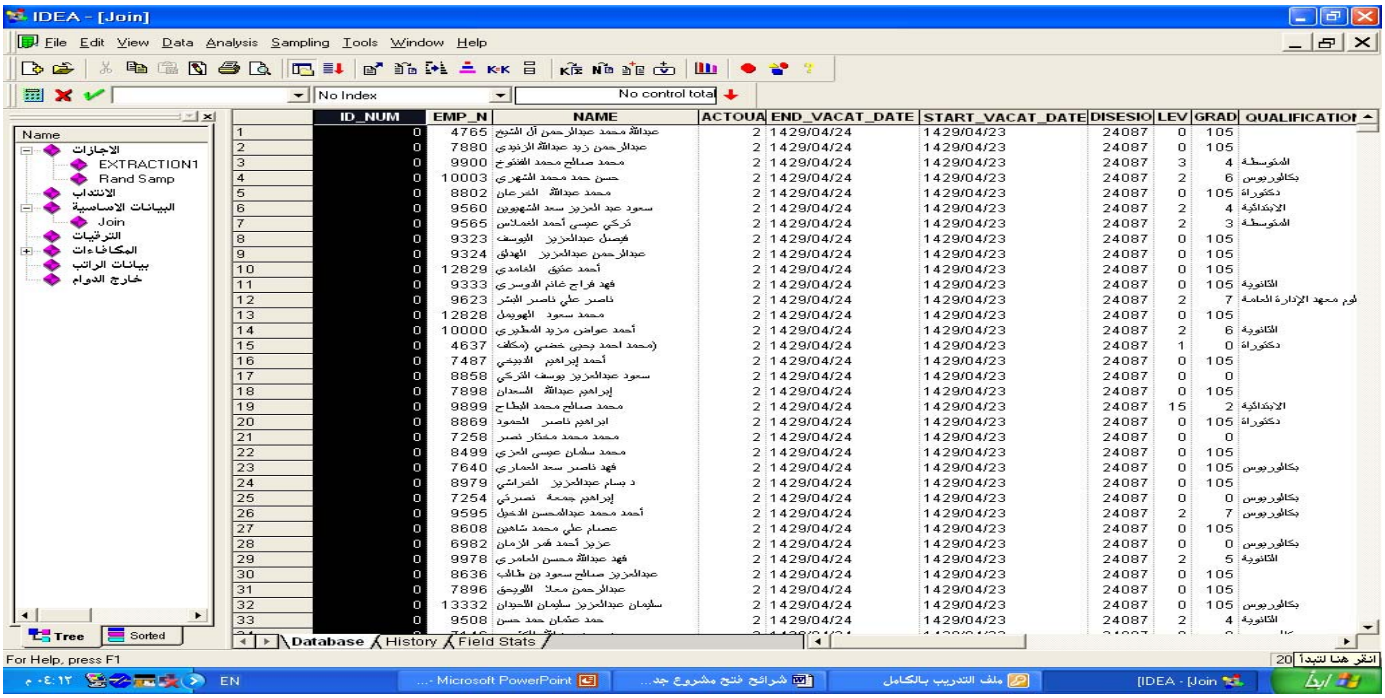


نلاحظ أن ملف الإجازات ظهر كملف ثاني , وبعد ذلك يمكننا أيضاً تحديد الحقول المراد إظهارها في التقرير من خلال Field التابع لملف الإجازات حتى يتم اختيار الحقول المهمة فقط , بعد ذلك نقوم باختيار Match من المربع لربط الملفين ببعضهما البعض عن طريق تحديد المفتاح الرئيسي بين الملفين والذي يتمثل برقم السجل المدني .

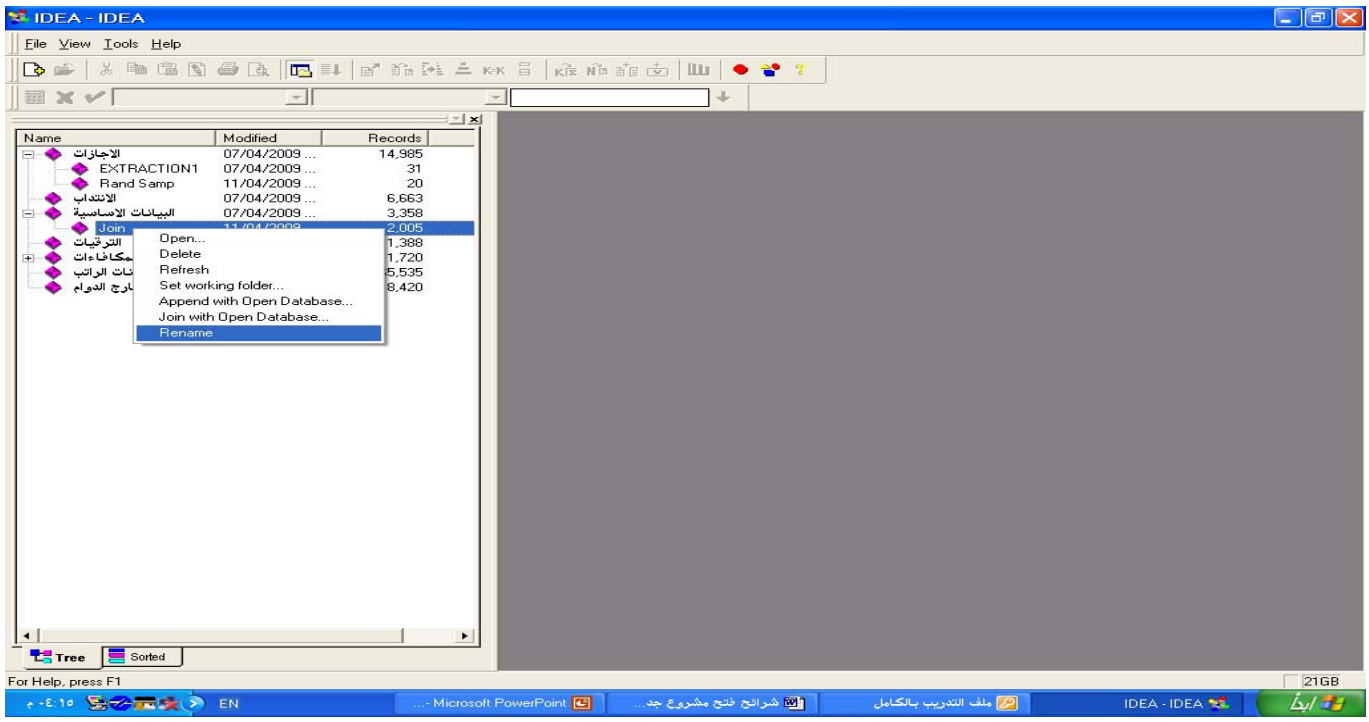
ويمكننا أيضاً اختيار مفاتيح أخرى مثل رقم الموظف واسم الموظف كما هو موضح في الشكل التالي:



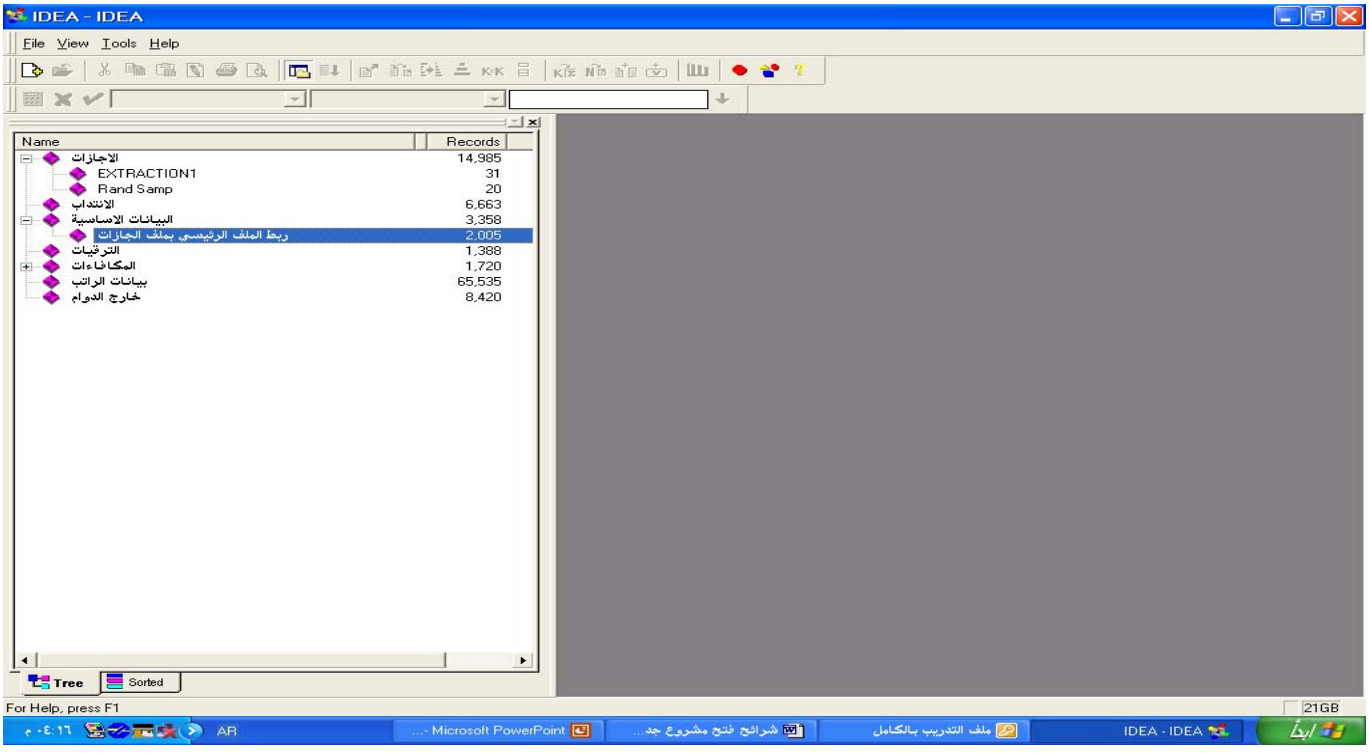
بعد ذلك نضغط OK ليتم الربط بين الملفين وستظهر النتيجة التالية :



ونلاحظ ظهور جميع الحقول التي تم اختيارها من الملفين في ملف واحد يسمى Join وبإمكاننا تغير اسم الملف إلى اسم آخر مثل **(ربط الملف الرئيسي بملف الإجازات)** وذلك بعد إغلاق الملف ثم إعادة التسمية كما هو موضح في الشكل التالي :



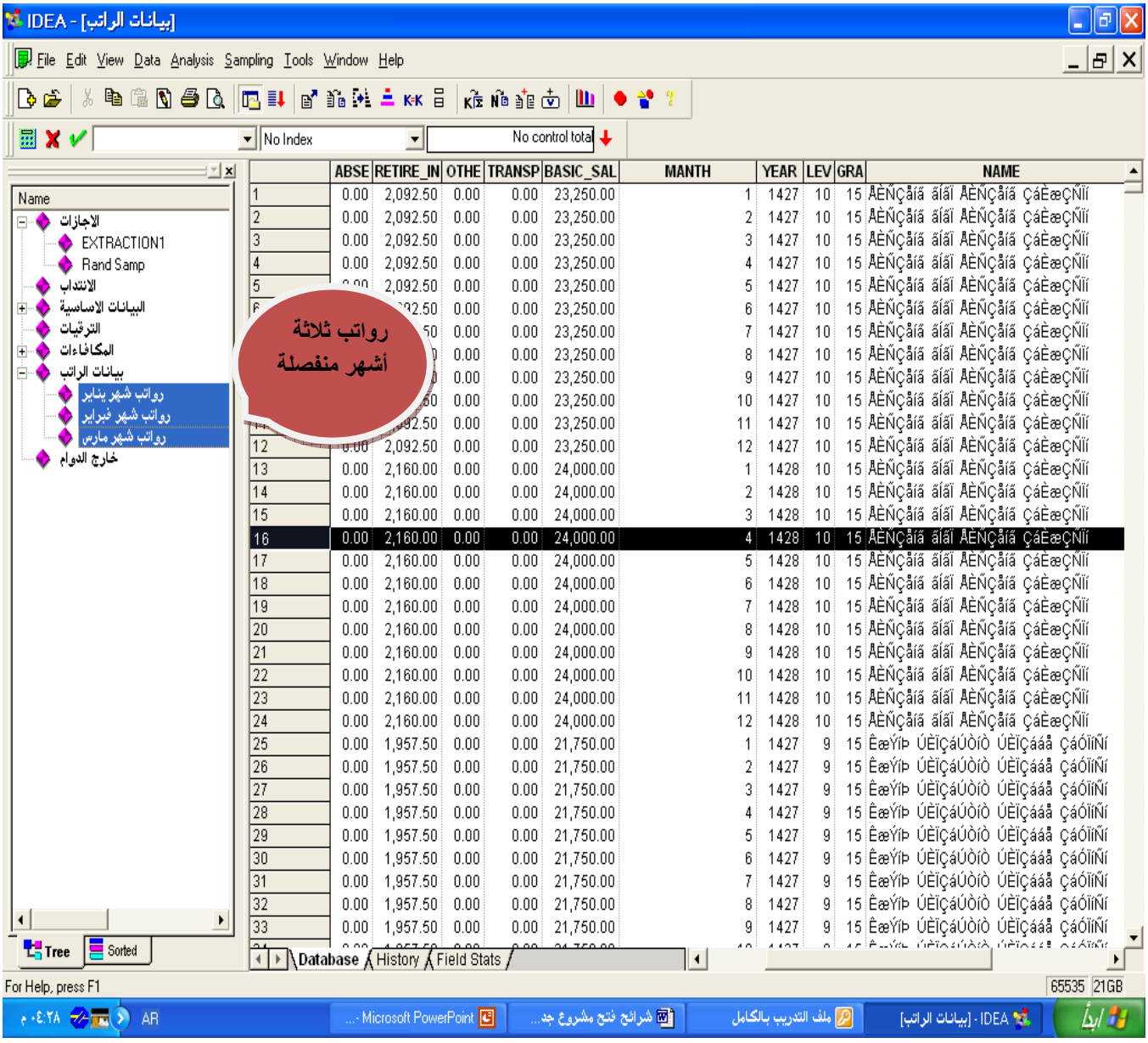
ومن ثم تسمية الملف كما هو موضح في الشكل التالي :



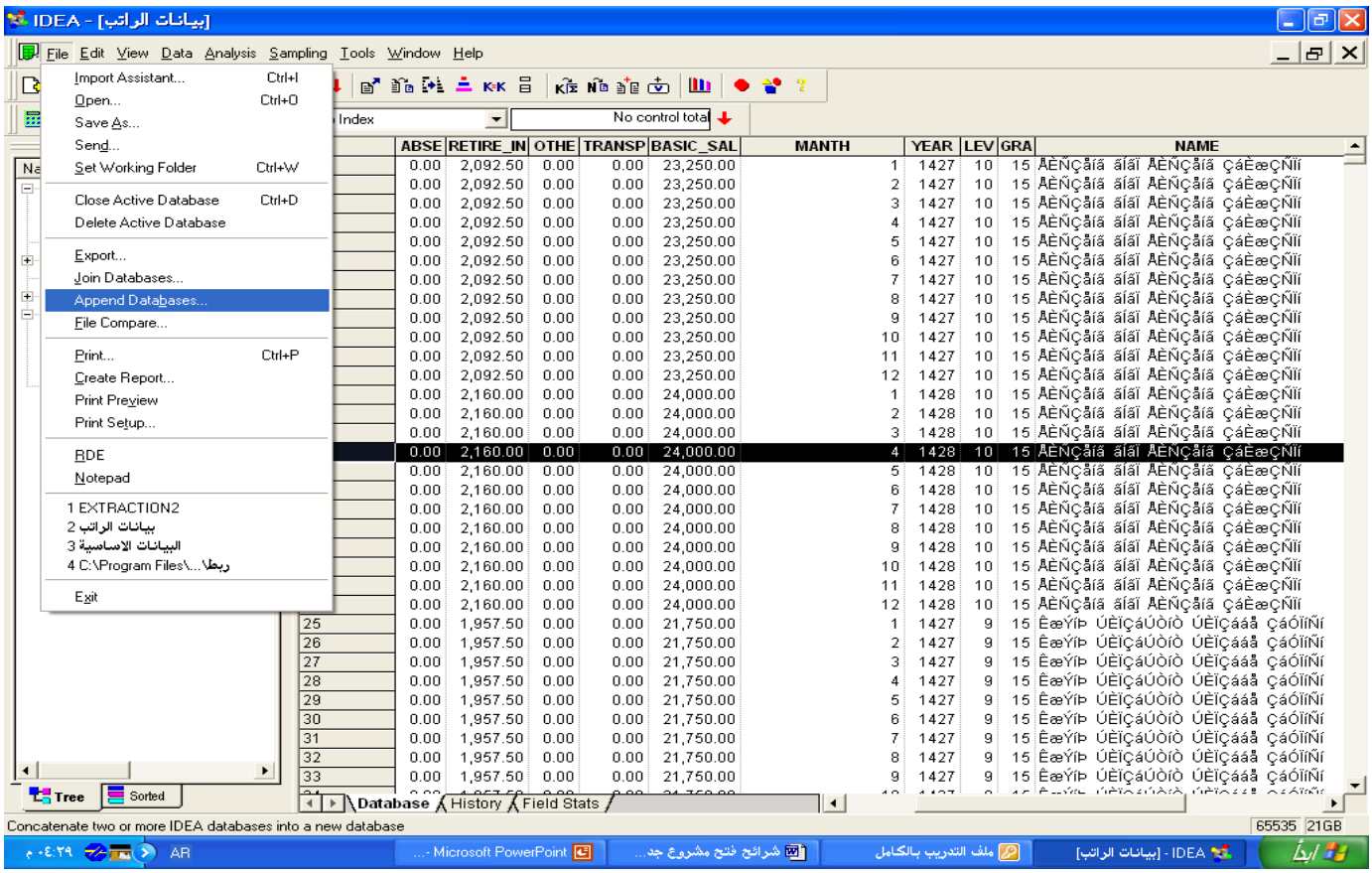
تطبيق رقم

الأمر append database

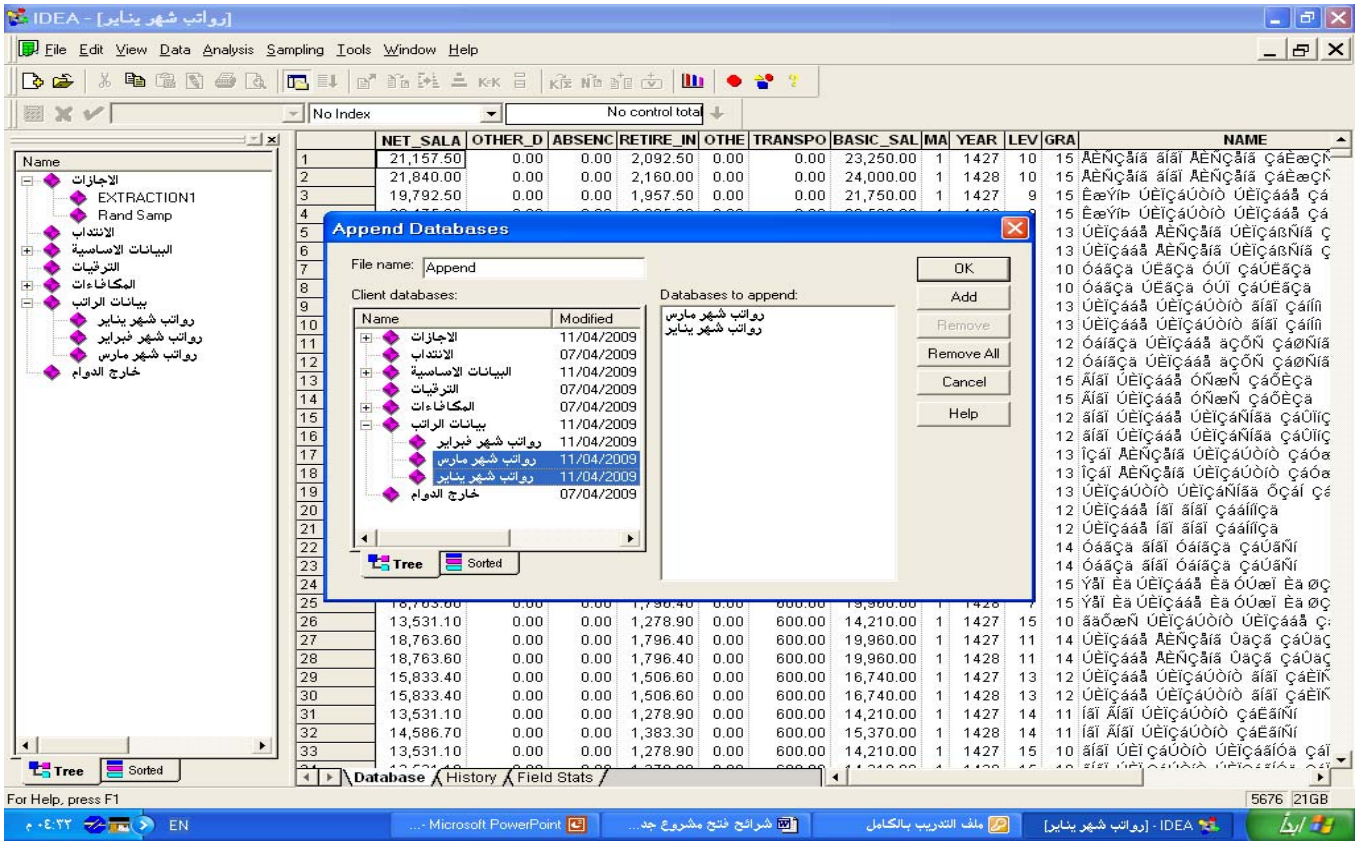
يقوم هذا الأمر بإضافة ودمج أكثر من ملف مع بعضهما تحمل نفس الحقول والخصائص (النوع والطول) ومثال ذلك ربط ملفات رواتب ثلاثة أشهر منفصلة لتكون مع بعضها في ملف واحد , والشاشات التالية توضح ذلك :



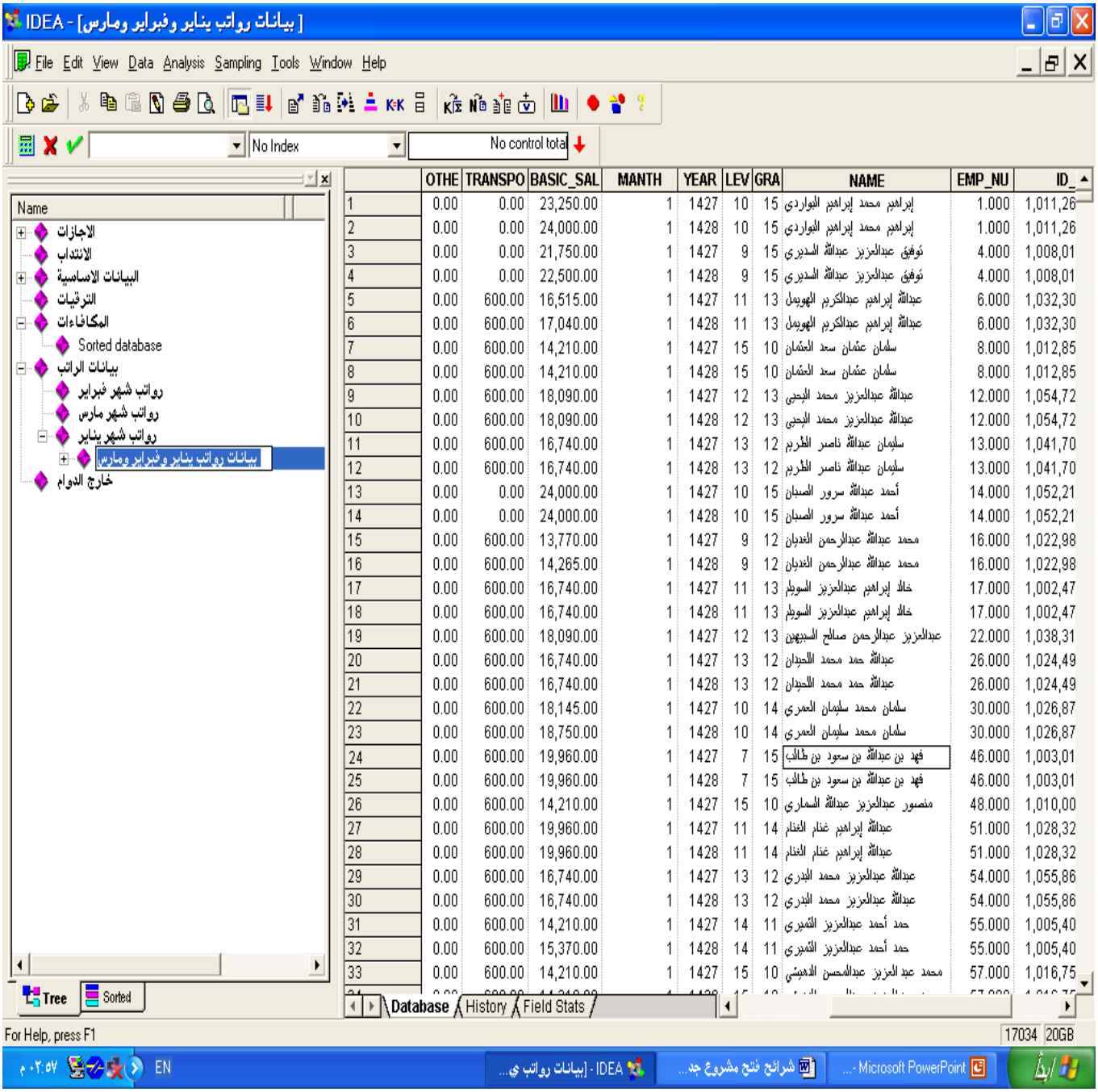
نلاحظ وجود رواتب ثلاثة أشهر منفصلة للأشهر يناير , فبراير , مارس كما هو موضح أعلاه , بعد ذلك يمكننا ربطها في ملف واحد , حيث نقوم بفتح الملف الأول ثم نقوم باختيار الأمر Append Database من القائمة File كما هو موضح أدناه :



بعد ذلك ستظهر الشاشة التالية :



بعد فتح الملف الأول والذي يمثل رواتب شهر يناير , نقوم بالضغط على Add لإضافة الشهرين التاليين فبراير ومارس وستظهر في الجانب المقابل للجدول , ثم نضغط OK ليتم دمجها في ملف واحد ونغير اسمه من Append إلى بيانات رواتب يناير وفبراير ومارس كما هو موضح أدناه :



