مقياس: إدارة تكنولوجيا المعلومات
السنة الثالثة ليسانس – إدارة الأعمال
أستاذ المادة: د. حريرش ناجي

المحور السابع:
الرقابة على نظم المعلومات

المحتويات:

أولا: أهمية الرقابة على نظم المعلومات الإدارية

1- الدقة في توفير المعلومات الضرورية:

يقصد بالدقة في توفير المعلومات التحرر من الاخطاء والتحريف وذلك من خلال اعتماد أسلوب الرقابة الملائمة على المدخلات والمخرجات والعمليات ، ونظراً للصعوبات التي قد تكتنف عملية الوصول إلى الدقة المطلوبة وخاصة بعد زيادة درجة تعقيد البيئة التي في ظلها تعمل المنظمات التي يوجد فيها نظام المعلومات لذا يقتضي الامر تحديد المستوى الملائم من الدقة المطلوبة وتقدير التكاليف المترتبة عليها . وعند القيام بتحديد هذا المستوى يجب تحليل المجالات الوظيفية في المنظمة وصولاً إلى تحديد حاجة كل مجال منها إلى الدقة المطلوبة ، وتكمن مبررات ذلك في ان بعض المجالات قد تحتاج إلى دقة عالية جداً تصل نسبة (100%) ومجالات اخرى تكون الدقة فيها غير مطلوبة أو ليست بالاهمية الكبيرة .

2- تجنب سوء استخدام المعلومات وتسريبها:

لا تقتصر اهمية الرقابة على فعاليات نظام المعلومات الادارية على ضمان دقة المعلومات التي يقوم النظام بتوفيرها ، وانما تتعداها إلى ضمان استخدام هذه المعلومات في الاتجاهات الصحيحة على النحو الذي يحقق الاهداف المخططة للنظام ، وايضاً إلى تامين تدفق المعلومات في القنوات المخصصة لها ومنع تسربها خارج هذه القنوات والذي ينعكس سلباً على كفاءة وفاعلية النظام وتؤدي إلى الحاق الضرر بالمنظمات التي يوجد فيها نظام المعلومات أو الافراد الذين يعملون فيها .

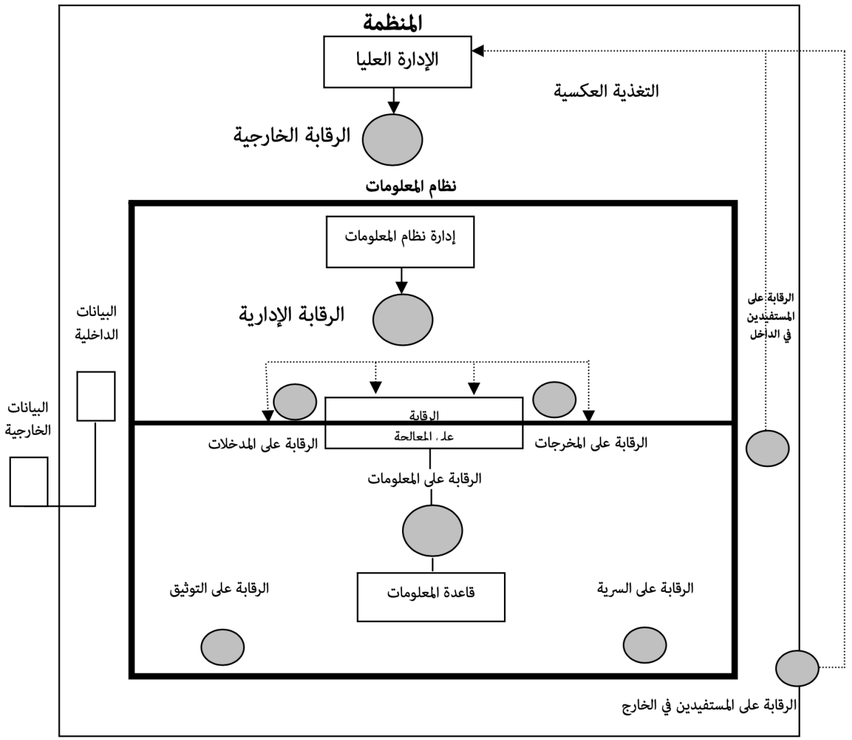
ثانيا: قواعد الرقابة على نظم المعلومات الادارية

