المحاضرة الثالثة: الرقابة الداخلية في ظل نظم المعلومات المحوسبة

أولا: الحاسوب ونظام الرقابة (الآثار والمشاكل)

1. الآثار الإيجابية للحاسوب في نظام الرقابة:

–التكامل والكفاءة: يعمل الحاسوب على تكامل الأنشطة الرقابية، فيسمح بالتعامل مع البيانات الضخمة وتوفير حلول رقابية قائمة على الذكاء الصناعي والتحليل المتقدم.

–السرعة في التنفيذ: يوفر الحاسوب القدرة على تنفيذ العمليات الرقابية بشكل أسرع من التدقيق اليدوي، مما يُسرّع عملية اتخاذ القرارات في الوقت المناسب.

–التحكم وتحليل البيانات: الحاسوب يسهل تحليل كميات هائلة من البيانات بدقة عالية، مما يسمح بإجراء الرقابة على نطاق واسع وبتكلفة أقل، ويقلل من تدخل العنصر البشري، ما يقلل بدوره فرص الخطأ البشري.

2. المشاكل المرتبطة باستخدام الحاسوب في نظام الرقابة:

–ارتفاع مخاطر الاختراق: يُعد النظام المحوسب عرضة للتهديدات الإلكترونية مثل الهجمات الخبيثة واختراقات الخصوصية.

–صعوبات الصيانة والتحديث: الأنظمة المحوسبة تتطلب تحديثات مستمرة لتبقى متوافقة مع أحدث معايير الأمان، الأمر الذي قد يكون مكلفًا ومعقدًا.

–التحديات البشرية: قلة خبرة العاملين في نظم المعلومات أو افتقارهم للتدريب اللازم قد يؤدي إلى ضعف نظام الرقابة. التدريب المستمر للعاملين يعد ضرورة لتجنب المخاطر.

ثانيا: الرقابة على التطبيقات

الرقابة على التطبيقات تعتبر من أهم الإجراءات التي تضمن سلامة البيانات وتعزز من موثوقية النظام المحوسب. وتشمل أنواع الرقابة المختلفة:

1. **الرقابة على المدخلات:** تعتمد على وضع آليات التحقق والتأكد من أن جميع البيانات المدخلة خالية من الأخطاء. تشمل هذه الرقابة ما يلي:
   - الفحص التلقائي للبيانات: مثلا، التحقق من أن جميع الحقول الضرورية قد تم ملؤها.
   - التأكد من شكل البيانات: كالتأكد من أن الأرقام السالبة أو القيم الغريبة غير مسموح بها في بعض الحقول.

2. **الرقابة على العمليات:** وهي تشمل التأكد من أن كل عملية داخل النظام تتم وفق القواعد المحددة مسبقًا، وتشمل:

- التنبيه التلقائي: إرسال تنبيهات في حال تم تعديل بيانات حساسة أو إجراء عمليات غير طبيعية.
- سجلات التدقيق: الاحتفاظ بسجلات رقمية لكل العمليات التي تمت داخل النظام، ما يسهل تعقب الأنشطة غير المشروعة.

3. **الرقابة على المخرجات:** للتأكد من أن جميع البيانات الصادرة من النظام دقيقة وصحيحة قبل استخدامها، وذلك من خلال:

- **التقارير النهائية:** التأكد من مراجعة التقارير النهائية قبل استخدامها.
- **التحقق من التعديلات:** في حال تم التعديل على البيانات قبل إنتاج التقارير، يتم توثيق من قام بالتعديل ومتى تم.

ثالثا: الرقابة في ظل التشغيل الإلكتروني للبيانات

تتطلب الرقابة في بيئة التشغيل الإلكتروني إجراءات خاصة (رقابة الوصول :Access Control)، تتم من خلال:

1. **إدارة الهويات والصلاحيات:** التأكد من أن الوصول إلى البيانات يتم وفق صلاحيات محددة مسبقًا، ويمكن تحسين الرقابة عبر نظام متعدد الطبقات يتطلب موافقات من مستويات إدارية مختلفة.
2. **التحقق الثنائي:** اعتماد التحقق الثنائي للدخول إلى النظام، بحيث يحتاج المستخدم إلى عنصرين للتحقق من الهوية (مثل كلمة المرور ورمز يُرسل عبر الهاتف).
3. **التحكم في العمليات الإلكترونية:** مثل المراجعة التلقائية للبيانات عند انتقالها بين الأقسام، والتحقق من أن النظام يعمل وفق السياسات والإجراءات المعتمدة.
4. **التدقيق الدوري للبيانات الإلكترونية:** يتم عبر تشغيل أدوات تحليل البيانات لاكتشاف أي أنماط غير طبيعية قد تشير إلى نشاط غير مشروع، مثل استخدام أدوات تحليل السجل (Log Analysis).

رابعا: الرقابة والتوثيق للمعلومات الإلكترونية

لضمان توافر وسلامة المعلومات الإلكترونية، يتم اتباع سياسات توثيق دقيقة:

1. **التوثيق المحاسبي الإلكتروني:** يشمل توفير نظام مستند إلى السحابة أو قواعد البيانات المركزية لتخزين كل العمليات المحاسبية بطريقة مشفرة تحافظ على الخصوصية.
2. **التوثيق القانوني:** يتم وفقًا للوائح والمتطلبات القانونية لضمان مطابقة النظام مع المعايير.
3. **نظام النسخ الاحتياطي الآمن:** الاحتفاظ بنسخ احتياطية للبيانات إلكترونيًا مع إمكانية استعادتها بشكل دوري للتحقق من سلامتها.

خامسا: مبادئ الرقابة في النظام المحاسبي

تعتمد الرقابة في النظام المحاسبي على عدة مبادئ لضمان فاعلية النظام:

1. **مبدأ التحقق المتبادل:** التأكد من أن جميع العمليات المحاسبية يتم التحقق منها من قبل أكثر من شخص.
2. **التوثيق المسبق لكل عملية:** حيث يتم تسجيل كل معاملة فور وقوعها دون تأخير.
3. **الفصل بين العمليات المتكاملة:** على سبيل المثال، يتم فصل مسؤولية إدخال البيانات عن مسؤولية مراجعتها لضمان موضوعية الرقابة.

سادسا: تقييم نظام الرقابة في ظل نظام المعلومات المحوسب

لتقييم كفاءة وفعالية نظام الرقابة، يجب اتباع خطوات منهجية:

1. **تحليل كفاءة النظام:** عبر استخدام أدوات متخصصة لتقييم قدرة النظام على تنفيذ عمليات الرقابة دون أخطاء أو تأخير.
2. **التدقيق الداخلي والخارجي:** حيث يقوم فريق التدقيق الداخلي بفحص نظام الرقابة بشكل دوري، مع الاستعانة بجهة خارجية في بعض الأحيان لضمان موضوعية التقييم.
3. **التقييم المستمر لمستوى الأمان:** من خلال اختبار قابلية النظام للاختراق واكتشاف الثغرات الأمنية عبر عمليات التدقيق المتخصصة، مثل اختبار الاختراق (Penetration Testing).