	OTHE	TRANSPO	BASIC_SAL	MANTH	YEAR	LEV	GRA	NAME	EMP_NU	ID_
1	0.00	0.00	23,250.00	1	1427	10	15	إبراهيم محمد إبراهيم البواردي	1.000	1,011,26
2	0.00	0.00	24,000.00	1	1428	10	15	إبراهيم محمد إبراهيم البواردي	1.000	1,011,26
3	0.00	0.00	21,750.00	1	1427	9	15	توفيق عبدالعزيز عبدالله السديري	4.000	1,008,01
4	0.00	0.00	22,500.00	1	1428	9	15	توفيق عبدالعزيز عبدالله السديري	4.000	1,008,01
5	0.00	600.00	16,515.00	1	1427	11	13	عبدالله إبراهيم عبدالكريم الهويمل	6.000	1,032,30
6	0.00	600.00	17,040.00	1	1428	11	13	عبدالله إبراهيم عبدالكريم الهويمل	6.000	1,032,30
7	0.00	600.00	14,210.00	1	1427	15	10	سلمان عثمان سعد العثمان	8.000	1,012,85
8	0.00	600.00	14,210.00	1	1428	15	10	سلمان عثمان سعد العثمان	8.000	1,012,85
9	0.00	600.00	18,090.00	1	1427	12	13	عبدالله عبدالعزيز محمد البحيي	12.000	1,054,72
10	0.00	600.00	18,090.00	1	1428	12	13	عبدالله عبدالعزيز محمد البحيي	12.000	1,054,72
11	0.00	600.00	16,740.00	1	1427	13	12	سليمان عبدالله ناصر الطريم	13.000	1,041,70
12	0.00	600.00	16,740.00	1	1428	13	12	سليمان عبدالله ناصر الطريم	13.000	1,041,70
13	0.00	0.00	24,000.00	1	1427	10	15	أحمد عبدالله سرور الصبان	14.000	1,052,21
14	0.00	0.00	24,000.00	1	1428	10	15	أحمد عبدالله سرور الصبان	14.000	1,052,21
15	0.00	600.00	13,770.00	1	1427	9	12	محمد عبدالله عبدالرحمن الغديان	16.000	1,022,98
16	0.00	600.00	14,265.00	1	1428	9	12	محمد عبدالله عبدالرحمن الغديان	16.000	1,022,98
17	0.00	600.00	16,740.00	1	1427	11	13	خالد إبراهيم عبدالعزيز السويلم	17.000	1,002,47
18	0.00	600.00	16,740.00	1	1428	11	13	خالد إبراهيم عبدالعزيز السويلم	17.000	1,002,47
19	0.00	600.00	18,090.00	1	1427	12	13	عبدالعزيز عبدالرحمن صالح السبيهين	22.000	1,038,31
20	0.00	600.00	16,740.00	1	1427	13	12	عبدالله حمد محمد اللحيدان	26.000	1,024,49
21	0.00	600.00	16,740.00	1	1428	13	12	عبدالله حمد محمد اللحيدان	26.000	1,024,49
22	0.00	600.00	18,145.00	1	1427	10	14	سلمان محمد سليمان العمري	30.000	1,026,87
23	0.00	600.00	18,750.00	1	1428	10	14	سلمان محمد سليمان العمري	30.000	1,026,87
24	0.00	600.00	19,960.00	1	1427	7	15	فهد بن عبدالله بن سعود بن طالب	46.000	1,003,01
25	0.00	600.00	19,960.00	1	1428	7	15	فهد بن عبدالله بن سعود بن طالب	46.000	1,003,01
26	0.00	600.00	14,210.00	1	1427	15	10	منصور عبدالعزيز عبدالله السماري	48.000	1,010,00
27	0.00	600.00	19,960.00	1	1427	11	14	عبدالله إبراهيم غنام الغنام	51.000	1,028,32
28	0.00	600.00	19,960.00	1	1428	11	14	عبدالله إبراهيم غنام الغنام	51.000	1,028,32
29	0.00	600.00	16,740.00	1	1427	13	12	عبدالله عبدالعزيز محمد البدري	54.000	1,055,86
30	0.00	600.00	16,740.00	1	1428	13	12	عبدالله عبدالعزيز محمد البدري	54.000	1,055,86
31	0.00	600.00	14,210.00	1	1427	14	11	حمد أحمد عبدالعزيز الشبيري	55.000	1,005,40
32	0.00	600.00	15,370.00	1	1428	14	11	حمد أحمد عبدالعزيز الشبيري	55.000	1,005,40
33	0.00	600.00	14,210.00	1	1427	15	10	محمد عبد العزيز عبدالمحسن الدهيشي	57.000	1,016,75

تطبيق رقم

بعض معادلات الفحص **Criteria**

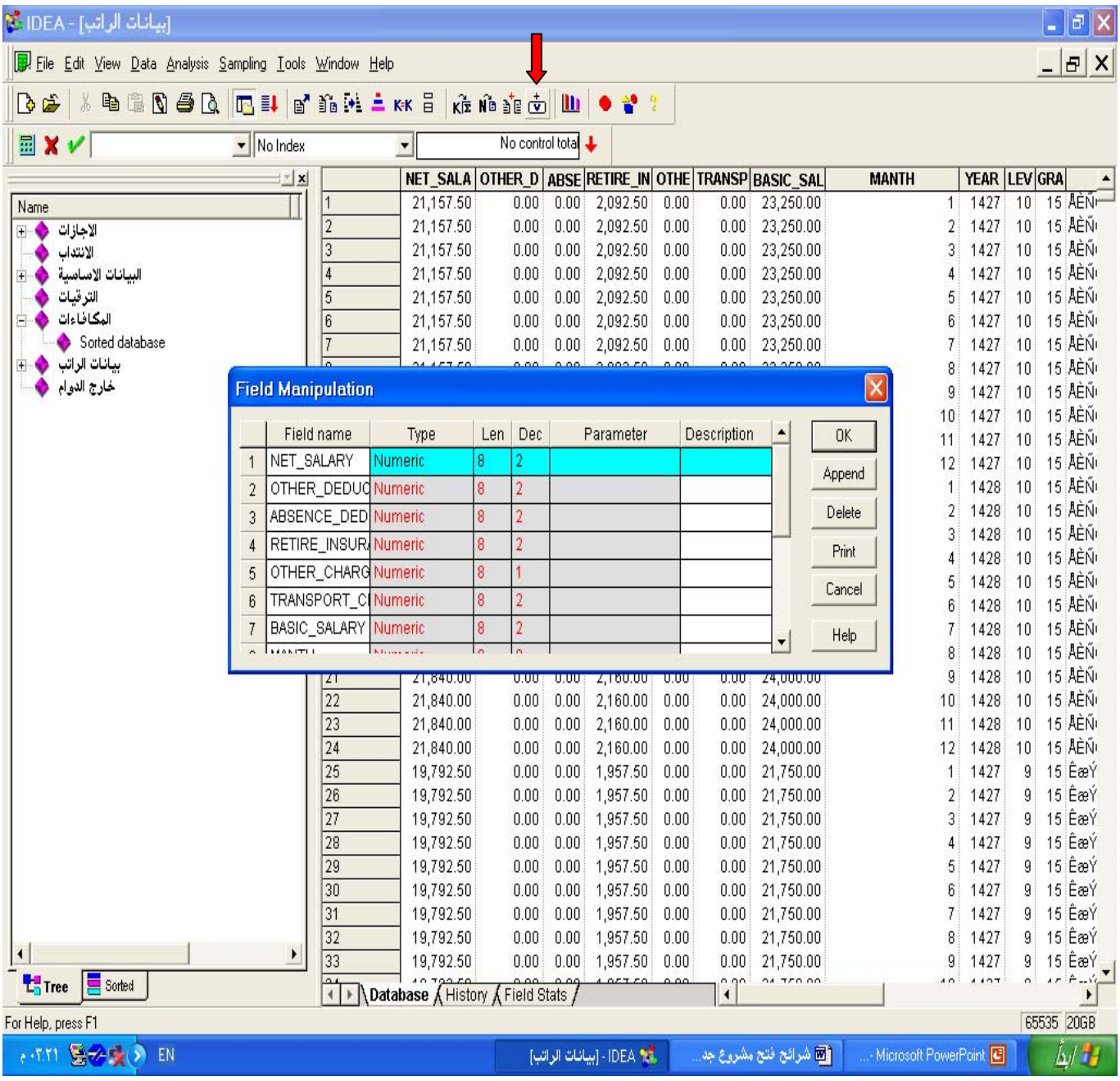
لكل معادلة شروط ومعايير ويتم تركيبها بناءً على الأفكار والاختبارات المراد تنفيذها , ومثال للاختبارات التي يمكن تنفيذها من خلال البرنامج التحليلي IDEA

- ✓ للتأكد من حساب صافي الراتب المصروف في الجهة محل الفحص بشكل صحيح .
- ✓ للتأكد من حساب بدل النقل بشكل صحيح .
- ✓ للتأكد من حساب التقاعد بشكل صحيح .
- ✓ للتأكد من حساب خارج الدوام .
- ✓ للتأكد من حساب بدل الانتداب .
- ✓ للتأكد من حساب المكافآت والعلاوات بشكل صحيح .
- ✓ للتأكد من احتساب مدة الإجازة بشكل صحيح .
- ✓ للتأكد من عدم تداخل الإجازة مع خارج الدوام أو الانتداب مع خارج الدوام .
- ✓ للتأكد من عدم تكرار الراتب .
- ✓ لتغيير نوع الحقل من حرفي إلى تاريخي لحساب فترة الانتداب والإجازة من خلال إضافة حقل جديد يمثل عدد الأيام .
- ✓ ومن خلال الأفكار السابقة سوف نتطرق لبعضها :

للتأكد من حساب صافي الراتب المصروف في الجهة محل الفحص بشكل صحيح نقوم بالآتي:

- ✓ نقوم بإنشاء حقل جديد وذلك لوضع القيمة التي سيتم احتسابها من خلال البرنامج
- ✓ نقوم بكاتبة المعادلة لحساب صافي الراتب
- ✓ يتم مقارنة ما تم احتسابه مع ما هو موجود فعلاً وتحديد الفرق ومن خلال الشاشات التالية سيتم توضيح هذا المثال :

- نقوم بفتح ملف الرواتب ثم نقوم بالضغط على الرمز (V) كما هو موضح أدناه تحت السهم وسوف تظهر الشاشة التالية .



بعد ذلك نقوم بالضغط على Append , وبعد سوف يظهر سطر جديد يمثل حقل فارغ في قاعدة البيانات ونقوم بتعبئته كالتالي :

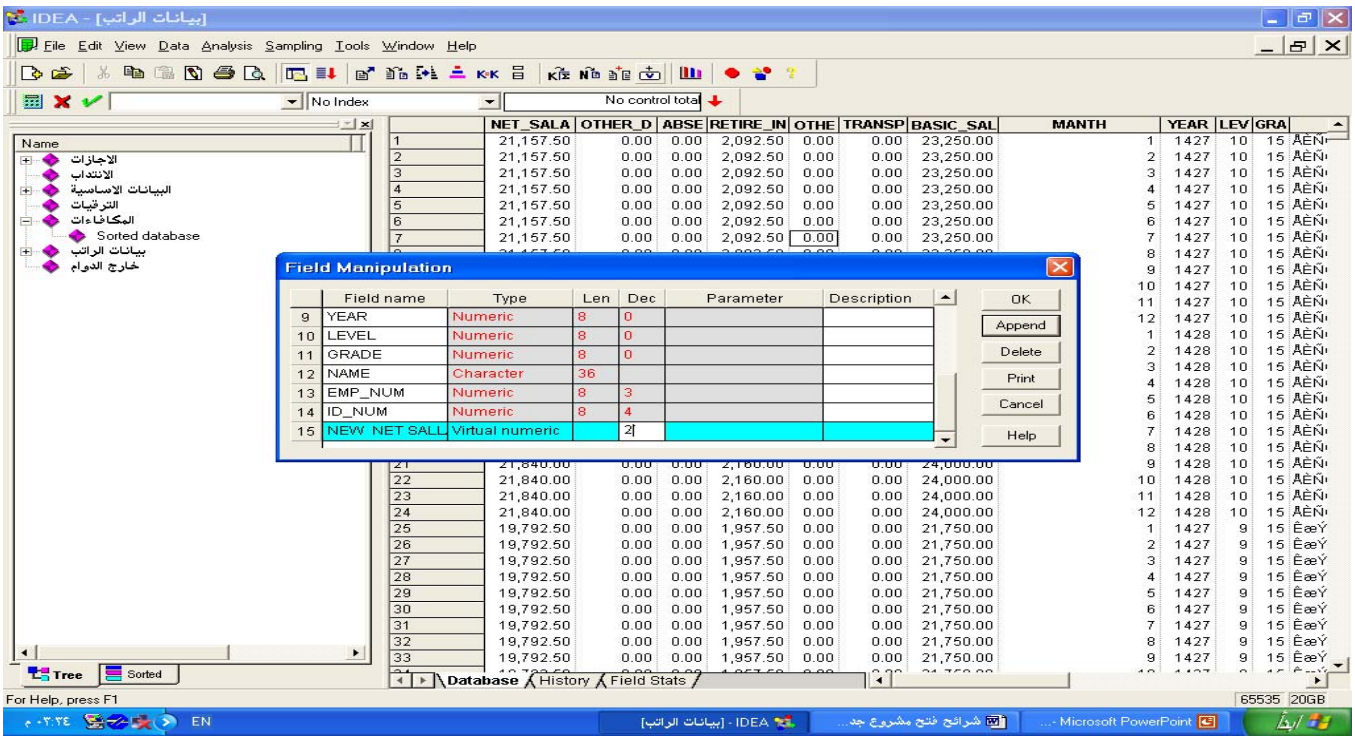
Field Name اسم الحقل

Type name نوع الحقل

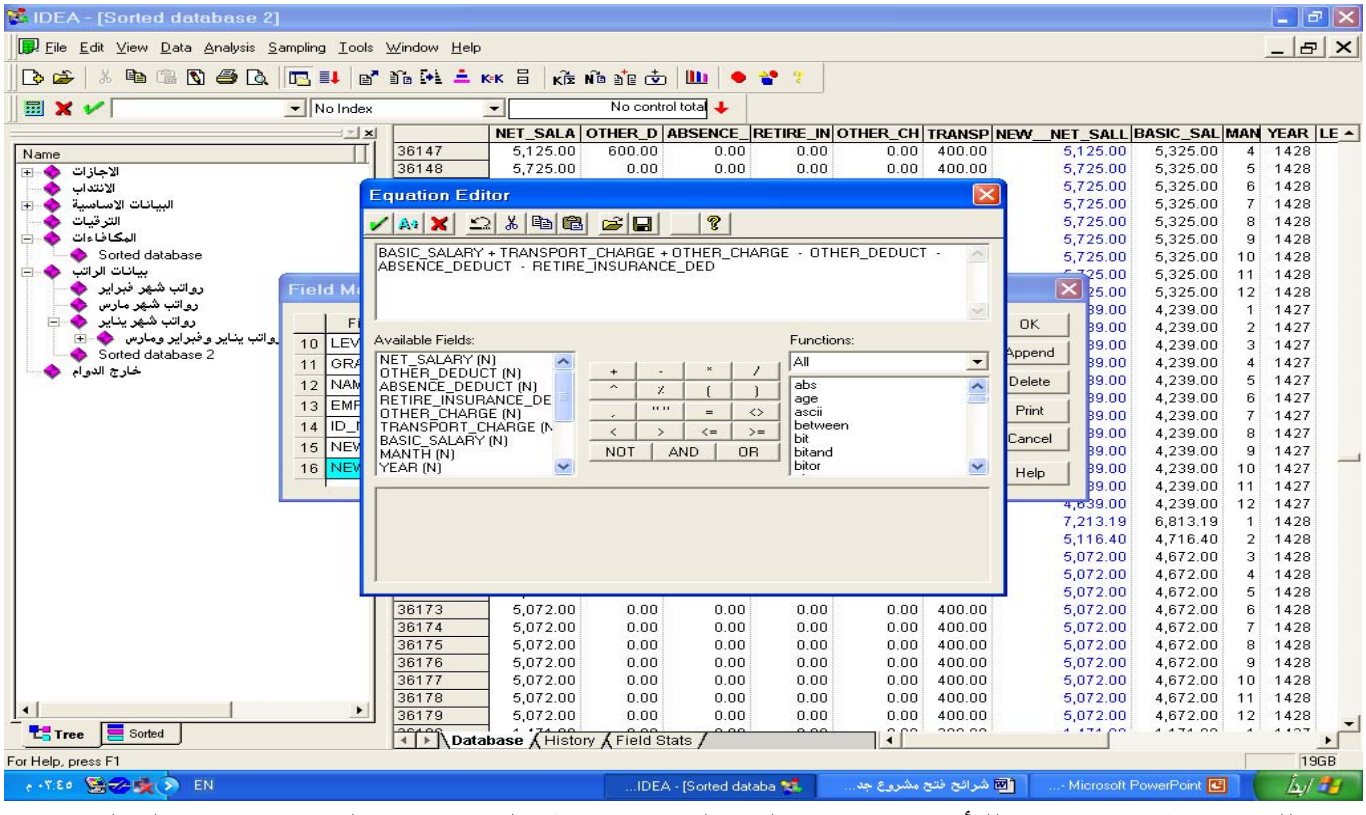
Dec الفاصلة العشرية

Parameter كتابة المعادلة

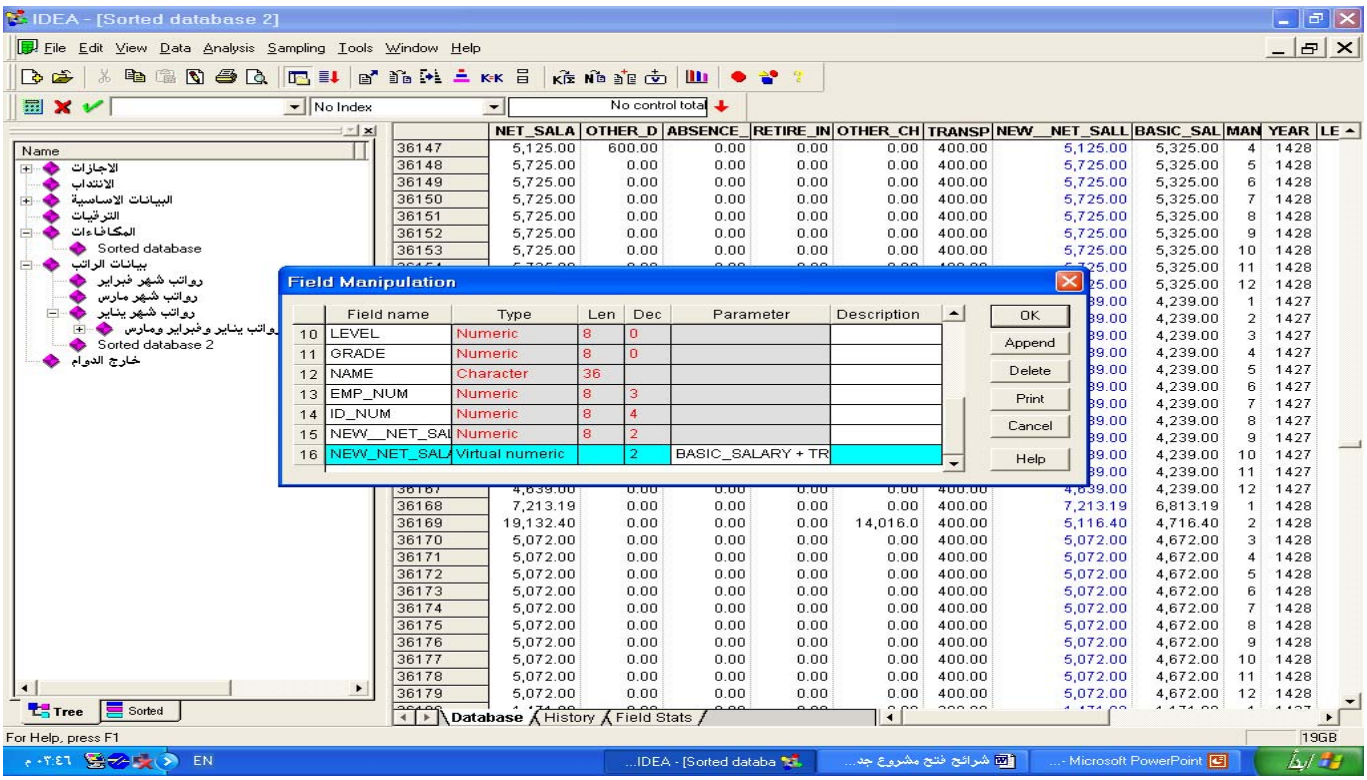
ويتم تعبئة البيانات كما هو موضح أدناه .



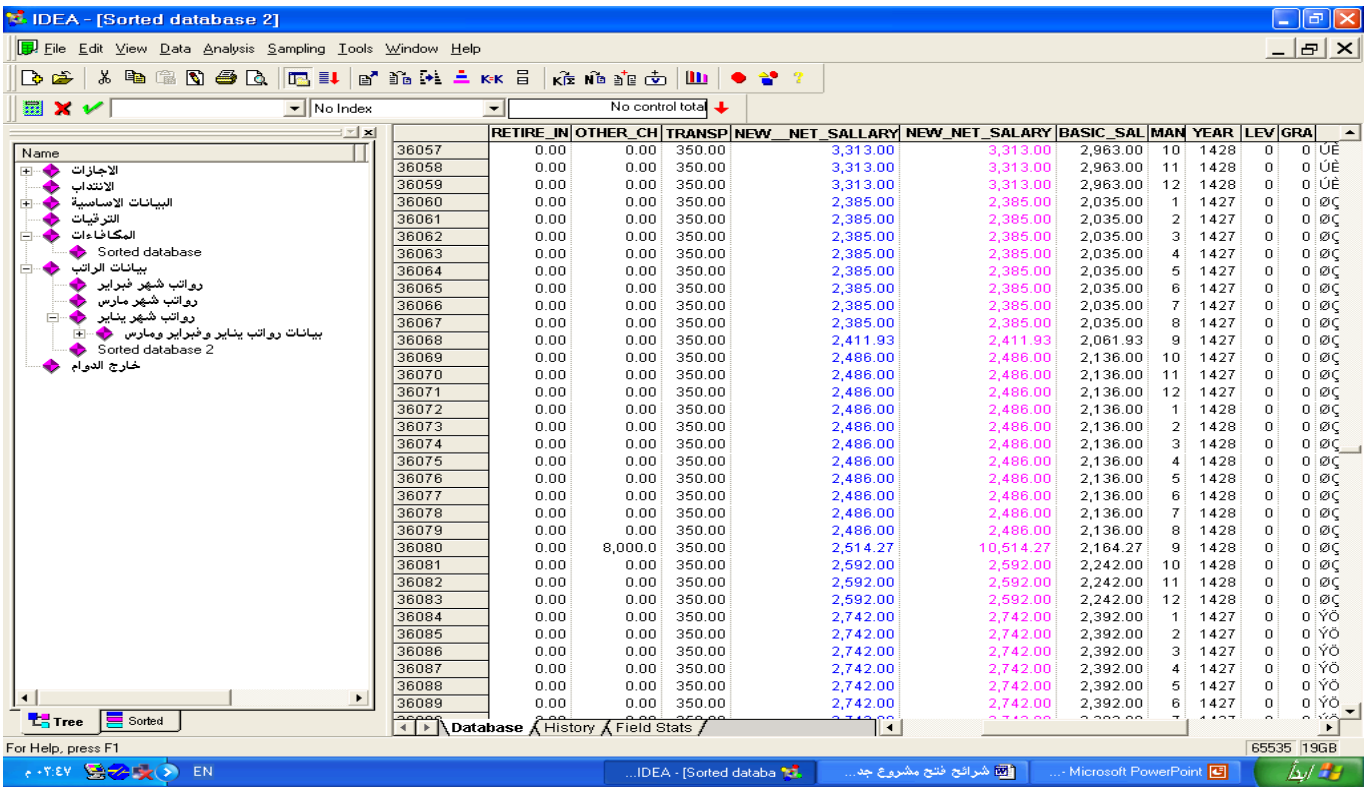
بعد ذلك نضغط على Parameter لكتابة المعادلة كما هو موضح في الشاشة التالية :



بعد ذلك نضغط علامة +A للتأكد من صحة المعادلة ثم نضغط على علامة (الصح) لإتمام العملية وسوف تظهر النتيجة كما هو موضح في الشاشة التالية :

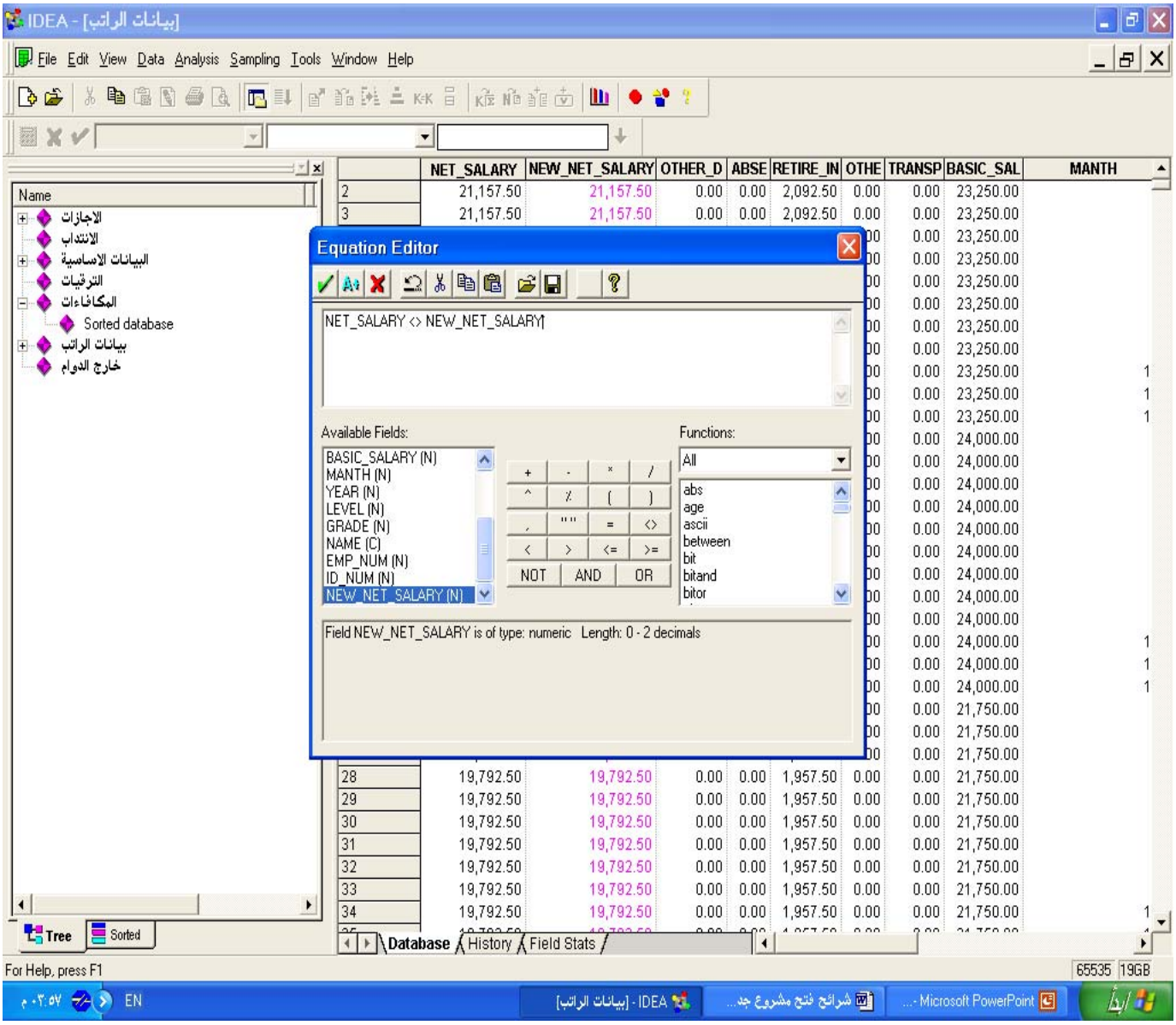


نقوم بالضغط على OK وسوف تظهر النتيجة التالية :

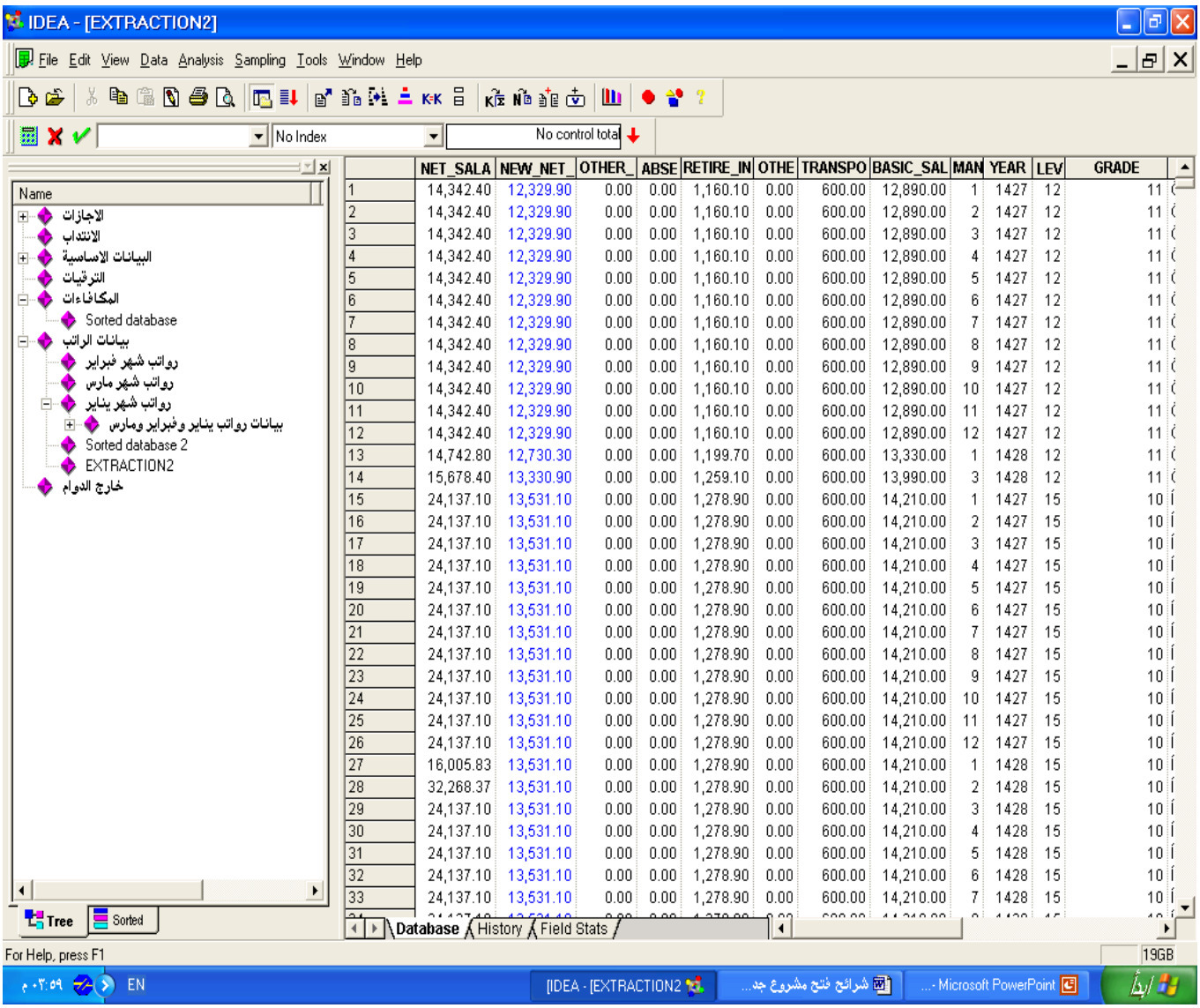


نلاحظ أنه ظهر الحقل الجديد الذي تمت إضافته واسمه New Net Salary بعد ذلك نقوم بمقارنة الحقل الموجود والمعطى من قبل الجهة مع الحقل الذي تم احتسابه كما سوف نوضحه في المعادلة التالية :

نذهب إلى الأمر Extraction من خلال القائمة Data ونضغط على الحاسبة في داخل المربع ونضع المعادلة التالية كما هو موضح أدناه :



بعد ذلك نضغط علامة +A للتأكد من صحة المعادلة ثم نضغط على علامة الصح ثم موافق لإتمام العملية وسوف تظهر النتيجة كما هو موضح في الشاشة التالية :



	NET_SALA	NEW_NET_	OTHER_	ABSE	RETIRE_IN	OTHE	TRANSPO	BASIC_SAL	MAN	YEAR	LEV	GRADE
1	14,342.40	12,329.90	0.00	0.00	1,160.10	0.00	600.00	12,890.00	1	1427	12	11
2	14,342.40	12,329.90	0.00	0.00	1,160.10	0.00	600.00	12,890.00	2	1427	12	11
3	14,342.40	12,329.90	0.00	0.00	1,160.10	0.00	600.00	12,890.00	3	1427	12	11
4	14,342.40	12,329.90	0.00	0.00	1,160.10	0.00	600.00	12,890.00	4	1427	12	11
5	14,342.40	12,329.90	0.00	0.00	1,160.10	0.00	600.00	12,890.00	5	1427	12	11
6	14,342.40	12,329.90	0.00	0.00	1,160.10	0.00	600.00	12,890.00	6	1427	12	11
7	14,342.40	12,329.90	0.00	0.00	1,160.10	0.00	600.00	12,890.00	7	1427	12	11
8	14,342.40	12,329.90	0.00	0.00	1,160.10	0.00	600.00	12,890.00	8	1427	12	11
9	14,342.40	12,329.90	0.00	0.00	1,160.10	0.00	600.00	12,890.00	9	1427	12	11
10	14,342.40	12,329.90	0.00	0.00	1,160.10	0.00	600.00	12,890.00	10	1427	12	11
11	14,342.40	12,329.90	0.00	0.00	1,160.10	0.00	600.00	12,890.00	11	1427	12	11
12	14,342.40	12,329.90	0.00	0.00	1,160.10	0.00	600.00	12,890.00	12	1427	12	11
13	14,742.80	12,730.30	0.00	0.00	1,199.70	0.00	600.00	13,330.00	1	1428	12	11
14	15,678.40	13,330.90	0.00	0.00	1,259.10	0.00	600.00	13,990.00	3	1428	12	11
15	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	1	1427	15	10
16	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	2	1427	15	10
17	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	3	1427	15	10
18	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	4	1427	15	10
19	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	5	1427	15	10
20	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	6	1427	15	10
21	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	7	1427	15	10
22	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	8	1427	15	10
23	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	9	1427	15	10
24	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	10	1427	15	10
25	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	11	1427	15	10
26	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	12	1427	15	10
27	16,005.83	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	1	1428	15	10
28	32,268.37	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	2	1428	15	10
29	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	3	1428	15	10
30	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	4	1428	15	10
31	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	5	1428	15	10
32	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	6	1428	15	10
33	24,137.10	13,531.10	0.00	0.00	1,278.90	0.00	600.00	14,210.00	7	1428	15	10

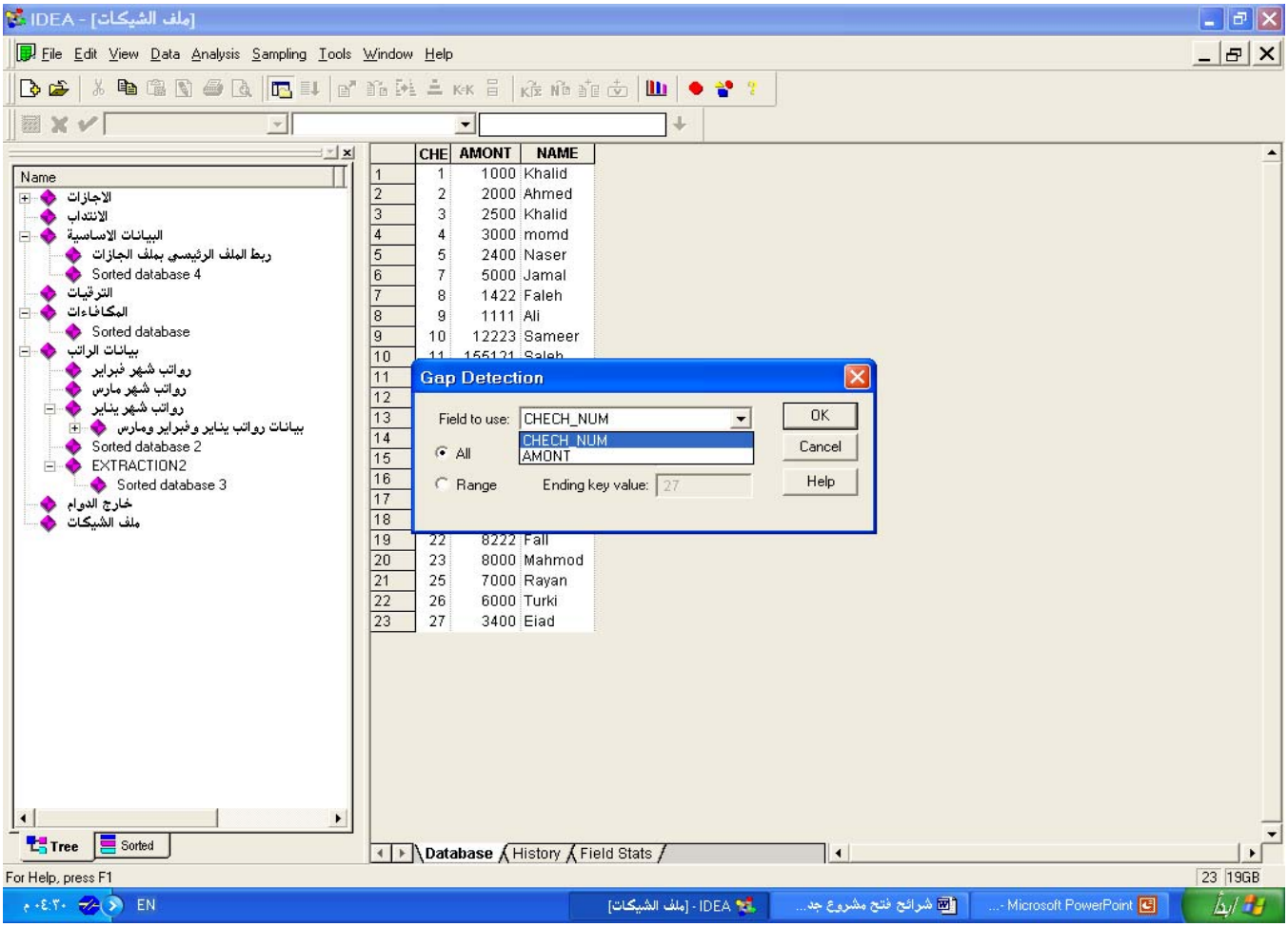
نلاحظ أنه ظهرت بعض الاختلافات في صافي الراتب .

تطبيق رقم

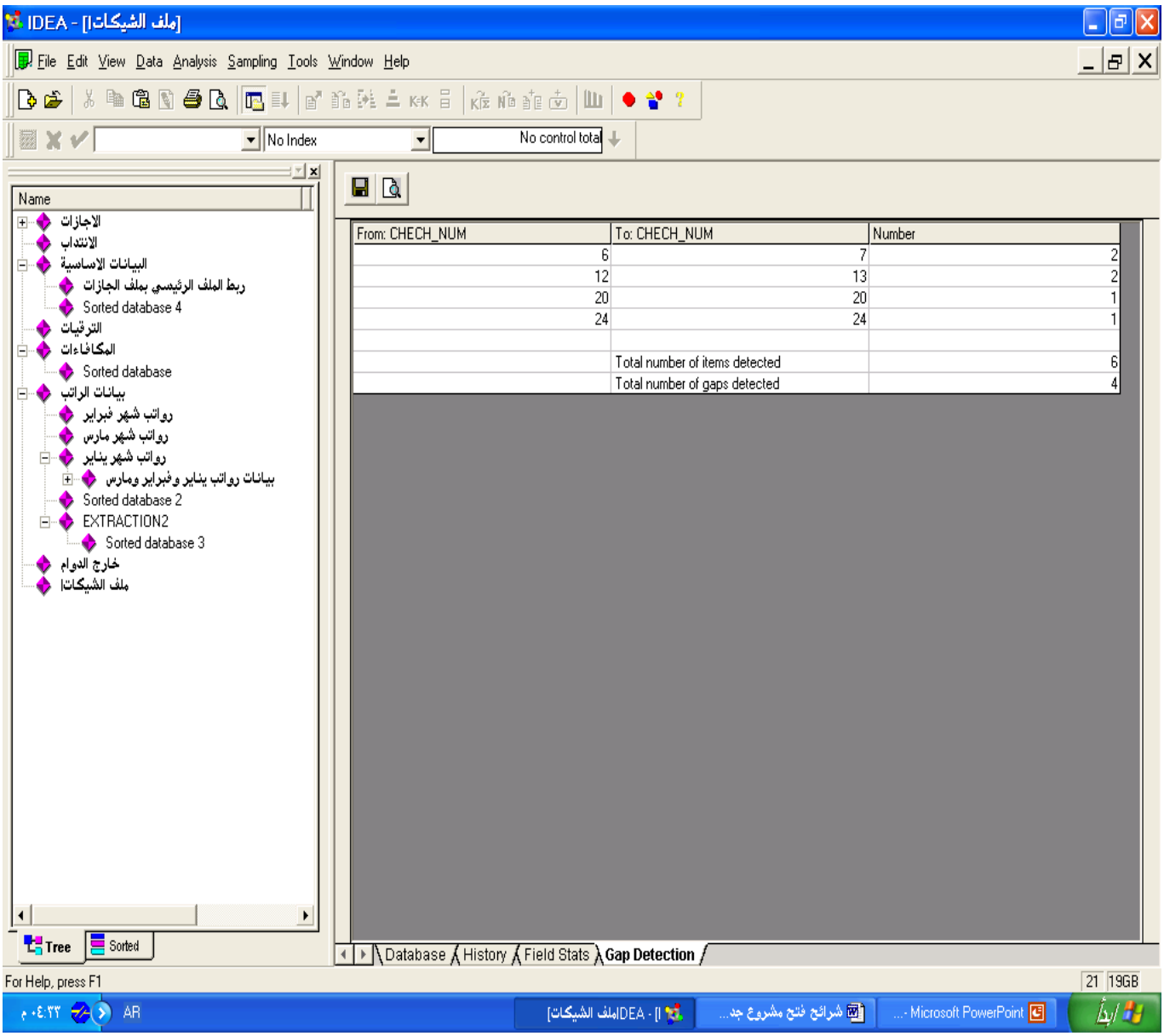
الأمر GAP الفجوات

يقوم هذا الأمر بفحص الثغرات الموجودة في ملف الشيكات أو الفواتير مثلاً وأي ملف يوجد فيه تسلسل أرقام ونريد معرفة النقص الموجود في هذا التسلسل مع ضرورة أن يكون الحقل المراد فحصه رقمي , والشاشة التالية توضح خطوات الفحص وتطبيق هذا الأمر :

نقوم بفتح الملف الخاص بالشيكات وبعده نقوم باختيار الأمر Gap من خلال القائمة Data وسوف تظهر الشاشة التالية :



بعد ذلك نحدد الحقل المراد فحصه تسلسلياً كما هو موضح أعلاه ثم نضغط OK للحصول على النتيجة التالية :

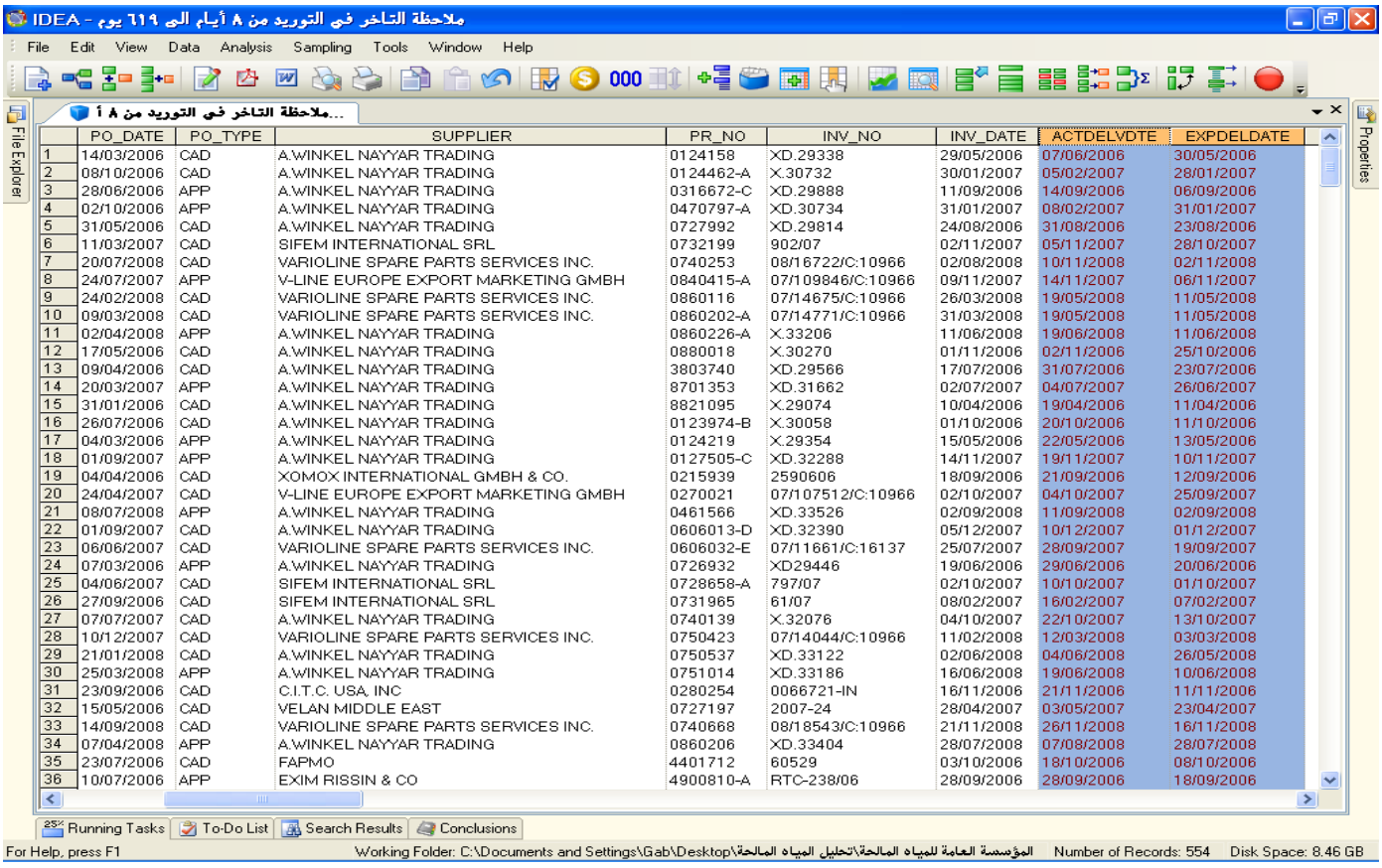


نلاحظ في الشاشة السابقة عدد الشيكات المفقودة وإجمالي الشيكات المفقودة وعدد الفجوات الموجودة في الملف .

تطبيق رقم

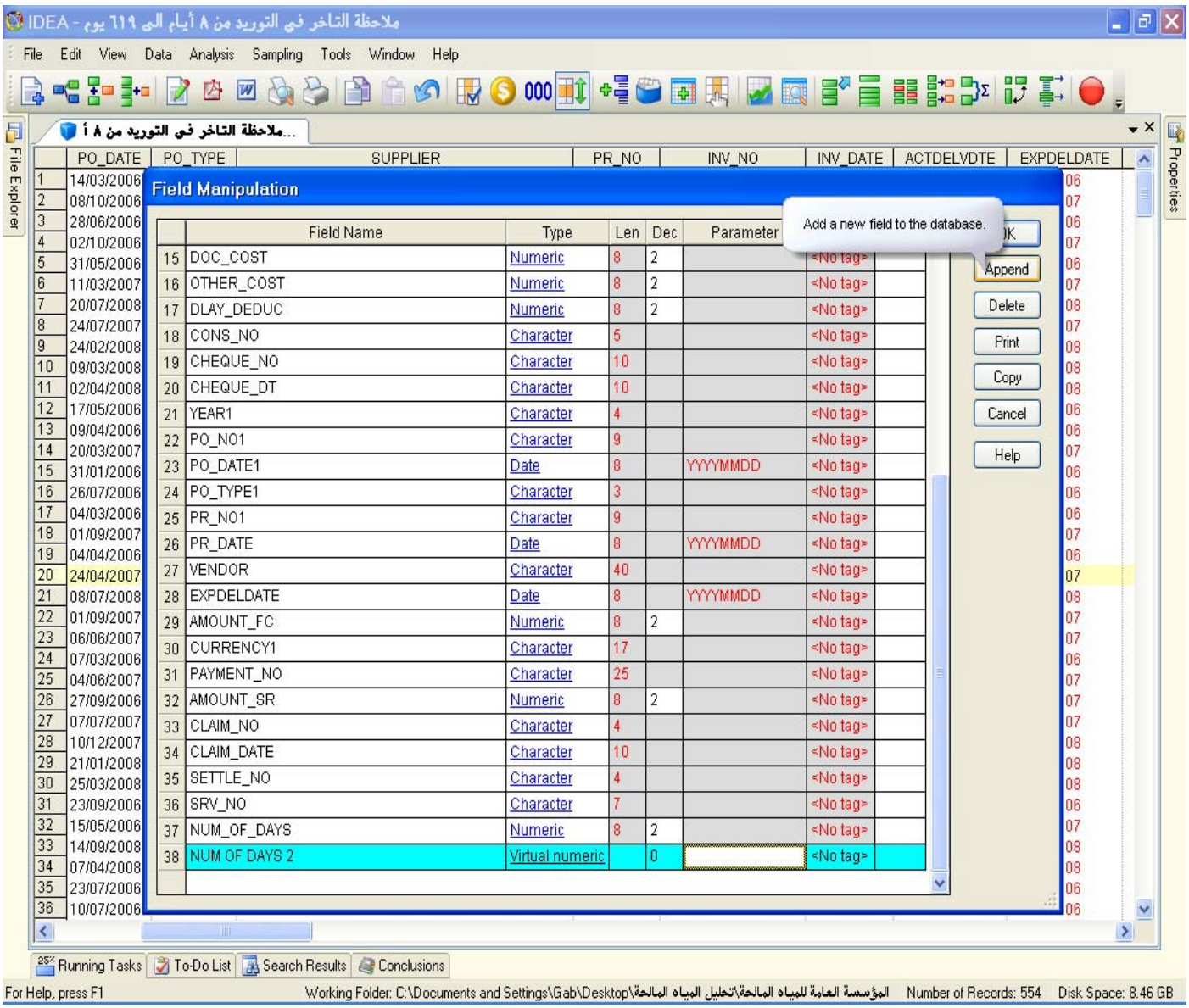
الأمر طرح تاريخ من تاريخ (Age) للحصول على عدد الأيام مثلاً بالمقارنة بين تاريخ بداية الإجازة ونهاية الإجازة , وبين تاريخ بداية الانتداب وتاريخ نهاية الانتداب لتحديد عدد الأيام الفعلية ومقارنتها بعدد الأيام المتوفرة في البيانات وكذلك تحديد تاريخ التوريد الفعلي والتاريخ المتوقع لتوريد الأصناف لحساب غرامات التأخير بدقة.

نقوم بفتح الملف ومن ثم الذهاب لعلامة (V) لإضافة حقل جديد ونسميه NUM OF DAYS وقبل ذلك ينبغي التأكد من أن التاريخين نوعهما Date , وإذا كانت غير ذلك يجب تحويلها إلى حقول تاريخية من خلال إضافة حقول تواريخ جديدة كما سبق شرحه ,وبعد ذلك نقوم باستخدام معادلة التحويل AGE للمقارنة بين التاريخين الجديدين اللذين تمت إضافتهما , أما إذا كانت التواريخ نوعها تاريخي فنقوم بمقارنة التاريخين مباشرة بدون أي تعديل على نوعيهما وسوف نوضح في الشاشات التالية طريقة مقارنة التاريخين للحصول على عدد أيام التأخير بين التاريخ المتوقع للتوريد والتاريخ الفعلي للتوريد كمثال تطبيقي .

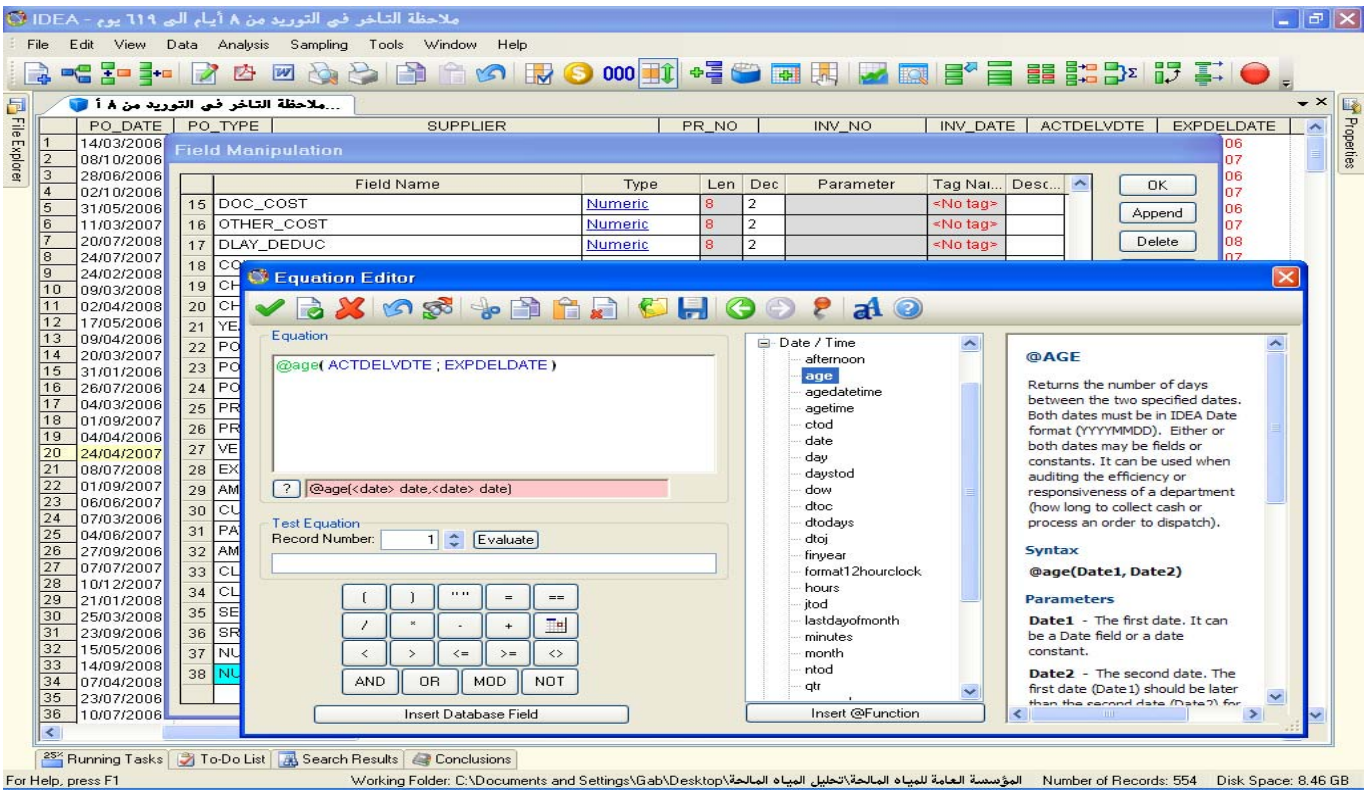


	PO_DATE	PO_TYPE	SUPPLIER	PR_NO	INV_NO	INV_DATE	ACTDELVDTE	EXPDELDATE
1	14/03/2006	CAD	A.WINKEL NAYYAR TRADING	0124158	XD.29338	29/05/2006	07/06/2006	30/05/2006
2	08/10/2006	CAD	A.WINKEL NAYYAR TRADING	0124462-A	X.30732	30/01/2007	05/02/2007	28/01/2007
3	28/06/2006	APP	A.WINKEL NAYYAR TRADING	0316672-C	XD.29888	11/09/2006	14/09/2006	06/09/2006
4	02/10/2006	APP	A.WINKEL NAYYAR TRADING	0470797-A	XD.30734	31/01/2007	08/02/2007	31/01/2007
5	31/05/2006	CAD	A.WINKEL NAYYAR TRADING	0727992	XD.29814	24/08/2006	31/08/2006	23/08/2006
6	11/03/2007	CAD	SIFEM INTERNATIONAL SRL	0732199	902/07	02/11/2007	05/11/2007	28/10/2007
7	20/07/2008	CAD	VARIOLINE SPARE PARTS SERVICES INC.	0740253	08/16722/C:10966	02/08/2008	10/11/2008	02/11/2008
8	24/07/2007	APP	V-LINE EUROPE EXPORT MARKETING GMBH	0840415-A	07/109846/C:10966	09/11/2007	14/11/2007	06/11/2007
9	24/02/2008	CAD	VARIOLINE SPARE PARTS SERVICES INC.	0860116	07/14675/C:10966	26/03/2008	19/05/2008	11/05/2008
10	09/03/2008	CAD	VARIOLINE SPARE PARTS SERVICES INC.	0860202-A	07/14771/C:10966	31/03/2008	19/05/2008	11/05/2008
11	02/04/2008	APP	A.WINKEL NAYYAR TRADING	0860226-A	X.33206	11/06/2008	19/06/2008	11/06/2008
12	17/05/2006	CAD	A.WINKEL NAYYAR TRADING	0880018	X.30270	01/11/2006	02/11/2006	25/10/2006
13	09/04/2006	CAD	A.WINKEL NAYYAR TRADING	3803740	XD.29566	17/07/2006	31/07/2006	23/07/2006
14	20/03/2007	APP	A.WINKEL NAYYAR TRADING	8701353	XD.31662	02/07/2007	04/07/2007	26/06/2007
15	31/01/2006	CAD	A.WINKEL NAYYAR TRADING	8821095	X.29074	10/04/2006	19/04/2006	11/04/2006
16	26/07/2006	CAD	A.WINKEL NAYYAR TRADING	0123974-B	X.30058	01/10/2006	20/10/2006	11/10/2006
17	04/03/2006	APP	A.WINKEL NAYYAR TRADING	0124219	X.29354	15/05/2006	22/05/2006	13/05/2006
18	01/09/2007	APP	A.WINKEL NAYYAR TRADING	0127505-C	XD.32288	14/11/2007	19/11/2007	10/11/2007
19	04/04/2006	CAD	XOMOX INTERNATIONAL GMBH & CO.	0215939	2590606	18/09/2006	21/09/2006	12/09/2006
20	24/04/2007	CAD	V-LINE EUROPE EXPORT MARKETING GMBH	0270021	07/107512/C:10966	02/10/2007	04/10/2007	25/09/2007
21	08/07/2008	APP	A.WINKEL NAYYAR TRADING	0461566	XD.33526	02/09/2008	11/09/2008	02/09/2008
22	01/09/2007	CAD	A.WINKEL NAYYAR TRADING	0606013-D	XD.32390	05/12/2007	10/12/2007	01/12/2007
23	06/06/2007	CAD	VARIOLINE SPARE PARTS SERVICES INC.	0606032-E	07/11661/C:16137	25/07/2007	28/09/2007	19/09/2007
24	07/03/2006	APP	A.WINKEL NAYYAR TRADING	0726932	XD29446	19/06/2006	29/06/2006	20/06/2006
25	04/06/2007	CAD	SIFEM INTERNATIONAL SRL	0728658-A	797/07	02/10/2007	10/10/2007	01/10/2007
26	27/09/2006	CAD	SIFEM INTERNATIONAL SRL	0731965	61/07	08/02/2007	16/02/2007	07/02/2007
27	07/07/2007	CAD	A.WINKEL NAYYAR TRADING	0740139	X.32076	04/10/2007	22/10/2007	13/10/2007
28	10/12/2007	CAD	VARIOLINE SPARE PARTS SERVICES INC.	0750423	07/14044/C:10966	11/02/2008	12/03/2008	03/03/2008
29	21/01/2008	CAD	A.WINKEL NAYYAR TRADING	0750537	XD.33122	02/06/2008	04/06/2008	26/05/2008
30	25/03/2008	APP	A.WINKEL NAYYAR TRADING	0751014	XD.33186	16/06/2008	19/06/2008	10/06/2008
31	23/09/2006	CAD	C.I.T.C. USA, INC	0280254	0066721-IN	16/11/2006	21/11/2006	11/11/2006
32	15/05/2006	CAD	VELAN MIDDLE EAST	0727197	2007-24	28/04/2007	03/05/2007	23/04/2007
33	14/09/2008	CAD	VARIOLINE SPARE PARTS SERVICES INC.	0740668	08/18543/C:10966	21/11/2008	26/11/2008	16/11/2008
34	07/04/2008	APP	A.WINKEL NAYYAR TRADING	0860206	XD.33404	28/07/2008	07/08/2008	28/07/2008
35	23/07/2006	CAD	FAPMO	4401712	60529	03/10/2006	18/10/2006	08/10/2006
36	10/07/2006	APP	EXIM RISSIN & CO	4900810-A	RTC-238/06	28/09/2006	28/09/2006	18/09/2006

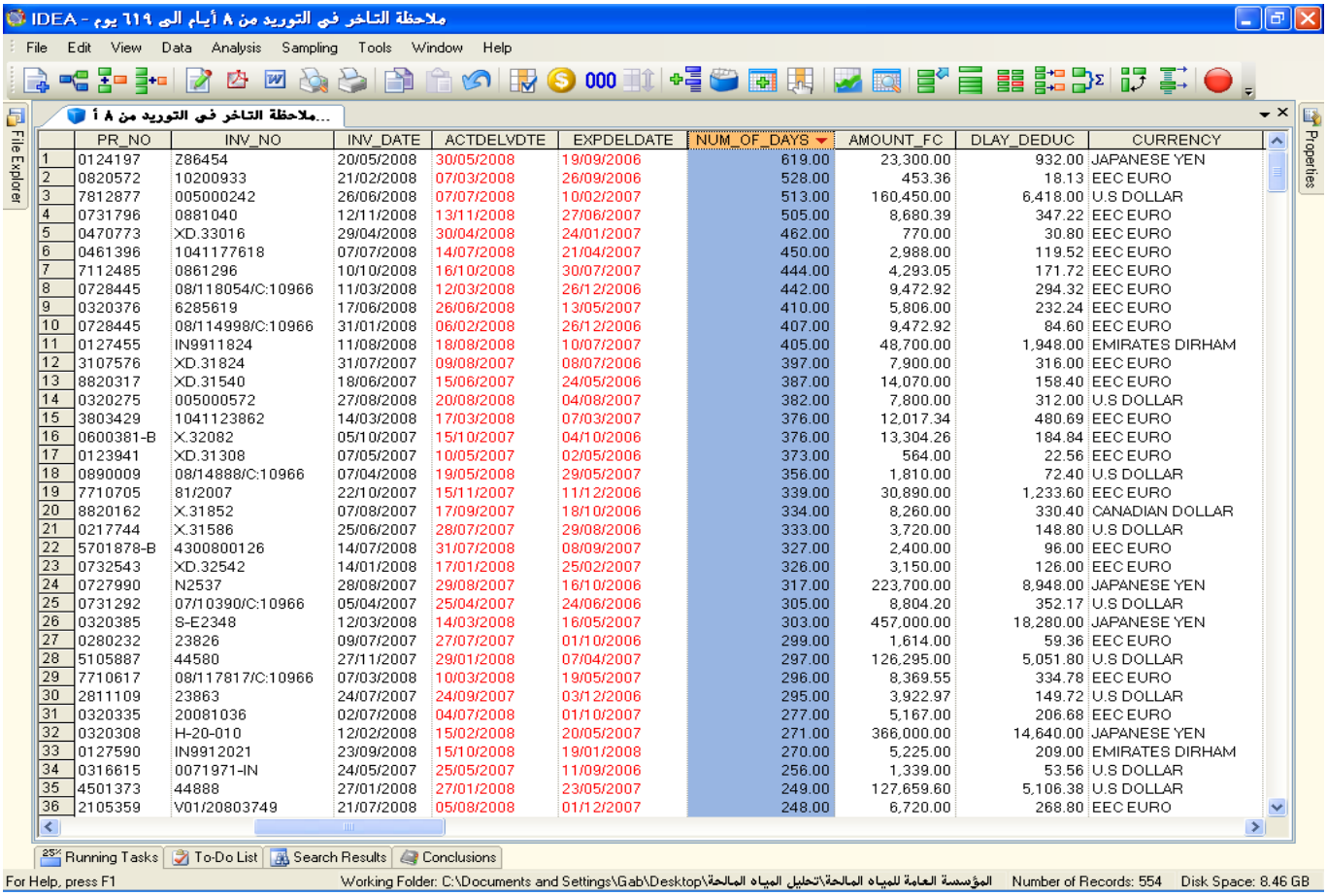
نلاحظ أنه لدينا حقلين ACTDELVDTE ويمثل التاريخ الفعلي للتوريد , وحقل EXPDELDATE ويمثل التاريخ المتوقع للتوريد , بعد ذلك نقوم بإدراج حقل جديد يمثل NUMOFDAYS عدد الأيام ونوضح ذلك بالشاشة التالية :



بعد ذلك نضع المعادلة التالية من خلال اختيار الشرط AGE ونضغط ضغطتين وبعدها سيظهر قوسين يتم إدراج التاريخين وبينهما الفاصلة المنقوطة (;) ونضغط موافق كما هو موضح أدناه وبعده سوف تظهر النتيجة متمثلة بعدد الأيام (الفرق بين التاريخين)



بعد ذلك سوف تظهر النتيجة التالية :



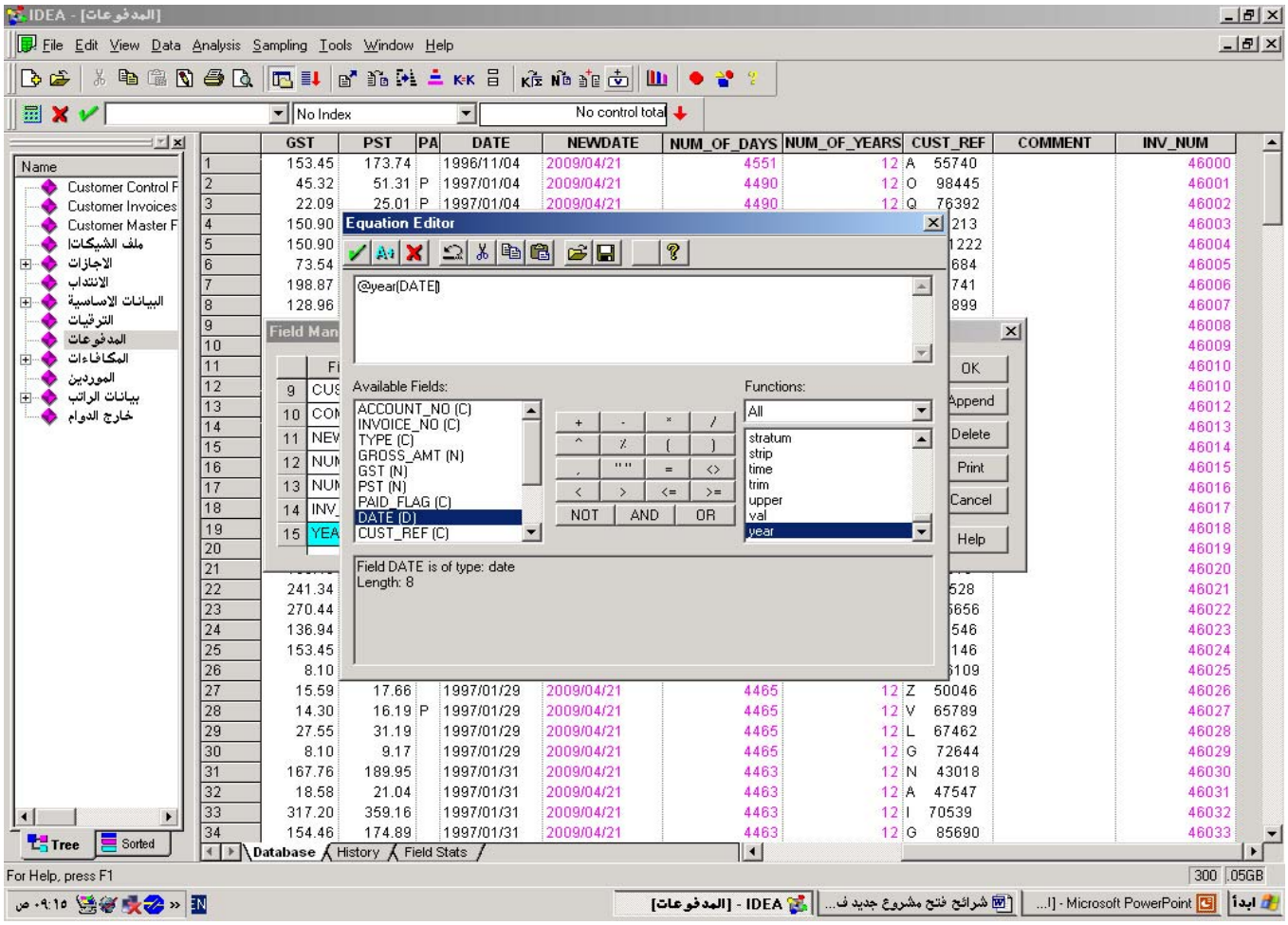
نلاحظ النتيجة تظهر عدد الأيام والتي تمثل الفرق بين التاريخ المتوقع للتوريد والتاريخ الفعلي للتوريد ومن هنا يظهر عدد أيام التأخير في التوريد وبعد ذلك يتم تصدير البيانات إلى الإكسل وإجراء بعض التنسيقات على الملف وبعدها يتم الاستفسار عن ذلك ومدى احتساب الغرامات من عدمها.

تطبيق رقم

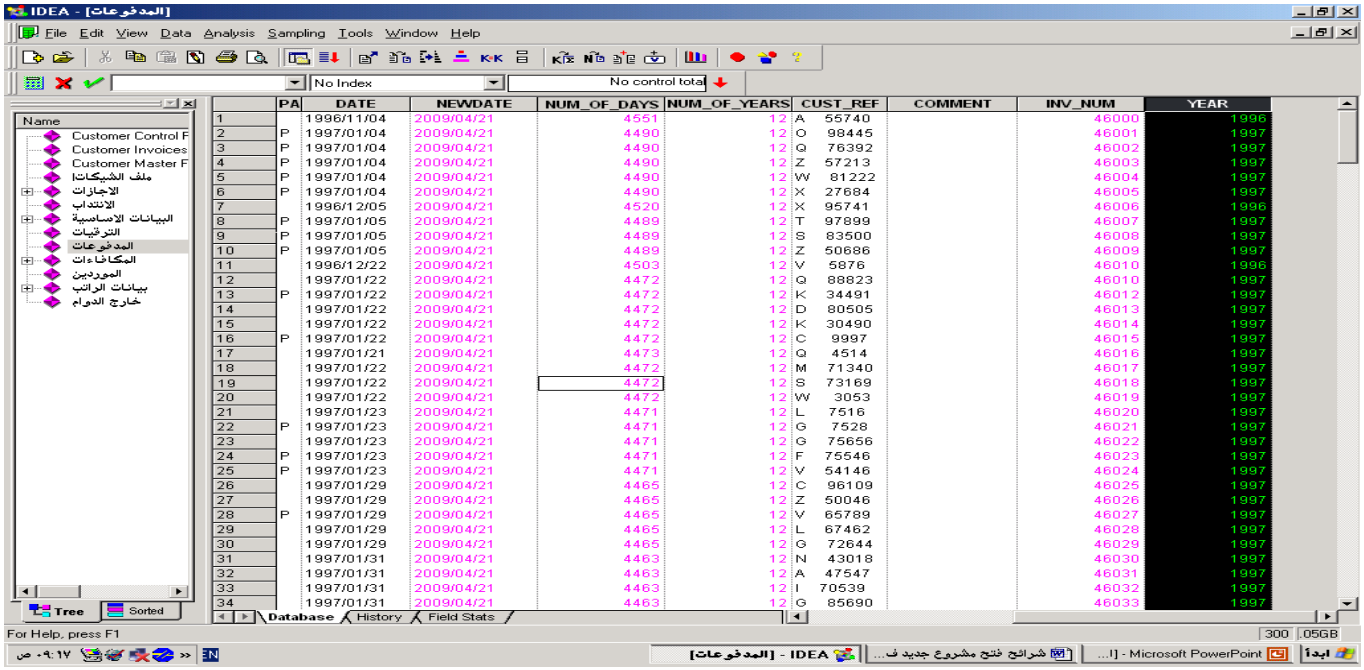
الأمر تقسيم التاريخ إلى ثلاثة أجزاء.

- نقوم بإنشاء ثلاثة حقول جديدة في الملف وهذه الحقول تعبر عن اليوم والشهر والسنة .
- وضع نوع الحقل رقمي .
- استخدام ثلاثة معادلات لتجزئة التاريخ إلى ثلاثة أقسام .

نقوم باختيار Year من خلال الذهاب للقائمة Function ونوضح ذلك في الشاشات التالية :



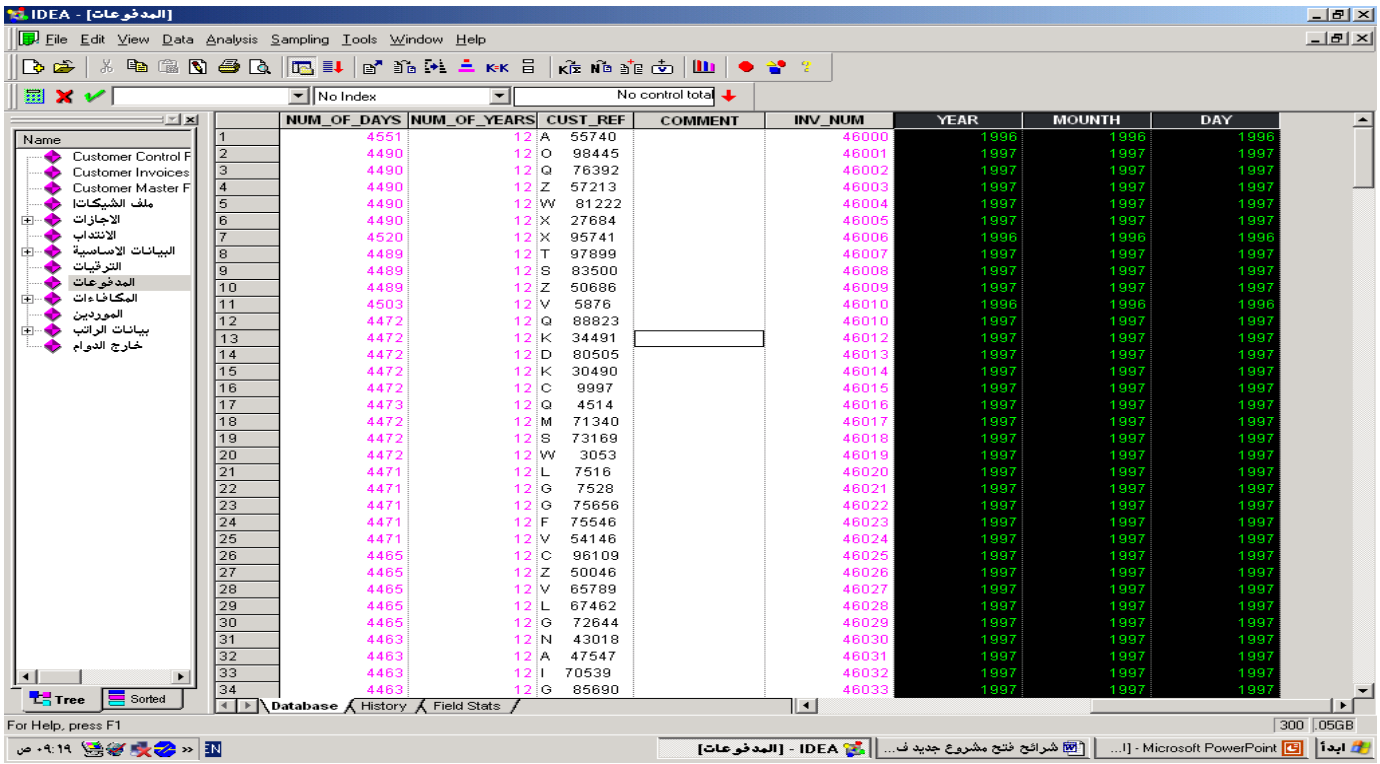
نلاحظ أننا بدأنا بإضافة الحقل الجديد وأسميناه Year السنة , ونطبق المعادلة السابقة من خلال اختيار الشرط Year ونضع التاريخ المراد تقسيمه , ونطبق ذلك على الشهر واليوم , وبعد تنفيذ ذلك نلاحظ التالي :



	PA	DATE	NEWDATE	NUM_OF_DAYS	NUM_OF_YEARS	CUST_REF	COMMENT	INV_NUM	YEAR
1		1996/11/04	2009/04/21	4551	12	A 55740		46000	1996
2	P	1997/01/04	2009/04/21	4490	12	O 98445		46001	1997
3	P	1997/01/04	2009/04/21	4490	12	Q 76392		46002	1997
4	P	1997/01/04	2009/04/21	4490	12	Z 57213		46003	1997
5	P	1997/01/04	2009/04/21	4490	12	W 81222		46004	1997
6	P	1997/01/04	2009/04/21	4490	12	X 27684		46005	1997
7		1996/12/05	2009/04/21	4520	12	X 95741		46006	1996
8	P	1997/01/05	2009/04/21	4489	12	T 97899		46007	1997
9	P	1997/01/05	2009/04/21	4489	12	S 83500		46008	1997
10	P	1997/01/05	2009/04/21	4489	12	Z 50686		46009	1997
11		1996/12/22	2009/04/21	4503	12	V 5876		46010	1996
12		1997/01/22	2009/04/21	4472	12	Q 88823		46010	1997
13	P	1997/01/22	2009/04/21	4472	12	K 34491		46012	1997
14		1997/01/22	2009/04/21	4472	12	D 80505		46013	1997
15		1997/01/22	2009/04/21	4472	12	K 30490		46014	1997
16	P	1997/01/22	2009/04/21	4472	12	C 9997		46015	1997
17		1997/01/21	2009/04/21	4473	12	Q 4514		46016	1997
18		1997/01/22	2009/04/21	4472	12	M 71340		46017	1997
19		1997/01/22	2009/04/21	4472	12	S 73169		46018	1997
20		1997/01/22	2009/04/21	4472	12	W 3053		46019	1997
21		1997/01/23	2009/04/21	4471	12	L 7516		46020	1997
22	P	1997/01/23	2009/04/21	4471	12	G 7528		46021	1997
23		1997/01/23	2009/04/21	4471	12	G 75656		46022	1997
24	P	1997/01/23	2009/04/21	4471	12	F 75546		46023	1997
25	P	1997/01/23	2009/04/21	4471	12	V 54146		46024	1997
26		1997/01/29	2009/04/21	4465	12	C 96109		46025	1997
27		1997/01/29	2009/04/21	4465	12	Z 50046		46026	1997
28	P	1997/01/29	2009/04/21	4465	12	V 65789		46027	1997
29		1997/01/29	2009/04/21	4465	12	L 67462		46028	1997
30		1997/01/29	2009/04/21	4465	12	G 72644		46029	1997
31		1997/01/31	2009/04/21	4463	12	N 43018		46030	1997
32		1997/01/31	2009/04/21	4463	12	A 47547		46031	1997
33		1997/01/31	2009/04/21	4463	12	I 70539		46032	1997
34		1997/01/31	2009/04/21	4463	12	G 85690		46033	1997

نلاحظ أنه تم إدراج الحقل الجديد ويظهر السنوات فقط .

وبعد تنفيذ نفس المعادلة السابقة على اليوم والشهر سوف تظهر الحقول بالشكل التالي :



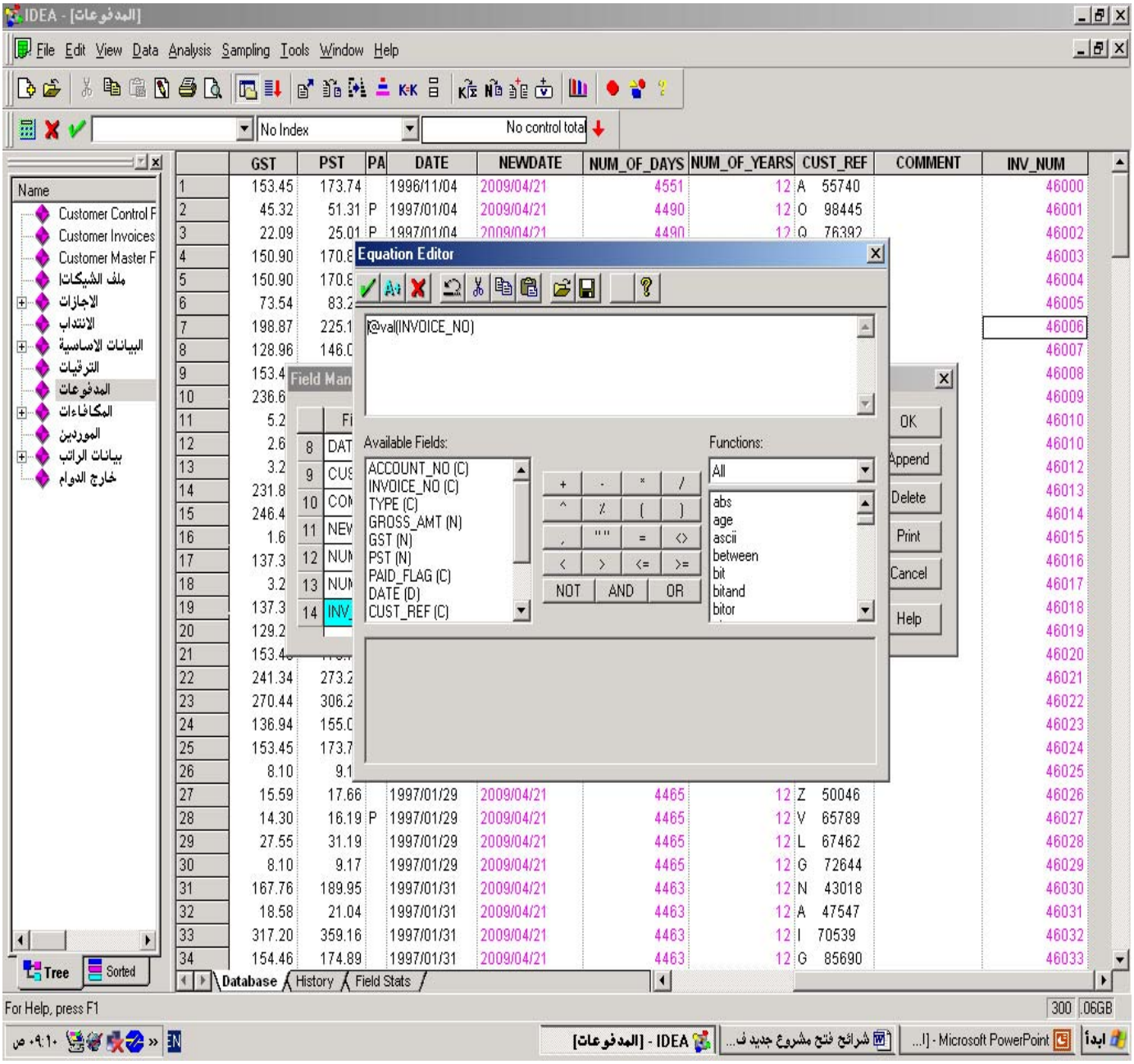
	NUM_OF_DAYS	NUM_OF_YEARS	CUST_REF	COMMENT	INV_NUM	YEAR	MOUNTH	DAY
1	4551	12	A 55740		46000	1996	1996	1996
2	4490	12	O 98445		46001	1997	1997	1997
3	4490	12	Q 76392		46002	1997	1997	1997
4	4490	12	Z 57213		46003	1997	1997	1997
5	4490	12	W 81222		46004	1997	1997	1997
6	4490	12	X 27684		46005	1997	1997	1997
7	4520	12	X 95741		46006	1996	1996	1996
8	4489	12	T 97899		46007	1997	1997	1997
9	4489	12	S 83500		46008	1997	1997	1997
10	4489	12	Z 50686		46009	1997	1997	1997
11	4503	12	V 5876		46010	1996	1996	1996
12	4472	12	Q 88823		46010	1997	1997	1997
13	4472	12	K 34491		46012	1997	1997	1997
14	4472	12	D 80505		46013	1997	1997	1997
15	4472	12	K 30490		46014	1997	1997	1997
16	4472	12	C 9997		46015	1997	1997	1997
17	4473	12	Q 4514		46016	1997	1997	1997
18	4472	12	M 71340		46017	1997	1997	1997
19	4472	12	S 73169		46018	1997	1997	1997
20	4472	12	W 3053		46019	1997	1997	1997
21	4471	12	L 7516		46020	1997	1997	1997
22	4471	12	G 7528		46021	1997	1997	1997
23	4471	12	G 75656		46022	1997	1997	1997
24	4471	12	F 75546		46023	1997	1997	1997
25	4471	12	V 54146		46024	1997	1997	1997
26	4465	12	C 96109		46025	1997	1997	1997
27	4465	12	Z 50046		46026	1997	1997	1997
28	4465	12	V 65789		46027	1997	1997	1997
29	4465	12	L 67462		46028	1997	1997	1997
30	4465	12	G 72644		46029	1997	1997	1997
31	4463	12	N 43018		46030	1997	1997	1997
32	4463	12	A 47547		46031	1997	1997	1997
33	4463	12	I 70539		46032	1997	1997	1997
34	4463	12	G 85690		46033	1997	1997	1997

تطبيق رقم

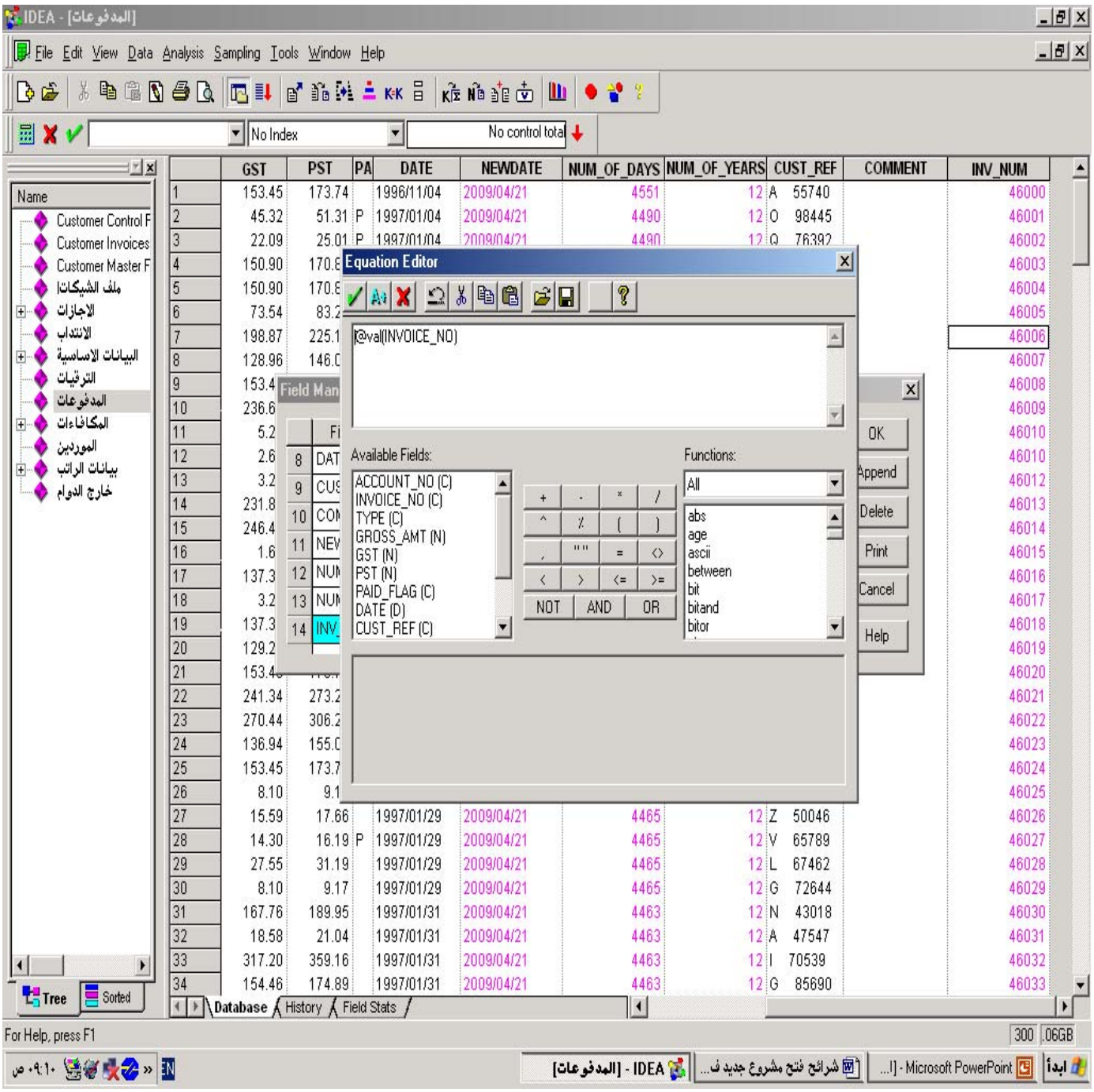
الأمر تحويل الرقم الحرفي إلى رقم حقيقي بواسطة الأمر Val (field_name)

- إنشاء حقل جديد في الملف عن طريق أمر append
- يتم اختيار نوع الحقل الجديد بان يكون رقمي

كتابة المعادلة الموضحة أدناه من خلال القائمة Function واختيار Val :



بعد ذلك سيظهر الحقل الرقمي كما هو موضح بعد تنفيذ المعادلة كما هو موضح في الشاشة التالية :

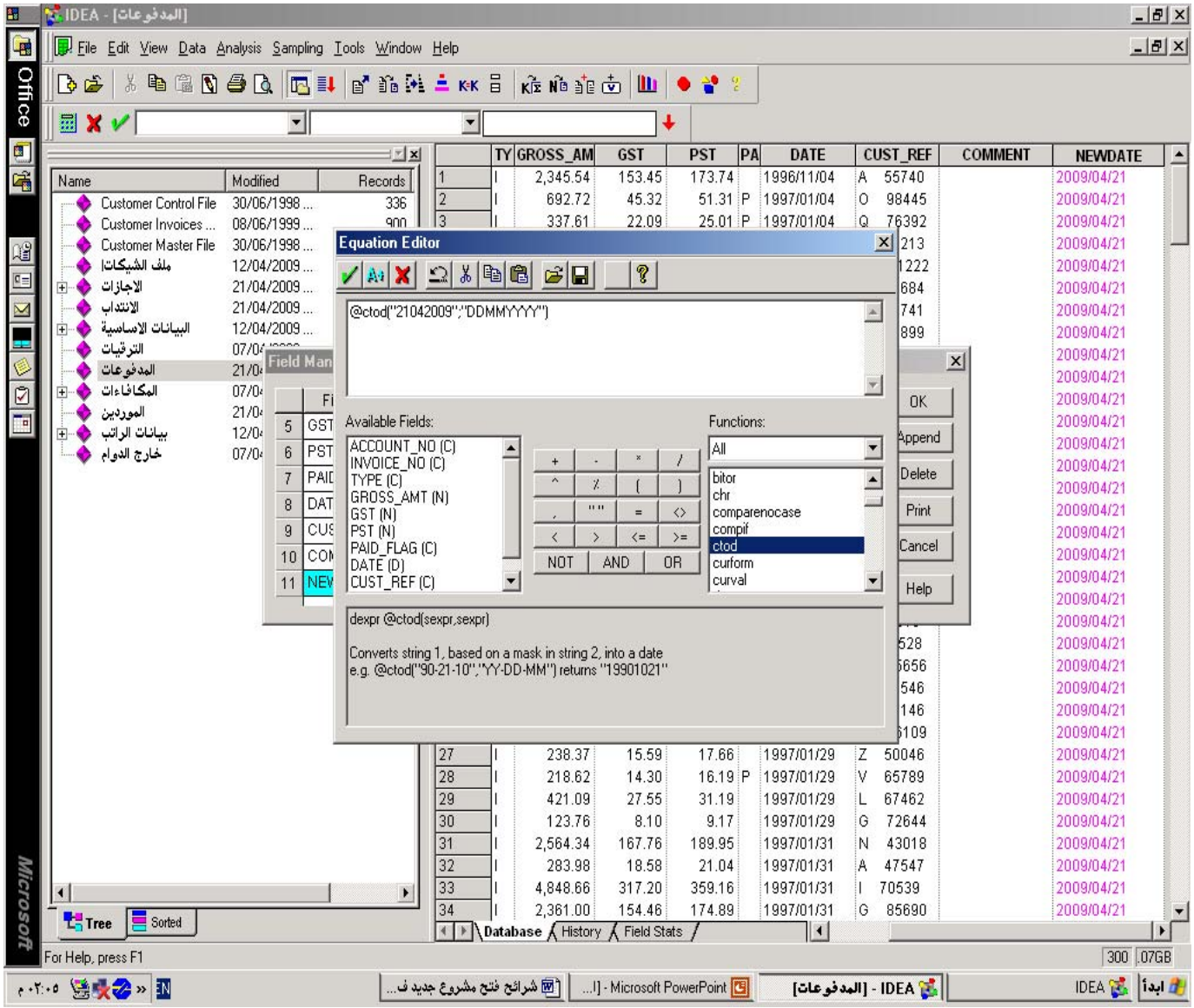


ونستطيع تطبيق المثال السابق على المبالغ التي تحمل التنسيق الحرفي وتحويلها إلى حقل رقمي وبفواصل عشرية ويمكن إجراء أية عمليات حسابية على الحقل الجديد .

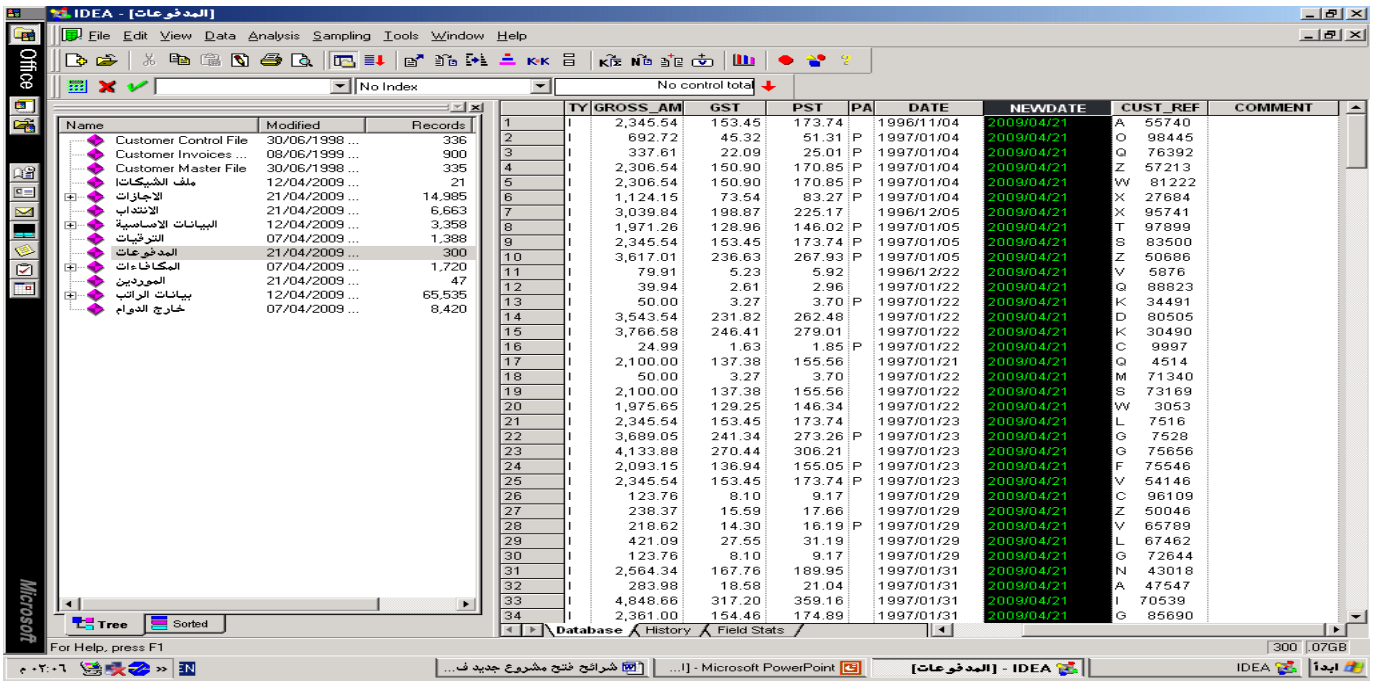
تطبيق رقم

طرح تاريخ من تاريخ مثل حساب مدة خدمة الموظف حيث يلزمنا إضافة حقل يمثل تاريخ اليوم وبعد ذلك يمكننا أن نطرح منه تاريخ التعيين والنتيجة تكون متمثلة بعدد الأيام ونقسمها على 365 يوم للحصول على عدد السنوات .

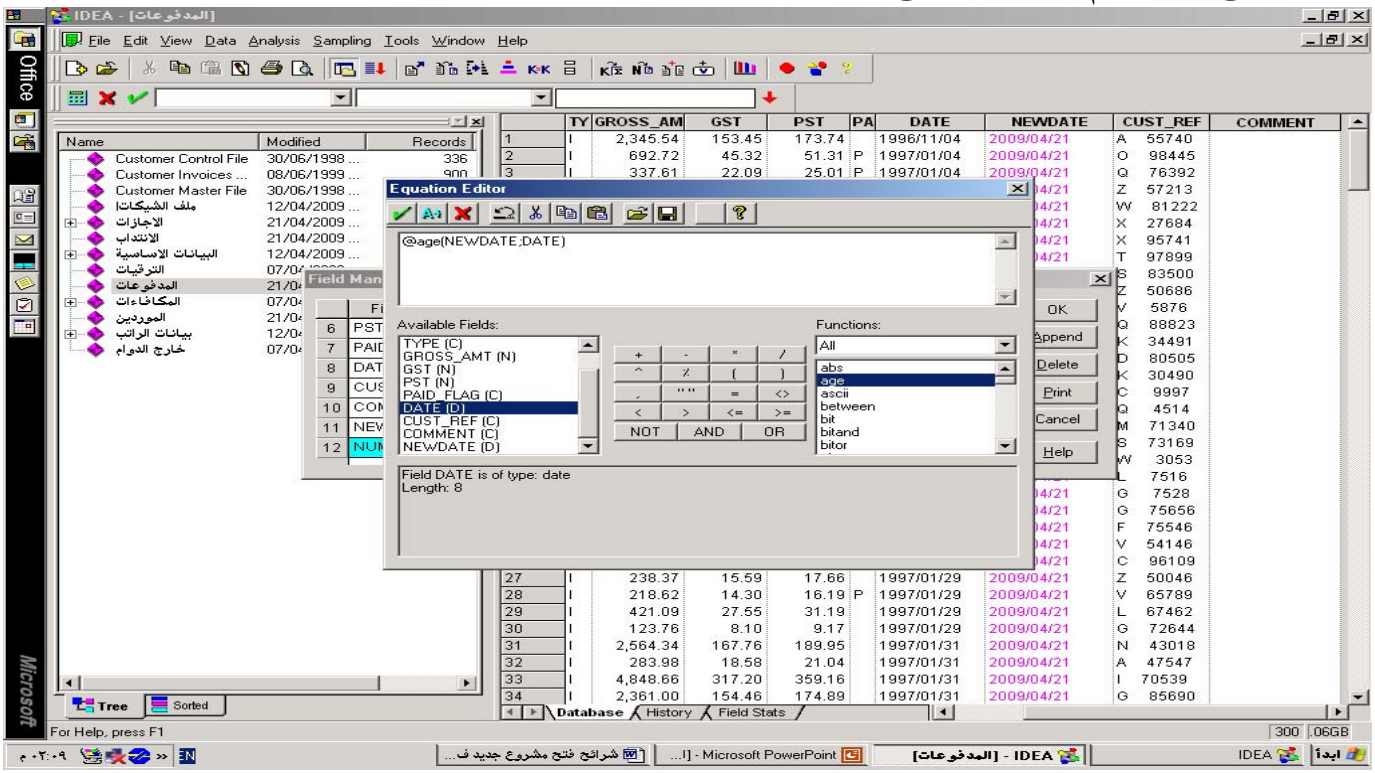
- نقوم بإضافة حقل جديد لوضع تاريخ اليوم بإسم NEW DATE ويكون نوعه تاريخي حيث نقوم بالذهاب للقائمة Function واختيار الأمر ctod ونكتب المعادلة التالية كما هو موضح في الشاشة التالية :



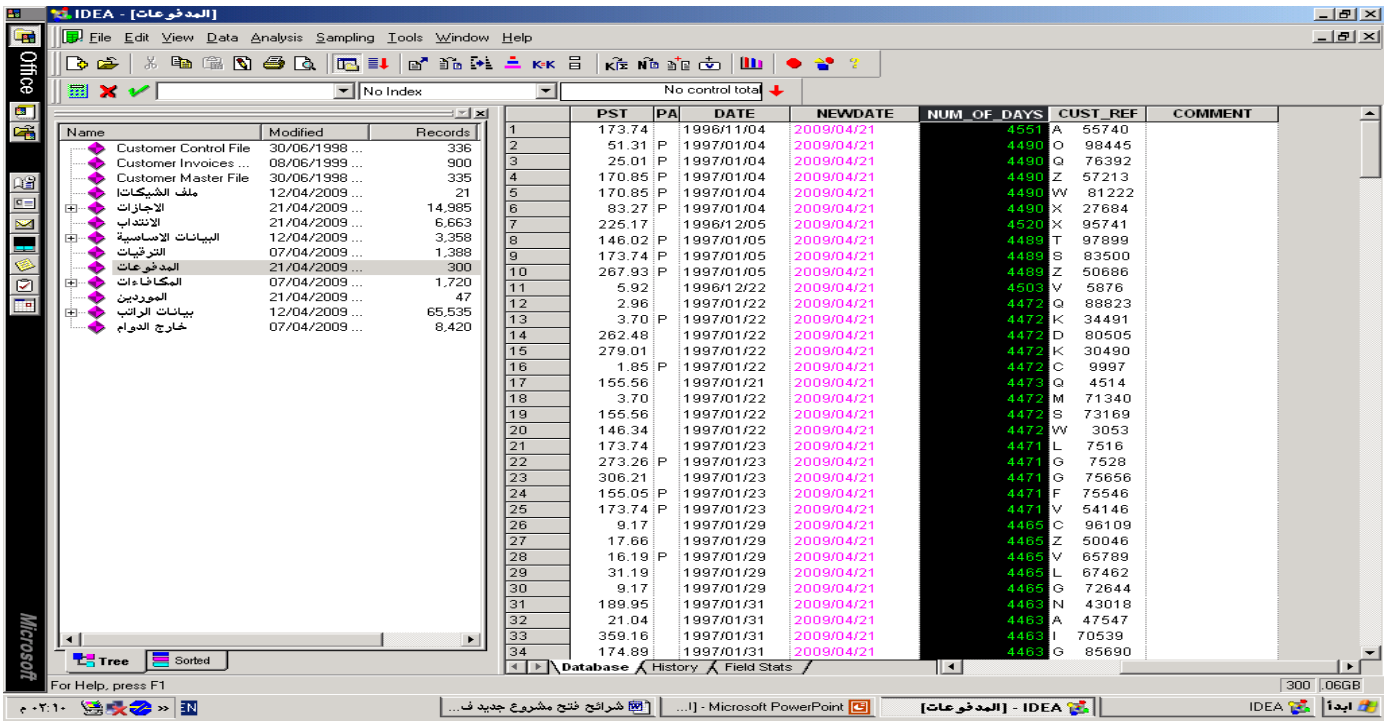
- بعد ذلك نضغط موافق من خلال علامة الصح , ثم OK
- بعدها سنحصل على النتيجة التالية والتي تمثل تاريخ اليوم .



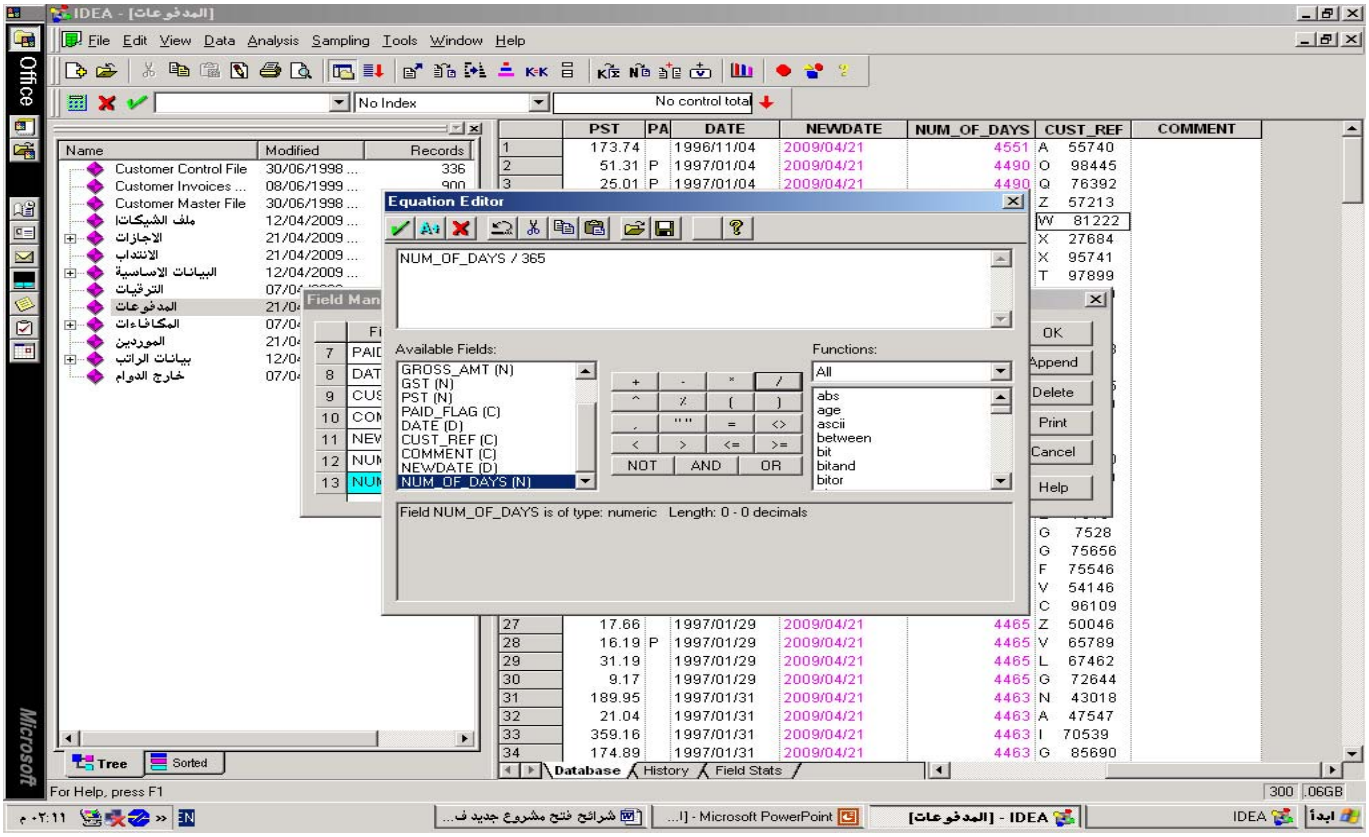
- بعد ذلك نقوم بطرح تاريخ اليوم من تاريخ التعيين المعطى ضمن البيانات ونقوم بتطبيق المعادلة التالية من خلال الأمر AGE كما سوف نوضحه تالياً :
- نقوم بإدراج حقل جديد ونسميه NUM OF DYES لمعرفة عدد الأيام ومن ثم نقوم بتقسيمها على 365 يوم للحصول على عدد السنوات .



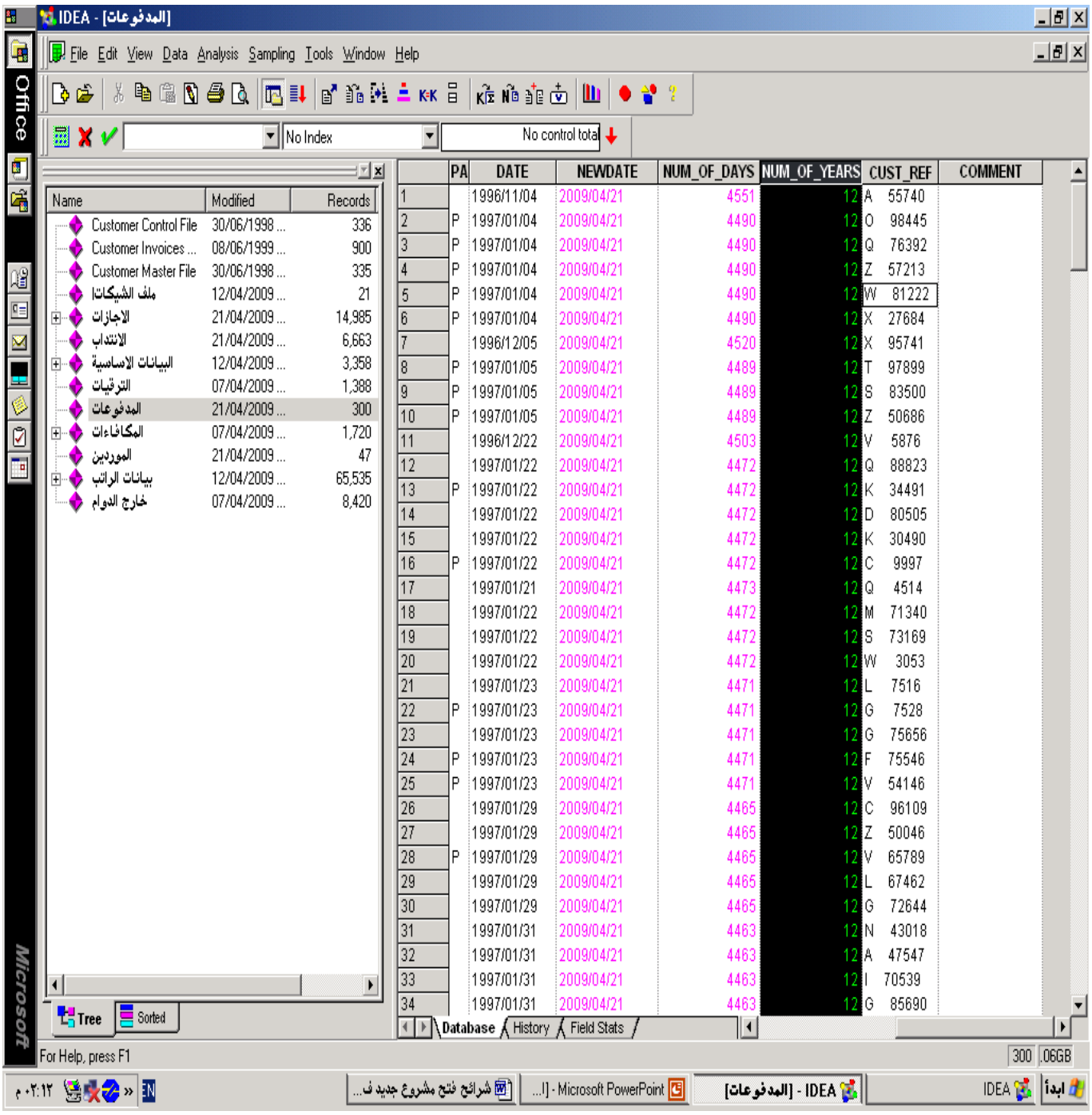
- بعد ذلك نضغط OK وسوف نحصل على النتيجة التالية :



- بعدها يمكننا أن نقسم عدد الأيام على 365 يوم للحصول على عدد السنوات كما هو موضح أدناه :



- بعد تنفيذ العملية ستظهر النتيجة التالية :



تطبيق رقم

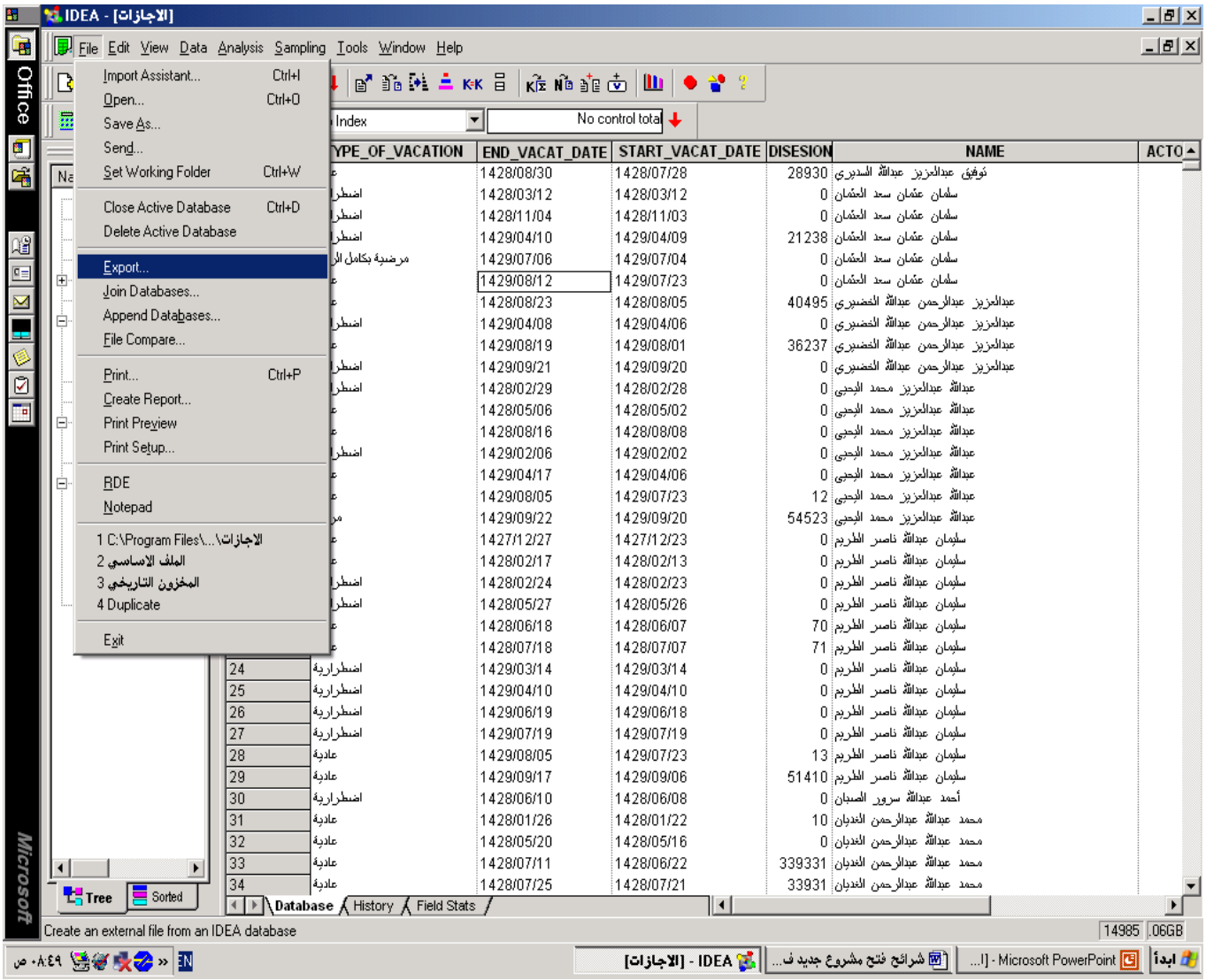
الأمر : تصدير البيانات Export

يستخدم أمر تصدير البيانات من برنامج الآيديا بعد إجراء عملية التحليل ونقلها وترحيلها إلى برنامج الإكسل وذلك من اجل التالي :

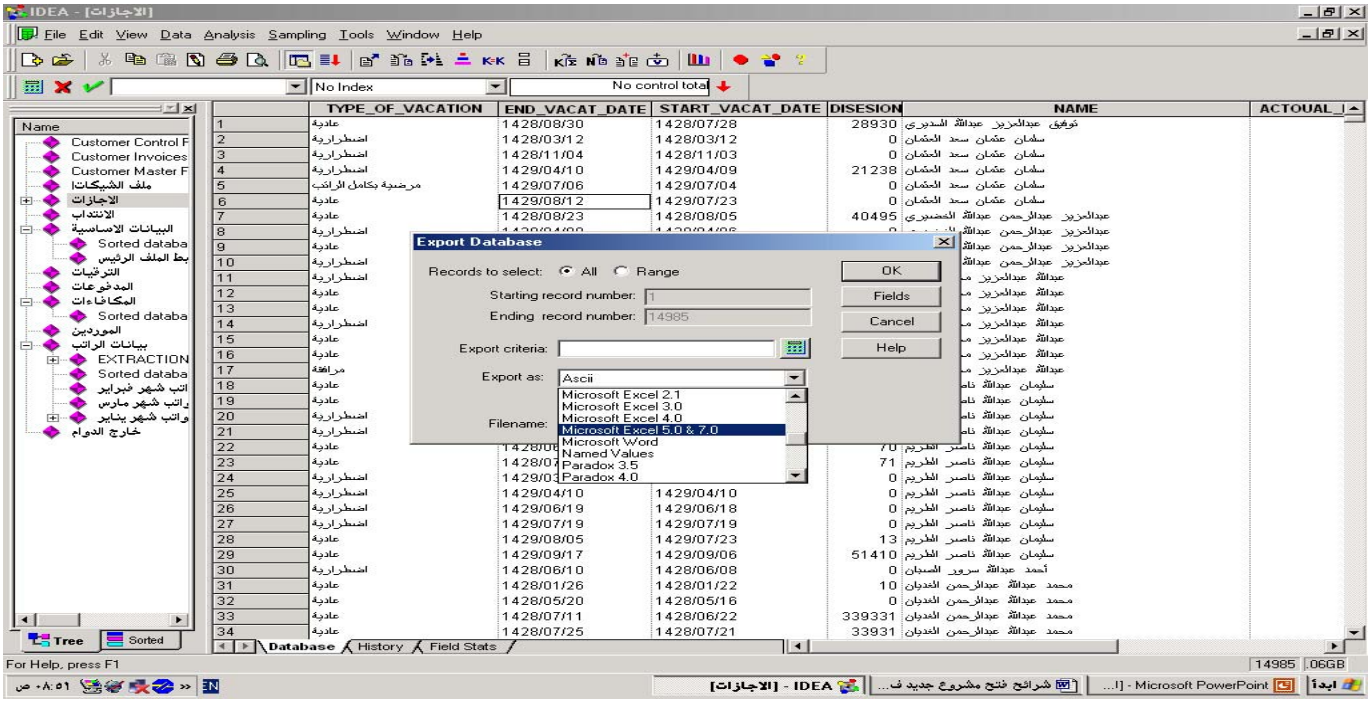
- كتابة التقرير بالتنسيق المطلوب والمفهوم للقارئ .
- توثيق عملية التحليل في برامج أخرى مثل التيمم ميت بإضافة هذه التقارير كمرفقات .

إذا أردنا تصدير ملف الإجازات على سبيل المثال نتبع التالي :

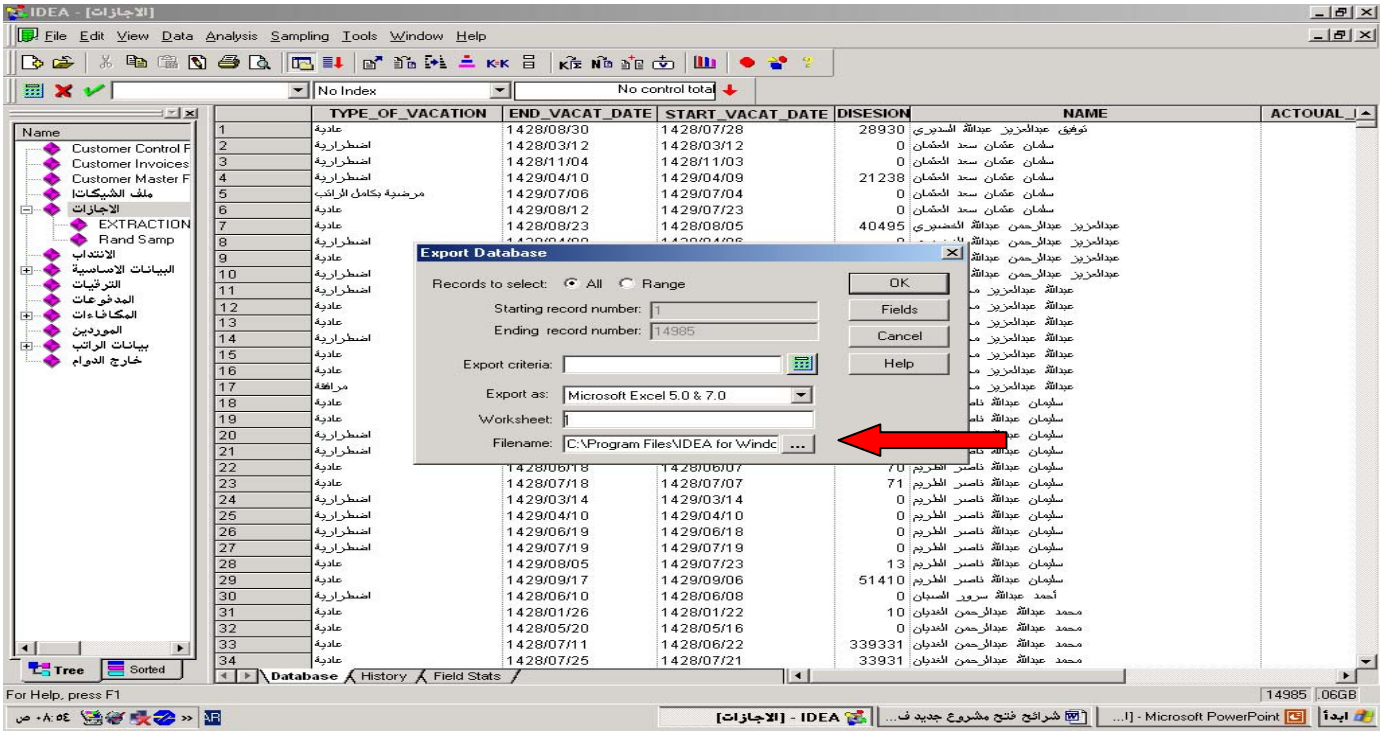
نذهب إلى القائمة File ومن ثم نقوم باختيار Export



بعد ذلك ستظهر الشاشة التالية :



ونقوم بتحديد نوع الحفظ باختيار اكسل , وبعد ذلك نقوم بتحديد مكان الحفظ سواء على سطح المكتب أو المستندات والشاشة التالية توضح ذلك .



بعد ذلك سيظهر الملف الذي تم تصديره في المكان الذي تم الحفظ فيه ويجرى عليه بعض التنسيقات حسب الرغبة حتى يظهر بالصورة المطلوبة .

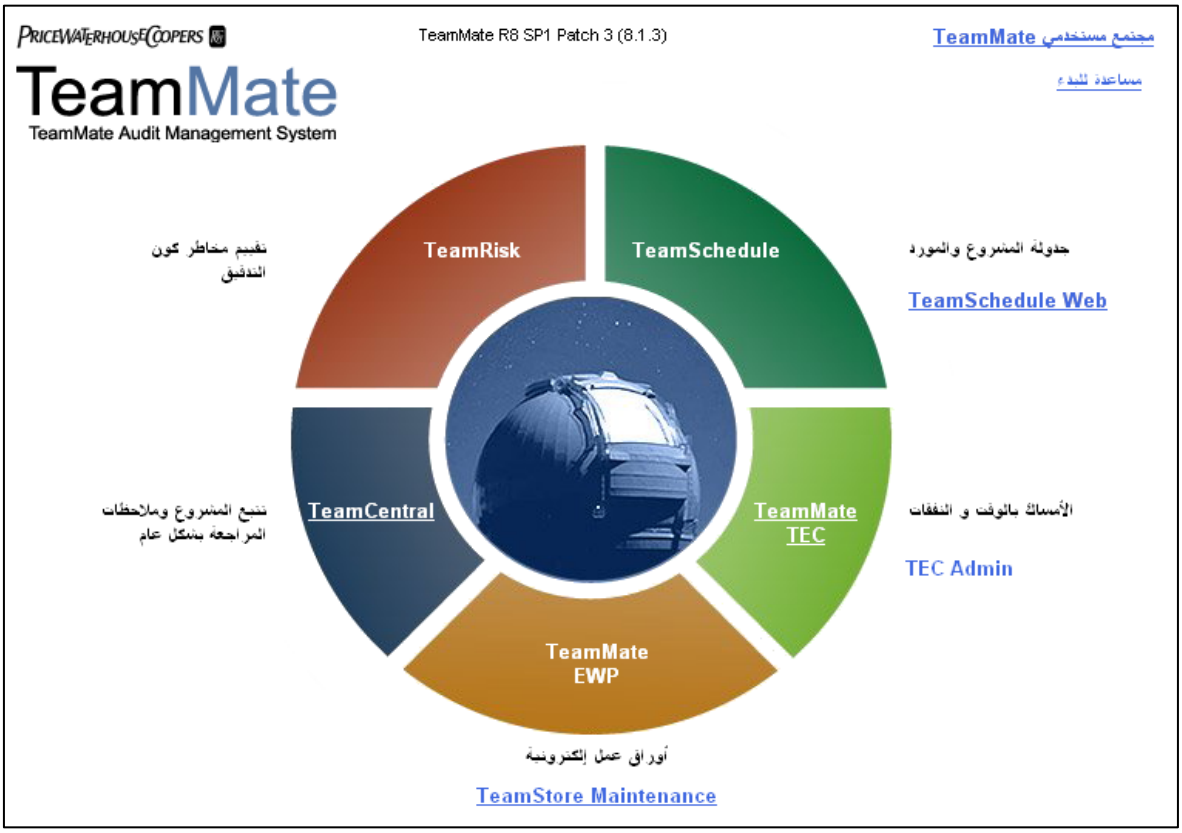
دليل استخدام

Teammate

نظام إدارة التدقيق

EWP

أوراق عمل الكترونية



جدول المحتويات

أولا: كيفية الدخول إلى البرنامج

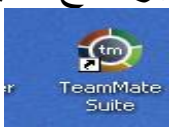
ثانيا: إنشاء مشروع جديد

ثالثا: إكمال إعدادات المشروع وتحديد فريق العمل والأدوار

رابعا: إحضار برامج العمل من مكتبة Team Store

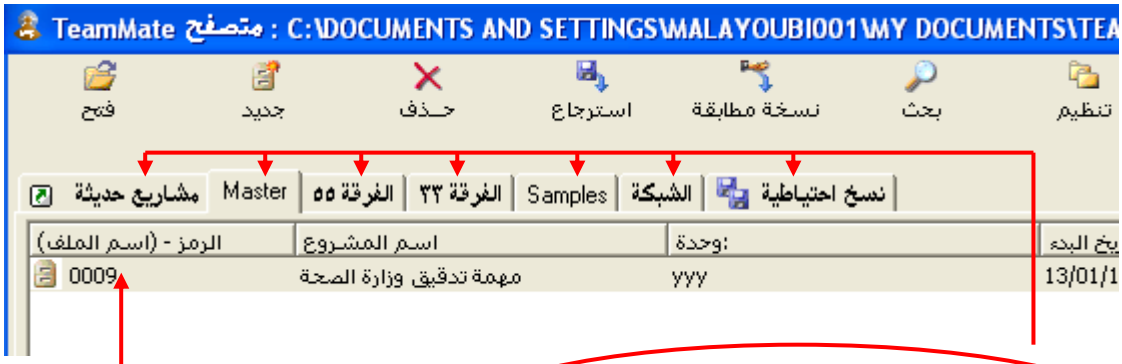
خامسا: ملاحظات التدقيق

أولا : كيفية الدخول إلى النظام:

- للدخول على برنامج التيم ميت اضغط على اختصار البرنامج الموجود على سطح المكتب 

- اختيار أوراق عمل الكترونية

- سوف تظهر لك نافذة المتصفح وبداخلها أماكن تخزين المشاريع وتصنيف الفرق والمشروعات التابعة لكل فرقة

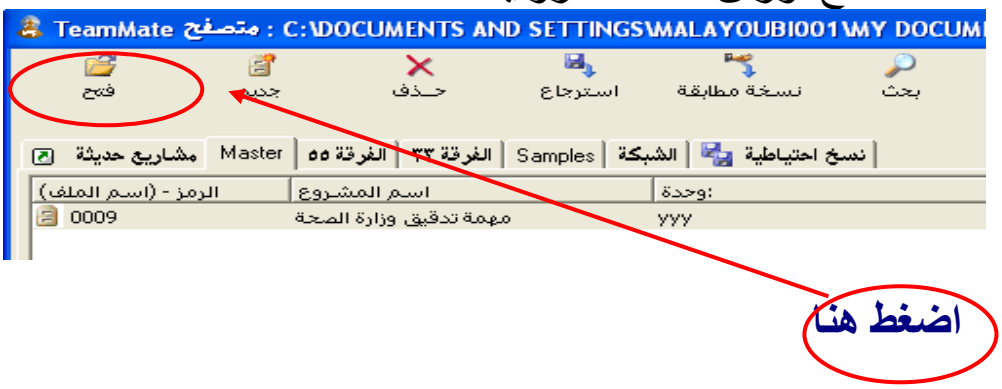


أمـــــاكن تخـــــزين المشـــــاريع وتقســـــيم المشـــــاريع الفـــــرق

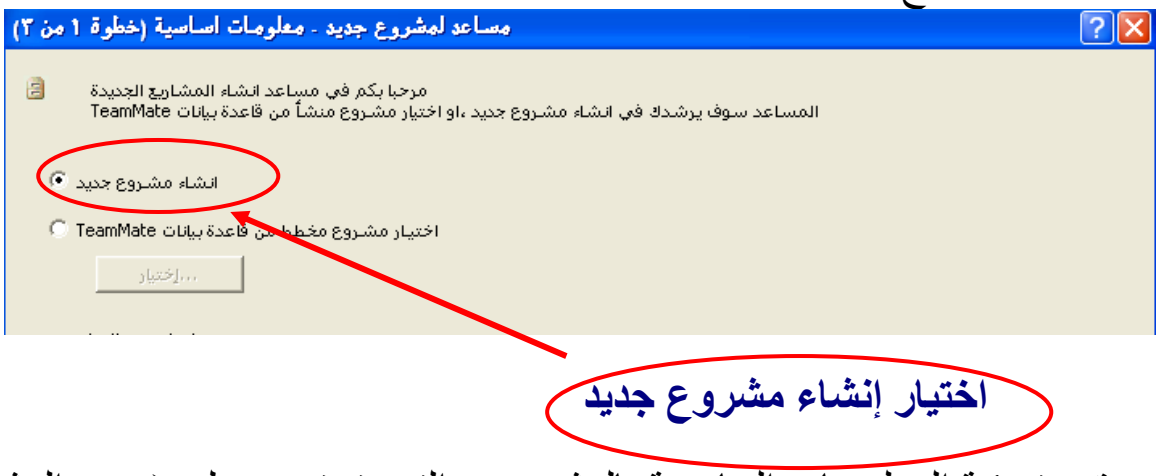
مشروع

ثانيا : إنشاء مشروع جديد :

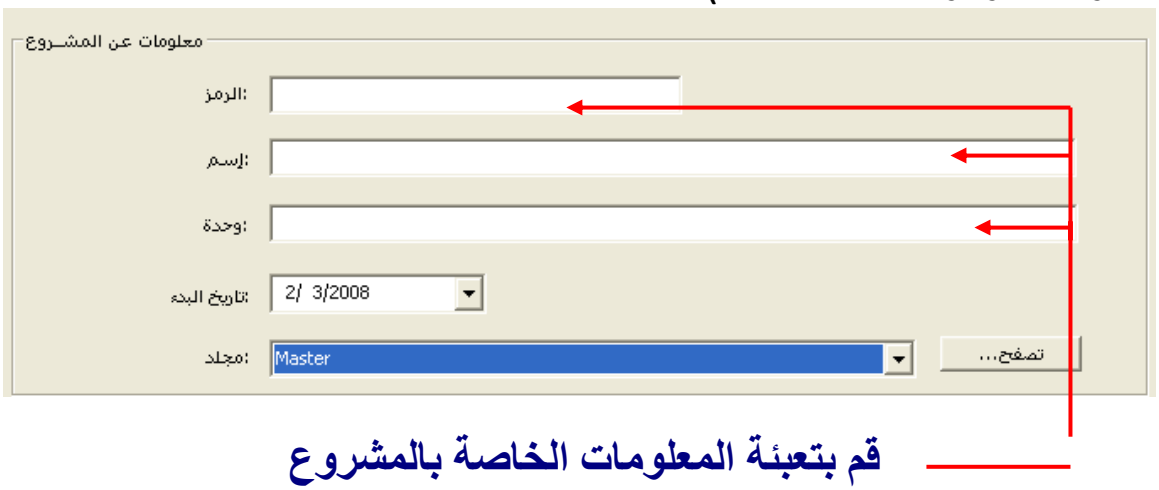
- لإنشاء مشروع جديد قم بالضغط على (جديد) من شاشة المتصفح التي ظهرت لك عند فتح أوراق عمل الكترونية



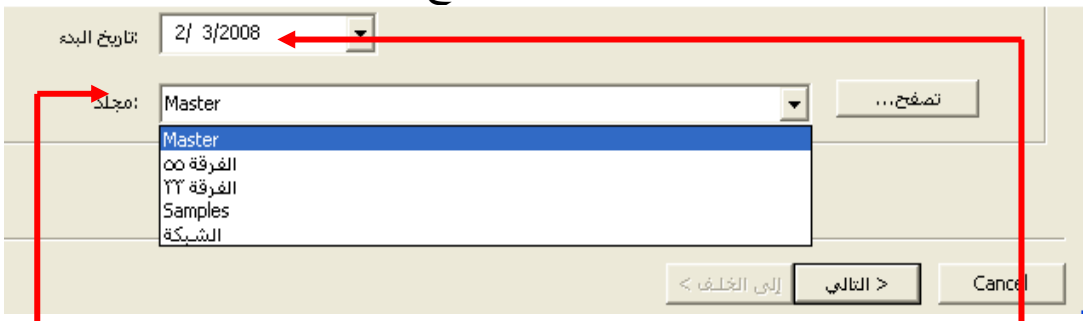
- ستظهر لك نافذة المتصفح (الخطوة الأولى) وستختار إنشاء مشروع جديد من نافذة المتصفح



- قم بتعبئة المعلومات الخاصة بالمشروع والتي تحتوي على(رمز المشروع واسمه والوحدة التابعة لها)

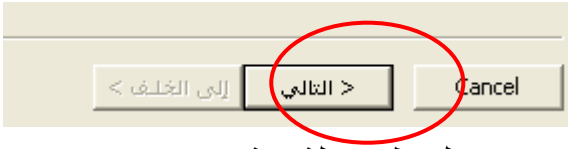


- سوف يقوم البرنامج من تلقاء نفسه بوضع تاريخ اليوم الذي تقوم به بإنشاء المشروع وبإمكانك تغير التاريخ إلى اليوم الذي تريد به بداية المشروع أو التاريخ الذي يتم تحديده وفق الخطاب التكليف المرسل لك
- من قائمة المجلد اختر مكان تخزين المشروع



اختر التاريخ المناسب أو التاريخ الذي تريد به بدء المشروع أو تاريخ بدء المهمة

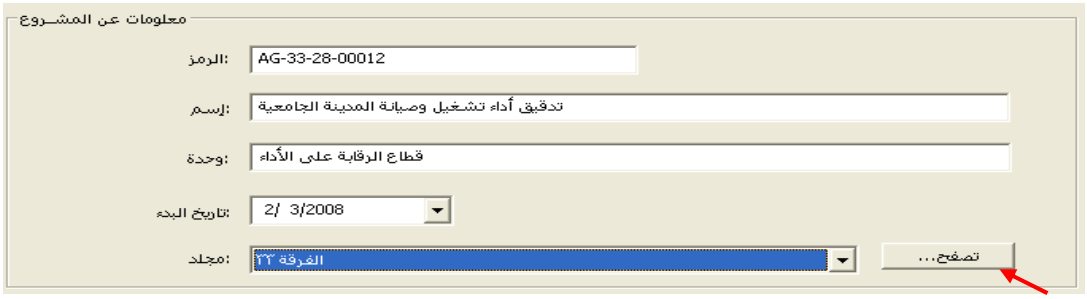
من مجلد اختر مكان تخزين المشروع أو الفرقة التابعة لها



- ثم اختر (التالي)
- ستظهر لك نافذة المكتبات (الخطوة الثانية) وهنا يتم اختيار المكتبة الخاصة بالفرقة أو الخاصة بنظام المكان الذي تعمل على تدقيقه

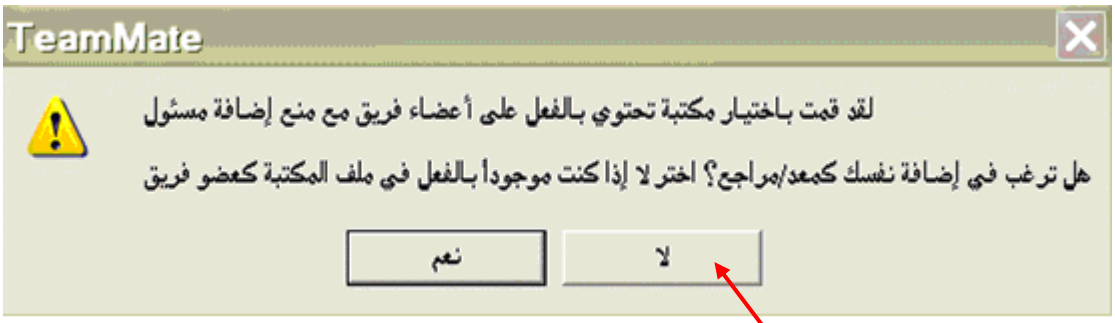
- لاختيار قالب مشروع من مكتبة Team Store اتبع الخطوات التالية :

1. اضغط على تصفح



اضغط هنا

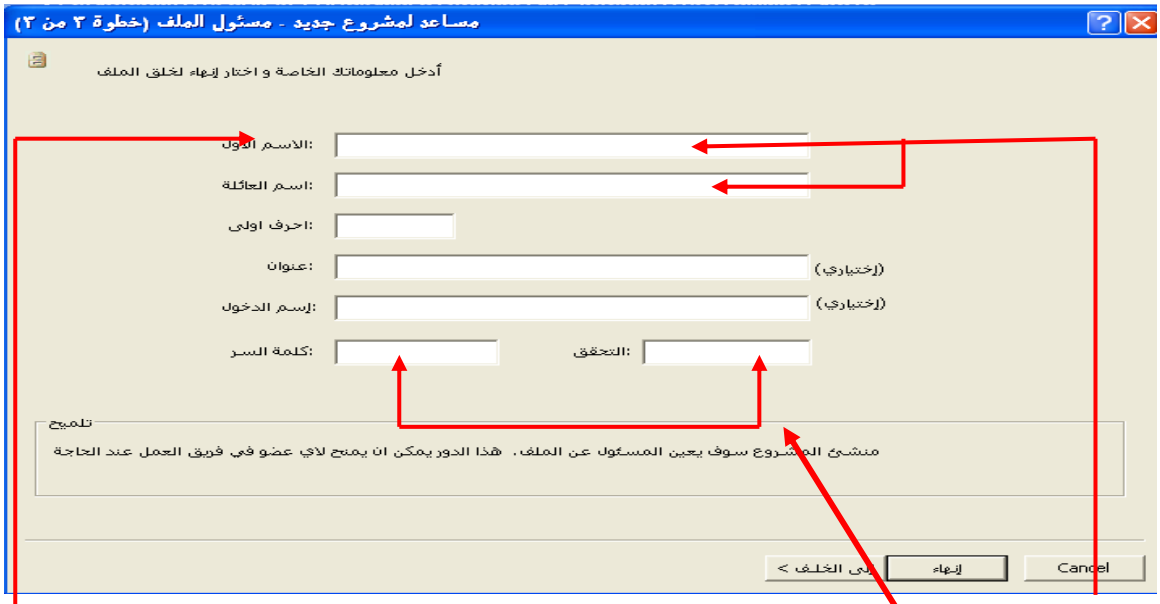
وبعد ذلك سوف تظهر لك النافذة التالية:



2. اختر(لا)

وبعد ذلك سيقوم برنامج التيم ميت بإنشاء المشروع الجديد وفق القالب الخاص بالفرقة التي تم اختيارها سوف تظهر لك الشاشة مسئول الملف (الخطوة الثالثة)

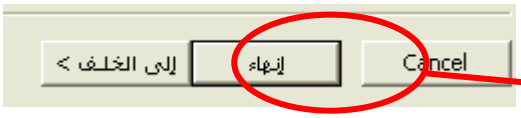
وبهذه الخطوة ستحدد من المسئول عن الملف وتعين كلمة مرور له , انظر الصورة.



ضع هنا اسم المسئول عن المشروع والذي سيكون مسئول عن إعداداته

ضع هنا التوقيع الخاص بك (رقمك الوظيفي)

هنا ستضع كلمة المرور الخاصة بالمسؤول عن الملف

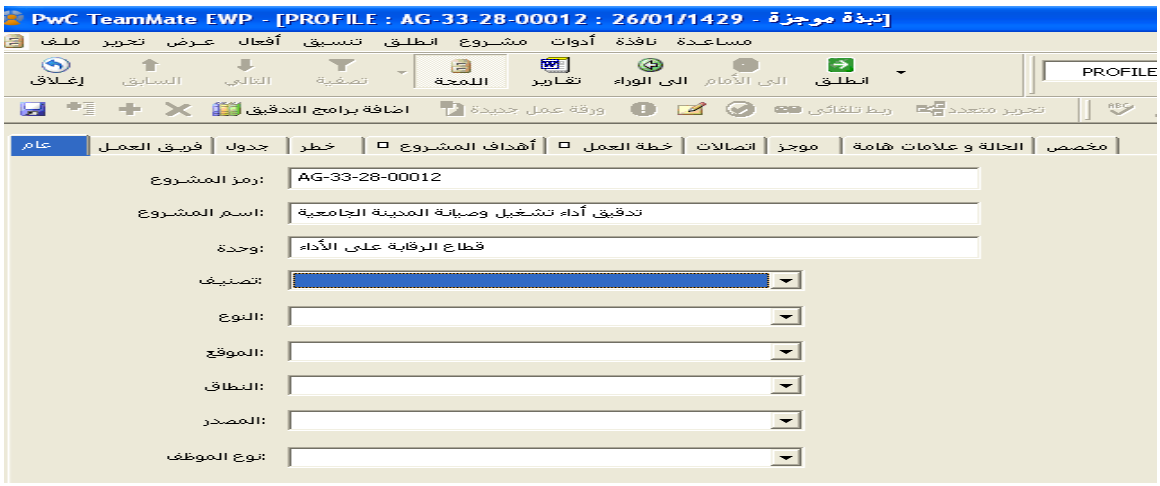


ثم الضغط على إنهاء

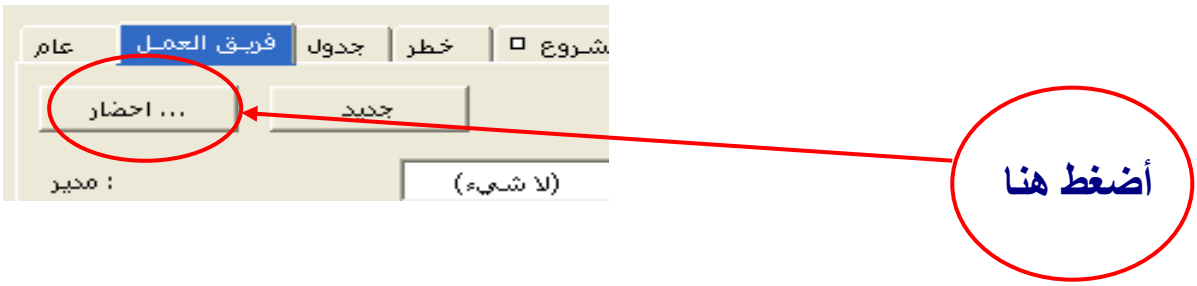
ثالثا : إكمال إعدادات المشروع وتحديد فريق العمل والأدوار :

بعد الانتهاء من إنشاء المشروع الجديد وفق القالب الخاص بالفرقة, يأتي دور المشرف بإكمال إعدادات المشروع وإضافة فريق العمل الخاص بهذا المشروع , ويتم عمل هذا من اختيار علامة التبويب (اللمحة)

وبعد الضغط على اللمحة سوف تخرج لك شاشة المتصفح نبذة موجزة وتبدأ بتعبئة الخيارات المتاحة لديك



ثم انتقل للاختيار فريق العمل والذي به تحدد فريق العمل وذلك بالضغط على إحضار



عندها سوف تظهر لك شاشة بأسماء المدققين

1. تختار المدقق بوضع علامة صح أمام اسمه
2. ثم الضغط على إضافة

أولا : اختر المدققين الذين تريد أن تضيفهم على المشروع بوضع إشارة صح أمام الاسم المراد اختياره

ثانيا: اضغط على إضافة لتحميل الأسماء المختارة على المشروع

المسؤوليات والرموز الخاصة بالمدققين:

المسئول عن الملف وهو المسئول عن الملف وإعطاء الصلاحيات وهو أيضا المسئول عن إعدادات المشروع

المعد فقط ويتم تخصيصه للمدقق الذي يراجع ويدقق ويفحص خطوات التدقيق داخل المشاريع

المراجع فقط وهو خاص بمشرفي الفرق ومشرفي الإدارات وهو مسئول عن مراجعة خطوات تدقيق المشروع دون عمليه إعداد وتدقيق خطوات التدقيق

معد/مراجع خاص لمدير الإدارة ومدير عام الإدارة وهو مسئول عن مراجعة وتعديل ومراجعة خطوات المشروع

للقراءة فقط لمن يصرح لهم بالإطلاع على المشروع دون التعديل عليه

رابعا : إحضار برامج العمل من مكتبة Team Store :

- الضغط بزر الفأرة الأيمن على علامة تبويب برنامج العمل واختيار: إحضار برامج التدقيق ، كما في الصورة التالية:

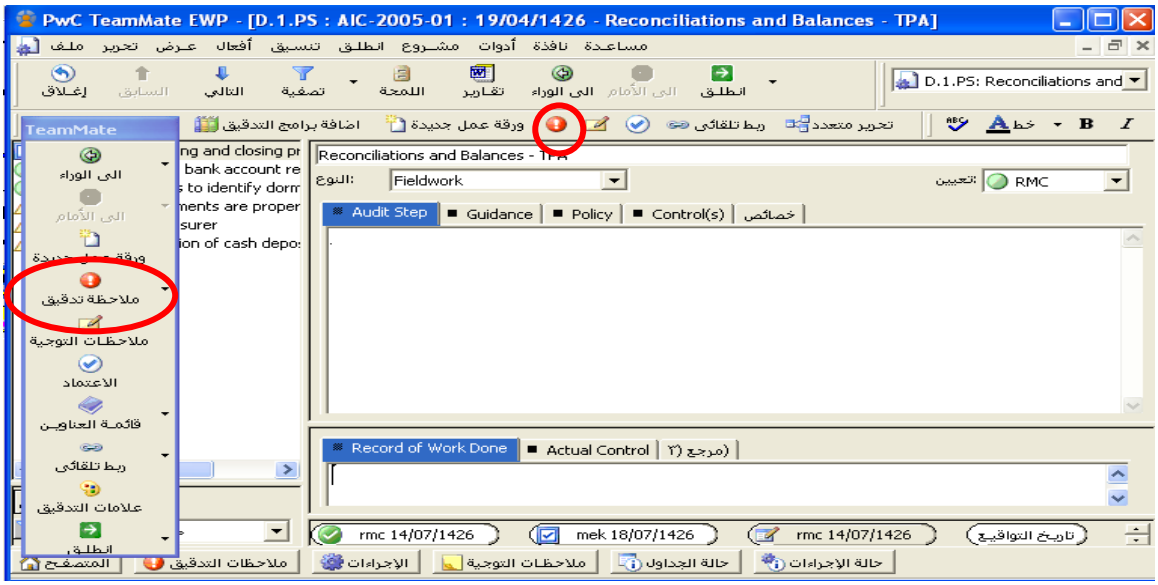
ومنها سوف تظهر الشاشة التالية و لإحضار برامج العمل الموجودة على شبكة الديوان

خامساً : ملاحظات التدقيق :

هي عبارة ملاحظات هامة أو جوهرية اكتشفت خلال عملية التدقيق أو المراجعة, وهي تنبه بوجود أمر خطير أو غير عادي قد يؤثر على طبيعة الحساب .

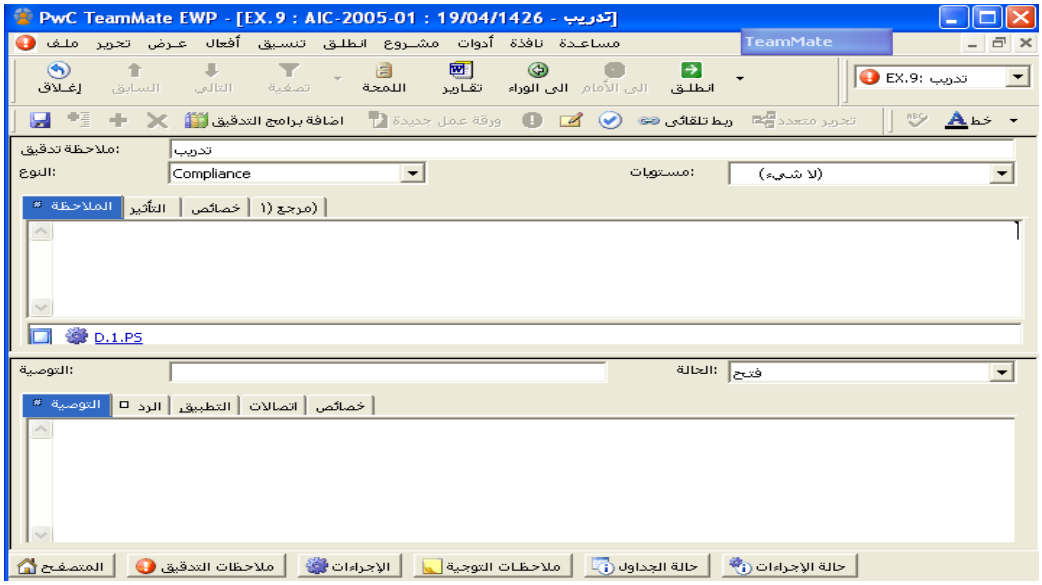
- **كيفية إنشاء ملاحظة تدقيق :**

تنشأ ملاحظة التدقيق بالضغط على شريط التيم ميت أو بالضغط على علامة ملاحظة تدقيق الموجودة بأعلى المتصفح كما هو موضح بالصورة

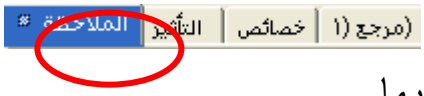


وبعد الضغط على علامة الملاحظة سوف تخرج لك شاشة إدخال ملاحظة جديدة ويتم إدخال عنوان للملحوظة ويتم اختيار نوع الملحوظة ومن ثم تضغط على الضغط (ok) كما هو مبين بالصورة

وبعد الإنهاء من الخطوة السابقة سوف تخرج لك هذه الشاشة



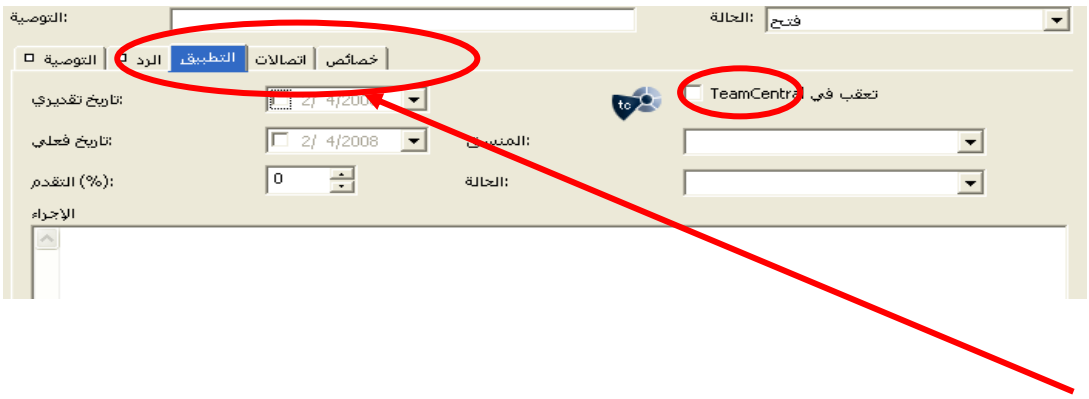
وتبدأ بملء الخانات الخاصة بالملاحظة وهي كالتالي:

الملاحظة:  ويكتب في هذه الخانة ما وجدت من ملاحظات والتعريف بها

التأثير : ويشرح بها مدى التأثير على الحسابات

- **الخصائص :** وبها تختار خصائص هذه الملحوظة من موقعها ومقدار الخطر(الخ..)
- **عنوان التوصية :** ويكتب بها عنوان للتوصية بحيث تظهر للقارئ عند مراجعتها

- **التوصية :** ثم تبدأ بوضع التوصيات وطريقة الحلول المفيدة للملاحظة في التوصيات
- **الرد :** يترك الرد في العادة إلى حين رد الإدارة المسئولة عن هذه الملحوظة وما تم اتخاذه فيها
- **التطبيق** : وهي من أهم الخانات بحيث يوضع تاريخ تقديري للتوصية وتوضع الحالة التي هي عليها ومن ثم يجب أن تضغط على تعقب في Team Central لكي تمكن الإدارة والجهات العليا من رؤية هذه الملاحظة ومنها تستطيع تعقب الملاحظة وما تم عليها من إجراءات



- **الاتصالات**:

وبها يوضع طرق الاتصال من هاتف وبريد الكتروني للشخص المسئول عن الملاحظة في (المؤسسة مكان التدقيق)

وعند الإنهاء يتم توقيع الملاحظة وإغلاقها من إغلاق

من شريط التيم ميت بضغط (اعتماد)

مصطلحات الحاسب الآلي

الهدف: تهدف هذه النشرة إلى تعريف المتدرب بالمصطلحات الأساسية المستخدمة في بيئة الرقابة الإلكترونية

(A
Administrator - المدير

شخص يقوم بإعداد مصادر الشبكة وتسجيل المستخدمين وأرقامهم السرية وصيانة المصادر.

Agent - عميل

في نظام (العميل/الموفر) (Client/Server) ، ذلك الجزء من النظام الذي ينفذ عملية إعداد وتبادل المعلومات نيابة عن برنامج المضيف Host أو الموفر Server.

Alert - تحذير

تقرير عن وجود خطأ بشكل صندوق تحذير أو صوت يطلقه الكمبيوتر.

ASCII - قاعدة المعايير الأمريكية لتبادل المعلومات

American Standard Code for Information Interchange معيار لتحويل الأحرف إلى أرقام وتحتوي على سبعة جزيئات بقيمة ثنائية تتراوح بين الصفر و 127.

Anonymous - مجهول

يتم استخدامه كاسم مستخدم للدخول على بعض الكمبيوترات البعيدة.

Authentication - التوثيق

تعريف هوية شخص أو الإجراءات الخاصة بذلك.

(B

Band Width - عرض النطاق

هي كمية المعلومات التي يمكنك إرسالها على خط معين في وقت محدد. عرض النطاق يقاس بعدد النبضات في الثانية Bits per Second وتكتب (bps).

BBS - لوحة إعلانات النظام

كمبيوتر مزود ببرامج معينة يوفر رسائل إلكترونية وملفات إضافة للخدمات الأخرى.

Binary - ثنائي

وسيلة عد تستخدم الرقمين 0 و 1 ، وهي الوسيلة التي يعمل بها الكمبيوتر داخلياً، وتحتوي الملفات الثنائية على ثمان جزئيات تتراوح بين صفر و 255

Browser - متصفح

برنامج يستخدم للإبحار في الشبكة العنكبوتية WWW.

(C

Client - تابع

جهاز كمبيوتر يقوم بطلب الخدمة من جهاز كمبيوتر آخر، فعندما يطلب كمبيوتر اشتراك مع موفر خدمة ISP فإنه يعتبر تابع لموفر الخدمة (ISP Client of).

Compression - ضغط

خطوات ضغط المعلومات لتخزين الملف في مساحة أصغر.

Connection - ربط

وسيلة اتصال بين جهازي كمبيوتر.

Crack - تخريب

مصطلح يطلق على برنامج يقوم بفك شفرة أحد البرامج المشتركة وجعله مجاني.

Cracker - مخرب

شخص يحاول الدخول على نظام ما دون تصريح ويسبب له أضرار.

(D

Data - بيانات
معلومات وبشكل خاص المعلومات المستخدمة بواسطة البرامج، أصغر وحدة في المعلومة يمكن للكمبيوتر فهمها هي bit.
Default - بديل افتراضي
قيمة أو فعل أو ترتيب يقوم الكمبيوتر بافتراضه في حال عدم قيام المستخدم بإعطاء تعليمات صريحة بخلاف ذلك. هذا النظام يمنع البرنامج من التعطل أو الاصطدام في حال عدم إعطاء قيمة بواسطة المستخدم.
Device - جهاز
1. **الأجزاء التي يتركب منها الكمبيوتر Hardware مثل الشاشة والطابعة وخلافه، هذه الأجزاء يمكن أن يطلق عليها أيضاً الأجزاء الخارجية Peripheral لأنها منفصلة بصورتها المادية عن الكمبيوتر ولكنها مربوطة به.**
2. **جزء من الكمبيوتر أو قطعة من الأجهزة الخارجية التي يمكنها نقل المعلومات.**
3. **أي قطع أو معدات يمكن ربطها بالشبكة مثل الكمبيوتر والطابعة وموفر الملفات وموفر الطابعة وخلافه.**

Dial-up - اتصال
استخدام التليفون أو ISDN لربط الكمبيوتر باستخدام مودم بخدمة الانترنت. وهي عكس الارتباط المستمر Permanent Connection وهذا يعني أنه كي تحصل على الخدمة فإنه عليك أن تعمل مكالمة هاتفية.
Domain - حقل
هو ذلك الجزء من الـ DNS الذي يحدد مكان شبكة كمبيوترك وموقعها في العالم.
DNS - نظام أسماء الحقول
Domain Name System هو نظام لتحديد العناوين الشبكية IP Addresses المطابقة للكمبيوترات المسماة والحقول Domains.. الـ DNS يتكون من سلسلة من المعلومات تفصل بينها نقاط.. خدمة أسماء الحقول Domain Name Service هي عبارة عن برنامج يقوم بتحويل أسماء الحقول Domain Names إلى عناوين شبكية IP Addresses.
(E
Electronic Mail البريد الالكتروني
يرمز له e-mail وهو نظام يمكن بموجبه لمستخدم الكمبيوتر تبادل الرسائل مع مستخدم آخر أو مجموعة مستخدمين بواسطة شبكة اتصال، ويحتاج البريد الالكتروني إلى برنامج بريد مثل: Outlook أو Eudora ليتمكن من الإرسال.
Emotion- رموز المشاعر
رموز تستخدم للتعبير عن المشاعر على الانترنت مثل « ابتسامة :) ، غضب :(»
Encryption - التشفير
هو معالجة كتلة من المعلومات بهدف منع أي شخص من قراءة تلك المعلومة باستثناء الشخص المقصود إرسالها إليه، وهناك العديد من أنواع التشفير.
(F
FAQs - الأسئلة المتكررة

Frequently Asked Questions وثيقة على الانترنت الغرض منها فحص وتدقيق المعلومات التي يحتاج إليها الكثير من الأشخاص بصفة متكررة.

Firewall - جدار نار

نظام تأمين لتقييد عملية الدخول على الكمبيوترات الموجودة على شبكة محلية LAN من أي مكان في الخارج.

Flame - التطهير

ردة فعل غاضبة لرسالة تم نشرها على Usenet أو القوائم البريدية Mailing List أو لوحات النقاش Message Boards ، التطهير يحدث لعدة أسباب مثل تعميم رسالة على الانترنت أو طرح سؤال توجد إجابته في الـ FAQs، حرب التطهير قد تحدث عندما يرد شخص تعرض للتطهير على الرسالة أو الرسائل التي وصلته.

(G

Gateway - بوابة

مصطلح (بوابة Gateway) لم يعد يستخدم حالياً ، والبوابة هي أداة أو برنامج اتصال يقوم بتسيير المعلومات من شبكة إلى أخرى.

Gopher - خدمة جوفر

نظام طورته جامعة مينيسوتا الأمريكية بهدف تسهيل عملية استخدام الانترنت وهو يعتمد على عملية البحث من خلال القوائم لقراءة الوثائق ونقل الملفات. Gopher يمكنه الإشارة إلى الملفات ومواقع Telnet ومراكز معلومات WAIS وغيرها.

(H

Hacker - متطفل

المتطفل هو الشخص الذي يشعر بالفخر لمعرفته بطرق العمل الداخلية للنظام أو الكمبيوتر أو الشبكات بحيث يسعى للدخول عليها دون تصريح.

Host - مضيف

غالباً ما يستخدم مصطلح (مضيف Host) للكمبيوتر الذي يتيح للمستخدمين الدخول عليه.

HTTP - بروتوكول نقل النص التشعبي

HTTP هي وسيلة تجعل من الممكن التصفح عبر وثائق الشبكة العنكبوتية، المستخدم يضغط على نقاط ربط موجودة على وثيقة الشبكة العنكبوتية مما يمكنه من الذهاب إلى تلك الوثيقة حتى لو كانت موجودة على جهاز آخر.

(I

ISDN - الشبكة الرقمية للخدمات الموحدة

Integrated Services Digital Network هي تكنولوجيا جديدة تحتوي على شبكات صوتية ورقمية في وسيلة واحدة وتعتبر خدمة اتصالات فائقة السرعة.

IP - بروتوكول الانترنت

Internet Protocol هو طبقة الشبكة الخاصة بحاشية بروتوكول TCP/IP والتي تستخدمها الأدوات على الانترنت للاتصال ببعضها. والـIP Address (عنوان بروتوكول الانترنت) هو العنوان الخاص بكل كمبيوتر متصل بشبكة ولكل عنوان الـIP طريقتين للكتابة إما رقمية (TCP/IP Address) مثل 212.26.66.3 أو حرفية (FQDN) وهي العناوين

التي نكتبها عادة في المتصفحات مثل ftp.empac.co.uk والعنوان الحقيقي هو الرقمي ولكن لصعوبة حفظه فنكتب العنوان الحرفي ولكن في الشبكة داخلياً يتم ترجمة العنوان الحرفي إلى العنوان الرقمي المطابق له.

ISP - مقدم خدمة الانترنت

Internet Service Provider هو الشركة التي يقوم المستخدم - عادة - بالاشتراك لديها للحصول على ربط بالانترنت، وهذه الشركة مرتبطة بالانترنت مباشرة من إحدى الشركات الأعضاء في CIX.

(J

JPEG

وسيلة لضغط الصور المستخدمة في الانترنت

(K

Kilobit - كيلو بت

وحدة قياس تعادل 1024 ب, وتستخدم عادة في تحديد الطاقة الاستيعابية للذاكرة

Kilobyte - كيلو بايت

وحدة قياس تعادل 1024 بايت.

(L

Layer - طبقة

شبكات الكمبيوتر قد تنظم على شكل مجموعة أعداد أكثر أو أقل من البروتوكولات المستقلة كل منها في طبقة Layer وقد تسمى مستوى Level.

Login - تسجيل

أي أن تقوم بتسجيل اسمك كمستخدم لنظام أو شبكة فيصبح لديك اسم مستخدم Login Name.

Log off - إنهاء عملية التسجيل

هو إخبار النظام بأنك أنهيت عملك وستقطع الارتباط.

Lurking - التواري

يستخدم هذا المصطلح للتعبير عن شخص ليس لديه مشاركة نشطة في مجموعة الأخبار أو لوحة النقاش أو قائمة البريد التي اشترك معها، ويفضل التواري للأشخاص المبتدئين الذين يريدون التأقلم في البداية مع الآخرين

(M)

Mailing List - قائمة بريد

قائمة بعناوين الكترونية لعدة أشخاص. كل شخص مشترك في هذه القائمة يرسل موضوعاً يخص اهتمامات هذه القائمة إلى كمبيوتر رئيسي يقوم بتحويل هذه الرسالة إلى جميع المشتركين في القائمة البريدية، هناك قوائم معدلة Moderated وتعني أن الرسالة ترسل في البداية إلى صاحب هذه القائمة ليدقق فيها وإذا تأكد من صلاحيتها يقوم بإرساله للبقية وهناك قوائم غير معدلة Un moderated وتقوم بإرسال الرسالة أوتوماتيكيا للمشتركين.

Megabyte - ميجا بايت

وحدة قياس تعادل 1024 كيلو بايت أو 1048576 بايت.

MIME - توصيلة بريد الانترنت المتعددة الأغراض
Multipurpose Internet Mail Extension نظام لتوفير القدرة على نقل البيانات غير النصية كالصور والصوت والفاكس من خلال البريد الالكتروني.
(N
Netiquette - آداب الشبكات
الالتزام بقواعد سلوك ملائمة عند استخدام الشبكة
NETBIOS - نظام شبكة المدخلات والمخرجات الأساسي
Network Basic Input/output System يسمح للأجهزة التي تعمل بنظام DOS من التحدث مع واستعمال خدمات الشبكة. نفس الاسم هو اسم بروتوكول شبكة محلية يستخدم بشكل واسع في منتجات ميكروسوفت.
Newsgroup - مجموعة أخبار
مجموعات الأخبار التي قد يصل عددها إلى 16.000 مجموعة تكون معاً الـUsenet، وهي بمثابة الصحف التي تناقش جميع موضوعات الحياة وأي موضوع قد يخطر ببالك، ومعظم موفري الخدمة يوجد لديهم موفر مجموعات أخبار Server Newsgroup.
(O
On-Line/Off-Line - متصل/غير متصل
On-Line تعني أن الكمبيوتر متصل حالياً بالشبكة وعكسه Off-Line أي غير متصل.
(P
PING - مجمع كتلة الانترنت
Packet Internet Grouper برنامج يستخدم لاختبار القدرة الوصولية وذلك بإرسال طلب صدى ICMP إليها وانتظار الرد
PPP - بروتوكول نقطة إلى نقطة
Point-to-Point Protocol إحدى وسيلتين لتبادل كتل البيانات عبر انترنت بواسطة خطوط الهاتف (الوسيلة الأخرى هي SLIP) بروتوكول PPP يوفر وسيلة ضغط للبيانات وتصحيح الأخطاء ولا يزال تحت التطوير.
POP - بروتوكول مكتب البريد
Post Office Protocol يسمح للمستخدم بتخزين رسائله في كمبيوتر شركة توفير الخدمة كي يقوم باسترجاعها فيما بعد، وهناك ثلاث طبعات لهذا النظام POP و POP2 و POP3.
Port - ميناء (منفذ)
تحديد موقع برنامج معين على كمبيوتر مضيف على الانترنت.. قبل سنوات قليلة كان على المستخدم تحديد البورت بنفسه ؛ المنفذ 23 خاص بالـTelnet والمنفذ 21 خاص بالـFTP، أما اليوم فمعظم البرامج تحدد المنفذ اتوماتيكياً.
Proxy - تفويض
طريقة يقوم بمقتضاها جهاز - موجه غالباً - بالرد على طلبات للدخول على مواقع معينة وبذلك يقوم بتنفيذ هذا الطلب بناء على الأوامر التي تلقاها وعلى التوجيه الذي صُمِمَ عليه.
(Q
Queue - صف

كتل احتياطية تنتظر المعالجة

(R

RAM - ذاكرة الدخول العشوائي

Random - Access Memory الجزء من ذاكرة الكمبيوتر الذي يقوم بتخزين المعلومات بصفة مؤقتة بينما هي تحت الاستخدام . أغلب الكمبيوترات تحتوي على 512 KB من ذاكرة الرام، هذه المعلومات إذا أغلقت الجهاز ولم تحفظها تختفي إلى الأبد.

Remote - بعيد

لا يمكن ربطه مباشرة باستخدام أسلاك محلية ولكنه يحتاج إلى أدوات اتصال.

Router - موجه

نظام كمبيوتر يتخذ القرارات الخاصة بتحديد اتجاهات الحركة على الانترنت.

(S

SLIP - بروتوكول الانترنت ذو الخط المتسلسل

Serial Line Internet Protocol هو بروتوكول يستخدم لتشغيل بروتوكول الانترنت IP على خطوط متسلسلة Serial Lines كدوائر الهاتف. عادة عند الارتباط بموفر خدمة يستخدم إما PPP أو SLIP.

Server - خادم (موفر)

جهاز يفتح للمستخدمين لتوفير الخدمات لهم كنقل الملفات وغيرها.. الشخص الذي يدخل على الـServer يسمى Client

Shell - المحارة

برنامج يوفر للمستخدم القدرة على التفاعل مع الكمبيوتر.

SMTP - بروتوكول نقل البريد البسيط

بروتوكول يستخدم لنقل البريد الالكتروني بين الأجهزة.

Spamming - التعميم

مصطلح يطلق على عملية تعميم رسالة في مجموعات الأخبار أو البريد الالكتروني. ويقابله التطهير Flaming.

Standard - معيار (افتراضي)

مجموعة من المواصفات لتصميم البرامج يتم الاعتراف بها من قبل بائعين أو منظمة رسمية.

(T

T1

مصطلح T&AT يعبر عن وسائل النقل الرقمية Digital التي تستخدم لنقل DS-1 الإشارات الرقمية المشكلة وذلك بسرعة 1.5 MB في الثانية (سرعة خارقة) وذلك باستخدام خط مؤجر Leased Line وهناك أيضاً T3 التي تستخدم لنقل DS-3 بسرعة 44.746 MB في الثانية.

TCP - بروتوكول التحكم بالنقل

يقوم هذا البروتوكول بتمرير المعلومات إلى بروتوكول الانترنت IP وهو مسئول عن التأكد من وصول الرسالة وأنها مفهومة.

Telnet - الاتصال عن بعد

Telnet هي بروتوكول انترنت معياري لخدمات الربط عن بعد ويسمح للمستخدم بربط جهازه على كمبيوتر مضيف جاعلاً جهازه وكأنه جزء من ذلك الكمبيوتر البعيد.

Trojan Horse - حصان طروادة

برنامج كمبيوتر يحمل داخله وسائل تسمح لمكونه الدخول إلى النظام الذي زُرعَ فيه.

URL - معين المصادر المنتظم

Uniform Recourse Locator وسيلة معيارية للإشارة للمصادر تقوم بتحديد نوع الخدمة بالإضافة إلى موقع الملف أو الدليل.

Unix - نظام يونيكس

نظام تشغيل تستخدمه معظم شركات توفير الخدمة ويقوم بربط عدة أجهزة تابعة Clients به للدخول عليه.

Usenet - شبكة المستخدم

شبكة من مجموعات الأخبار تتكون من 16.000 مجموعة أخبار تهتم بجميع شؤون الحياة.

(V

Virus - فيروس

برنامج يكرر ويضاعف نفسه عن طريق دمج نفسه بالبرامج الأخرى ويضر الكمبيوتر كثيراً.

(W

White Pages - الصفحات البيضاء

مراكز معلومات توفر خدمات ومعلومات عن أشخاص معينين.

Whois

برنامج يتيح لمستخدمه البحث في مراكز المعلومات عن أشخاص وعناوين.

WAIS

نظام يتيح لمستخدمه البحث عن موضوع معين باستخدام كلمات مفتاحيه Keywords.

Winsock

نظام التقاء في ويندوز، وإذا أردت الدخول على الانترنت فيجب أن يتوفر لديك ملف يدعى winsock.dll موضوع داخل النظام. المشكلة التي تتكرر كثيراً هي أنه ليس جميع البرامج تعمل مع نفس طبعة Winsock تطبيق trumpet الذي يستعمله الكثيرون يستخدم لتوفير ربط SLIP بين حاسباتهم وتقوم الانترنت بتوفير نسخة من Winsock.

WWW - الشبكة العنكبوتية العالمية

برنامج يعمل باستخدام نقاط ربط Hypertext link كي يتمكن المستخدم من التصفح بواسطة النقر على الروابط.

Worm - دودة

برنامج يكرر نفسه ولكنه يتكاثر في الشبكة بشكل مقصود بعكس الفيروسات، دود الانترنت الذي حدث عام 1988 ربما يكون الأشهر فقد استطاع الدود أن يتكاثر في أكثر من 6000 نظام.

WYSIWYG – ما تراه هو ما تحصل عليه

What You See Is What You Get هو مصطلح يطلق على بعض برامج تصميم صفحات الويب التي تتيح رؤية ما ستكون الصفحة عليه من خلال البرنامج نفسه وهو يطلق على البرامج التي تكتب لغة الهتمل في الخلفية نيابة عنك.

(X

X - Modem

بروتوكول يستخدم لنقل الملفات بين حاسبين عادة بواسطة مودم.

(Y

Yellow Pages - الصفحات الصفراء

خدمة تستخدم بواسطة إداريي UNIX بغرض إدارة مراكز المعلومات الموزعة عبر الشبكة.

Y - Modem

بروتوكول يستخدم لنقل الملفات بين حاسبين عادة بواسطة مودم.

(Z

Z - Modem

بروتوكول يستخدم لنقل الملفات بين حاسبين عادة بواسطة مودم.

Zone - نطاق

مجموعة من أدوات الشبكة Apple Talk.

انتهى بحمد الله

تمرين رقم (1)

الهدف: يهدف هذا التمرين إلى تقييم مدى ادارك المشاركين لدور أساليب الرقابة المدعومة بالحاسوب و مزايا استخدامها في الرقابة والاعتبارات والمسائل التي يجب أخذها بعين الاعتبار عند استخدامها.

الوقت المخصص:

بقديم الحالة : عشرة دقائق

مناقشة المجموعة: عشر خمسة عشر دقيقة

استخلاص المعلومات في وجود جميع الأعضاء: عشر دقائق

تفاصيل الحالة:

قبل الشروع في تنفيذ مهمة رقابية اجتمع مدير العام لإدارة الرقابة على الشركات بالجهاز برئيس وأحد أعضاء فريق الرقابة المكلف بتنفيذ المهمة الرقابية لدى إحدى البنوك.

(أ) في البداية صرح المدير العام بالأهمية القصوى لهذه المهمة بحكم انها أول تجربة سيخوضها الجهاز في مجال الرقابة الشاملة (رقابة مالية ومطابقة وأداء) على المؤسسات البنكية ومن ناحية ثانية حجم الشركة وكذلك نظرا لحجم المعاملات. وحث المدير العام رئيس الفريق على مزيد العمل وتضافر جهود كل أعضاء الفريق لكسب هذا الرهان.

(ب)وبعد ذلك تدخل رئيس الفريق وعبر عن صعوبة المهمة نظرا لعدم توفر الخبرات لدى الجهاز في مجال الرقابة على المؤسسات البنكية من ناحية والعدد هام لفروع البنك وحجم المعاملات. وعلى هذا الأساس لا يمكن للفريق تغطية كل المجالات والعمليات بحيث سيقتصر الفريق في عمليات الفحص على عينات فقط . كما طلب رئيس الفريق من المدير العام تمكينه من أكبر عدد ممكن من المراقبين ومدة زمنية طويلة لكي يتمكن من تنفيذ هذه المهمة.

(ج) وعندها تدخل عضو الفريق الذي كان حاضر في الاجتماع والذي أنهى من مدة شهر دورة تدريبية حول الرقابة على تقنية المعلومات، وبين إنه بالإمكان إنجاح هذه المهمة بأقل عدد ممكن من المراقبين وفي فترة زمنية معقولة لو استخدمنا أساليب الرقابة المدعومة بالحاسوب.

(د) تدخل المدير العام وطلب من العضو تقديم أكثر التفاصيل على ما اقترحه. فبين أن استخدام هذه الأساليب من شأنه أن يفيدنا على مستوى تخطيط وتنفيذ المهمة، كما أنها تمكننا من تحليل كامل للبيانات التي تهم مجال أو نشاط معين عوضا عن عينات فقط ومن ناحية ثانية ستمكننا من القيام بالعديد من الاختبارات الرقابية في وقت قصير بحيث يمكننا تغطية أهم مجالات البنك.

(ه) فتدخل رئيس الفريق مبينا أنه لا يمكن استخدام هذه الأساليب نظرا لكلفتها العالية من شراء حاسبات محمولة وبرمجيات الرقابة وتدريب المراقبين عليها. بالإضافة إلى ذلك لا تستخدم هذه الأساليب إلا في الرقابة المالية في حين أننا مطالبون بالقيام برقابة المطابقة وتقييم الأداء، هذا علاوة على الأخطار التي يمكن أن تتسبب فيها للبنك مثل اضطراب الأنظمة المستخدمة وإتلاف أو تغيير على مستوى البيانات. وعلى هذا الأساس لا أوافق استخدام هذه الأساليب في هذه المهمة.

المطلوب : ما هو رأيكم في هذا الموضوع.

الحل المقترح للتمرين رقم (1)

1- تأثير استخدام أساليب الرقابة المدعومة بالحاسوب على المدة الزمنية للمهمة الرقابية وعدد المراقبين لتنفيذها :

استخدام أساليب الرقابة المدعومة بالحاسوب في العملية الرقابية من شأنه أن يقلص من المدة الزمنية وتمكن من ربح الوقت بحكم توفر العديد من البرامج المتخصصة في الرقابة والتي تمكن من القيام بتحليل كم هائل مت البيانات في وقت وجيز. بالإضافة إلى ذلك يمكن الاحتفاظ بالمعطيات واستخدامها في مهمات رقابية لاحقة وبالتالي كل هذه العوامل من شأنها كذلك التقليص في عدد أعضاء فريق الرقابة.

2- أساليب الرقابة المدعومة بالحاسوب وتخطيط وتنفيذ المهمة الرقابية :

يعود استخدام أساليب الرقابة المدعومة بالحاسوب بالفائدة على المهمة الرقابية خاصة على مستوى التخطيط والتنفيذ ، من ذلك بالإمكان اختيار نطاق أوسع وأشمل للمهمة وتغطية أكبر عدد من المجالات الرقابية ومنح الأولوية للمجالات الرقابية ذات المخاطر العالية. كما أن إمكانية استخدام المعطيات مخزنة بواسطة أساليب الرقابة المدعومة بالحاسوب خلال المهمات الرقابية المستقبلية من شأنه أن يؤثر على تنفيذ وتخطيط المهمة الرقابية على مستوى المدة الزمانية وتركيبة فريق الرقابة.

3- تحليل جميع البيانات عوضا عن الاقتصار على العينات :

عند استخدام الأساليب اليدوية لا يمكن تحليل كل بيانات الجهة الخاضعة للرقابة خاصة بالنسبة للجهات كبيرة الحجم، وبالتالي يقتصر المراقب في هذه الحالة على عينة من البيانات لتحليلها والاعتماد عليها للمصادقة على بقية البيانات، إلا أنه بإستخدام أساليب الرقابة المدعومة بالحاسوب بالإمكان تحليل جميع البيانات المتوفرة إلكترونيا لدى الجهة وفي وقت وجيز باستخدام بعض برامج الرقابة المتوفرة .

4 - القيام بعدد هام من الاختبارات :

إن أغلب برامج الرقابة المعممة والمتوفرة للمراقبين تشتمل على عديد الوظائف التي تمكن من إجراء العديد من الاختبارات على البيانات المتوفرة لدى الجهات الخاضعة للرقابة. ومن أهم هذه الاختبارات يمكن ذكر عمليات التجميع والمقارنات والتقارير الاستثنائية والتقادم والتسجيلات المتكررة وكشف الثغرات. كما تجدر الإشارة إلى أنه حتى بالنسبة للبرامج الأخرى بإمكان المراقب برمجة عديد الوظائف التي تمكنه من اختبار البيانات المتوفرة.

5- كلفة أساليب الرقابة المدعومة بالحاسوب :

يتطلب استخدام أساليب الرقابة المدعومة بالحاسوب رصد مبالغ مالية هامة لاقتناء المعدّات والبرامج وتدريب المستخدمين. إلا أن هذا لا يعني أن استخدام أساليب الرقابة المدعومة بالحاسوب هي عملية غير مجدية في كل الحالات ، حيث يجب القيام بدراسة جدوى يقارن فيها الكلفة مع الفائدة أو العائد من استخدام هذه الأساليب. كما تجدر الإشارة إلى أن الأموال المخصصة لحيازة واستخدام هذه الأساليب تعتبر بمثابة الاستثمار وبالتالي سيستخدم لفترة طويلة والعائد سيكون حتما هاما ويغطي التكلفة .

6 - استخدام أساليب الرقابة المدعومة بالحاسوب بصفة حصرية في الرقابة المالية :

لا تستخدم هذه الأساليب بصفة حصرية فقط في أعمال الرقابة المالية بل يمكن استخدام تحليل البيانات في رقابة الأداء وأيضًا الرقابة التفتيشية. يستخدم لـ CAATs كذلك لتحليل بيانات الجهة الخاضعة للرقابة وهذا هو الأسلوب السائد بسبب سهولة استخدامه. ويتوفر لتحليل البيانات تشكيلة من برمجيات التدقيق وأدوات لغة SQL ، والتي صممت بصفة عامة للاستخدام في أنظمة الحاسب الشخصي.وتتلاءم هذه الأدوات مع رقابة المطابقة والأداء والرقابة القضائية / التفتيشية بالإضافة إلى التدقيق المالية.

7- المخاطر المحتملة من استخدام أساليب الرقابة المدعومة بالحاسوب

لا يخلو استخدام أساليب الرقابة المدعومة بالحاسوب من بعض المخاطر تتعلق بقواعد البيانات وأنظمة تقنية المعلومات للجهة الخاضعة للرقابة ، خاصة عندما يتمّ تشغيل هذه الأساليب على نظام تقنية المعلومات الخاص بالجهة الخاضعة للرقابة، سواء مباشرة من حاسب شخصي أو شاشة طرفية أو عن طريق توصيل حاسب المراقب بشبكة الجهة الخاضعة للرقابة. ومن بين المخاطر المحتملة يمكن ذكر اضطرابات الأنظمة و تغيير أو حذف بيانات الجهة الخاضعة للرقابة بدون قصد واضطراب على مستوى أداء وتكامل البيانات. ولتفادي هذه المخاطر بإمكان المراقب تنزيل البيانات على نظام تقنية المعلومات الخاص أو جهاز الرقابة وتشغيل CAAT من حاسبه. في هذه الحالة يجب التأكد من صحة وشمولية البيانات المنزلة.

تمرين رقم (1)

الهدف: لتحديد عناصر التحكم المادية والبيئية

الوقت المخصص:

القراءة الفردية: خمسة دقائق

مناقشة المجموعة الفرعية: خمسة عشر دقيقة

استخلاص المعلومات في وجود جميع الأعضاء: خمسة عشر دقيقة

إن الهدف من سيطرة الوصول المادية هو منع الوصول الغير مصرح إلى خدمات تقنية المعلومات. يمكن أن تتراوح عناصر تحكم الوصول المادية من الأنواع المختلفة للأبواب إلى وسائل التحكم الإجرائية الإدارية البسيطة. على نحو مماثل، فإن عناصر تحكم البيئية من أجل منع، كشف وخمد أي ضرر على خدمات تقنية المعلومات من الأخطار البيئية مثل الماء، مصدر الطاقة إلخ،

الجزء الأول

أنت مطالب بأن تناقش في المجموعة الخاصة بك عناصر تحكم المتعددة لأي من العناصر المُعطاة أدناه (ستُخصص عناصر التحكم للمجموعة):

- عناصر تحكم المادية
- منع الحرائق، الكشف والإخماد
- منع ضرر الماء، عناصر تحكم الصيانة وإدارة المرافق .
- حماية وتحكم مصدر الطاقة

بعد مناقشة وسائل السيطرة المتعددة التي قد تكتب في ورقة تعليمات.

الجزء الثاني

I. بعد أن تنتهي المجموعة من كتابة ورقة التعليمات الخاصة بهم بقلم الألوان الذي تم إعطاءه لمجموعتهم ويجب أن يمروا على ورقة التعليمات باتجاه عقارب الساعة للمجموعة التالية.
II. سيلاحظون في استلام ورقة التعليمات للمجموعة الأخرى نقاط إضافية بقلم الألوان الخاص بهم ووضع أيضًا علامة متقاطعة على النقاط التي لا يوافقون عليها. يمكن أن يتم هذا التمرين فقط حتى تُشغل الموسيقى. عندما تتوقف الموسيقي ستمر ورقة التعليمات باتجاه عقارب الساعة إلى المجموعة التالية.
III. قم بتكرار الخطوة (الثانية) حتى يرى جميع المجموعات ورقة تعليمات جميع المجموعات الأخرى.

الحل المقترح للتمرين رقم (1)

1- عناصر التحكم المادية :

ا- إجراءات إدارية :
موظفون يلبسون شارات هوية أو أسماء .
إلغاء حقوق الوصول للموظفين المطرودين .
الزوار : دخول الزوار يتطلب معرفة من هم , لصالح من يعملون , من يزورون , تاريخ الوصول , تاريخ الخروج . قد يطلب منهم تزويد نوع من أنواع التعريف قبل السماح لهم بالدخول او قد يتم مرافقتهم .

إجراءات مكتبية: وبمعنى أخر ما هي الإجراءات التي تتم عندما يترك الموظفون مكاتبهم مثلا عندما يذهب الموظفون منازلهم في الليل او عندما يخرجون لتناول الغداء . توضع أجهزة الكمبيوتر المحمولة في إدراج ويقفل عليها ويقفل على الأقراص المرنة ايضا.

ب- أقفال على الأبواب :
- **أبواب أقفال ميكانيكية .**
- **أبواب أقفال ممزوجة (مفتاح وأرقام)**
- **أبواب أقفال الكترونية .**
- **أبواب أقفال حيوية .**

عناصر تحكم أخرى .
- **كاميرات فيديو .**
- **حراس امن .**
- **أسوار خارجية للمباني**
- **أجهزة إنذار .**

2- منع وكشف وإخماد الحرائق :
- **منع التدخين .**
- **استخدام مواد بناء ضد الحرائق .**
- **أجهزة إنذار اكتشاف الأدخنة .**
- **معدات إخماد الحرائق مثل الماء والغاز .**

3-الماء وإدارة المرافق :
- **غرفة الحاسوب في مكان مرتفع وليست في السرداب .**
- **غرفة الحاسب بعيدة عن أماكن انحدارات المياه او خزانات المياه .**
- **أجهزة إنذار اكتشاف المياه .**
- **منع الأطعمة والاشربة في غرفة الكمبيوتر .**
- **التنظيف المنتظم لغرفة الكمبيوتر .**

4- مزود الطاقة :

- **مثبتات الفولتية .**
- **المولدات الاحتياطية .**
- **أجهزة تزويد التيار الغير متقطع .**
- **كابلات التيار البديلة .**

تمرين رقم (2)

الهدف من هذا التمرين تعليمك المفاهيم لقاعدة البيانات وإنشاء جدول وتعريف حقوله.

1. المطلوب منك إنشاء أسماء الحقول وتعريف خصائصها
2. المطلوب منك تفريغ محتويات هذا الجدول ووضع البيانات تحت أسماء الحقول المناسبة واختيار المفتاح الرئيسي والمفتاح الفرعي

Basic Information of Employee

783315 Mohamed Riyami 1/4/1969 25/6/1992 Sr.Auditor A+ Oman 4200 Second	849520 Hakeem BenAzraq 27/3/1966 23/3/1991 Director O+ Tunis 5000 First
533424 Fatima Salem 13/8/1974 1/9/1999 Auditor B+ Jordan 3900 Third	984329 Ali Kawari 16/4/1964 10/5/1988 Supervisor A+ Qatar 4900 Second

Data Table

Table Property

Field	Type	Size

الحل المقترح

الحل المقترح للتمرين رقم (2)

Data Table

EmpId	FName	LName	DOB	DOJ	Position	Bgroup	Country	Basic	Grade
783315	Mohamed	Riyami	1/4/1969	25/6/1992	Sr.Auditor	A+	Oman	4200	Second
849520	Hakeem	BenAzraq	27/3/1966	23/3/1991	Director	O+	Tnis	5000	First
533424	Fatima	Salem	13/8/1974	1/9/1999	Auditor	B+	Jordan	3900	Third
984329	Ali	Kawari	16/4/1964	10/5/1988	Supervisor	A+	Qatar	4900	Second

Table Property

Field	Type	Size
EmpId (PK)	Number	6
FName	Character	15
LName	Character	20
DOB	Date	8
DOJ	Date	8
Position	Character	15
Bgroup	Character	3
Basic	Number	Double
Grade	Character	10

تمرين رقم (2)

الوقت المخصص: خمس وثلاثون دقيقة

القراءة الفردية: خمسة دقائق

مناقشة المجموعة الفرعية: خمسة عشر دقيقة

استخلاص المعلومات في وجود جميع الأعضاء: خمسة عشر دقيقة

الهدف: يُعد هدف التمرين هو تحديد/ اقتراح وسائل سيطرة متعددة للوصول المنطقي الذي يمكن أن يُستخدم لمنع/تقليل المخاطر في الحالات المختلفة المُقدمة أدناه:

أ) بينما يتعامل نظام المعاشات المُدار بالكمبيوتر مع طباعة أوامر دفع المعاشات متضمنة مبالغ كبيرة من المال، فقد أرادت الإدارة جعل الأفراد مسؤولين عن الإضافات/التعديلات للبيانات

ب) هناك خطر وهو محاولة الموظفين الذين تم وقفهم عن العمل بتخريب النظام.

ج) أثناء محادثة عارضة، فقد وجد المراجع بأن السيد جاك كان يستخدم نفس كلمة السر لأكثر من سنتان.

د) كلمة السر الخاصة بالسيد خالد هي abc.

ه) بينما كانت الأنسة منى مُدخلة بيانات فقط، فقد أراد السيد لين، وهو مسؤول النظام بتعيين متطلبات الوصول المطلوب الأدنى.

و) تلبّي تطبيقات البرامج حاجة المبيعات والمالية والمخازن وأقسام إدارة المقترضين والموظفين في هذه الأقسام التي تستخدم التطبيق.

ز) أراد السيد علي، وهو مسئول النظام، التأكد من إنه لا يتم استخدام تطبيق البرنامج في العطلات بدون تصريح خاص.

ح) أراد السيد أحمد، وهو مسؤول أمن تقنية المعلومات، بأن يتم إخباره بصورة دورية بمحاولات تسجيل الدخول الفاشلة.

ط) ووجدت الأنسة سلوى، وهي المراجع، أثناء تفتيش عرضي لموقع الكمبيوتر بأن كثير من المداخل الطرفية ما زالت مُسجلة الدخول إلى نظام التطبيق.

ي) أثناء محاولة الأنسة حنان ، وهي المراجع، بفحص مداخل التحكم، حاولت تسجيل الدخول للنظام عن طريق تخمين ثلاثين كلمة سر مُختلفة ولكنها لم تستطيع الوصول لأن كلمة السر ليست سهلة حتى يتم خرقها.

الحل المقترح للتمرين رقم (2)

أ- يجب أن يكون لكل مستخدم رمز تعريف فريد، و يجب أن يتم تخزين رمز تعريف لآخر أو المستخدم الأخير الذي عدل البيانات ويجب أن تخزن في قاعدة البيانات لتثبيت المسئولية .

ب- يجب أن يكون هناك إجراءات بها تفاصيل إنهاء الخدمة لموظف أو تحويله ويتم إبلاغ مسئول النظام بهؤلاء المستخدمين لإلغاء رمز التعريف الخاص بهم .

ج- يجب أن يجبر النظام المستخدمين بشكل آلي ليغيروا كلمات سرهم في الفترات المحددة , فترة تغيير كلمة السر يمكن أن تتفاوت طبقا لصنف المستعمل , فالمستخدمين المهمين مثل المبرمجين يجب أن تتغير كلمات سرهم بشكل أكثر .

د- طول كلمة السر يجب أن تحدد , قد تكون مابين 6 إلى 8 رموز .

- يجب ان يضمن النظام أن كلمة السر هي مزيج حرفي رقمي .
- يجب نصح المستخدمين أن لا يخصصوا كلمات السر التي يمكن ان تخمن بسهولة .

ه- حقوق القراءة والكتابة هي التي يمكن ان تزود بينما حقوق التعديل او الحذف فلن تزود

- حقوق الدخول إلى الجداول الرئيسية لن تزود .
- برنامج دخول مكتوب قد يزود للدخول الضروري .
- كتابة برنامج خاص للدخول إلى أماكن معينة فقط

و- يجب تخصيص برامج دخول منفصلة في التطبيق .

- يجب أن يخصص المستخدمون وصول أو دخول إلى الوحدات ذات العلاقة بهم .
- دخول من خلال أطراف معينة ومخصصة للأقسام المعنية فقط.
- دخول طرفي محدد حيث أن وحدات طرفية معينة مخصصة لكل قسم .

ز- تحديد أوقات وأيام يسمح بالدخول إلى التطبيق .

ح- سجل تدقيق لتسجيل محاولات الدخول الفاشلة .

- مسئول الأمن يجب أن يبلغ رسميا في فترات معينة بأي انتهاكات أمنية .
- انقطاع الكهرباء أو غلق تلقائي للمحطات الطرفية المهملة لفترة معينة .

ي- يجب أن يكون هناك حد أقصى لعدد محاولات الدخول بحيث انه إذا تم إدخال كلمة السر الخاطئة لأكثر من عدد محدد فان تعريف المستخدم يجب أن يقفل بشكل ألي .