1- قاعدة قبول الرقابة:

من بين اهم قواعد الرقابة على نظام المعلومات هي قاعدة قبول الرقابة التي تشير إلى ضرورة كون الرقابة مقبولة من قبل العاملين في المنظمة وخاصة المستفيدين من خدمات النظام والعاملين في نظام المعلومات ، فالرقابة تساعد الادارة في خلق الثقة بالنظام لإنجاز العمليات اليومية وبلوغ الاهداف المرغوبة ، ويمكن القول بان قبول الرقابة تنصب على العنصر البشري ذلك لأن العاملين في المنظمة يمكن ان يساهموا في افشال أي مشروع ، إذ ان عدم القبول قد ينتج عنه فقدان السيطرة على النظام على النحو الذي يقود به إلى الفشل.

2- قاعدة النقاط الحرجة:

وتشير إلى ضرورة وجود نقاط محددة يتم التركيز عليها لحساسيتها واهميتها في منع تضخيم الخطأ الحاصل أو مضاعفة الانحراف المتحقق، إذ تساعد هذه النقاط في الابقاء على درجة مناسبة من الرقابة الضرورية



3- قاعدة المسؤولية الرقابية:

بعد تحديد نقاط الرقابة الحرجة يناط مسؤولية الرقابة على هذه النقاط للأفراد عند مستوى العمل المناسب لتلك النقاط ، مع التأكيد على ضرورة كون المسؤولية الرقابية متضمنة للمقاييس الكمية والنوعية التي في ضوئها تتحدد تلك المسؤولية ، ان ضمان هذه القاعدة سوف يعزز من فرص كفاءة الرقابة

ثالثا: أساليب الرقابة على نظم المعلومات الادارية

1- الرقابة الادارية العامة:

الرقابة على دائرة نظام المعلومات الإدارية، وتضم الجوانب التالية:

الخطة الرئيسة؛ خطة الرقابة الطارئة؛ الرقابة على الهيكل، الرقابة على تطور العاملين.

الرقابة على تحليل النظم وصياغة البرمجيات، وتضم ما يلي:

الأساليب والإجراءات؛ تحليل النظم؛ الجوانب الكتابية والمنطقية، التوثيق.

الرقابة على مركز الحاسب الالكتروي، من خلال الآليات التالية:

حركة ونشاط العاملين؛ الأشرطة والأقراص؛ صيانة الحاسب.

الرقابة على أمان وسلامة نظام المعلومات، وتشمل الجوانب التالية:

البرمجيات؛ الأجهزةو والمعدات؛ الحماية من الحريق؛ نظام التكييف

2- الرقابة التشغيلية:

المدخلات	عملية المعالجة	المخرجات	قاعدة المعلومات
التحقق	الاختبار العقلاني	الشاشة	السيطرة على البيئة
الرقابة الاجمالية	المطابقة	التحكم في توزيع المعلومات	تجنب خطر الحريق
أنواع اخرى	التدقيق المتعاقب	المقارنة	نسخ احتياطية
-	البرهان الرياضي	ترقيم القوائم	حماية أغلفة الملفات
-	-	المستفيدون	اعادة بناء الملفات

رابعا: الرقابة على أمن المعلومات

1- أهمية الرقابة على أمن المعلومات:

1- على الرغم من ان العديد من المختصين لديهم خبرات وممارسات متباينة اعتمادا على الفرص المختلفة التي توفرها اعمالهم وبيئاتهم الثقافية وارتباط ذلك بالمشاكل والصعوبات المتعلقة بالمعلومات إلا أن هؤلاء المختصين لم تتوفر لديهم الفرصة والدافعية لانجاز الدراسات عن أمنية المعلومات بانفسهم.

2- ازدياد حاجة مدراء المنظمات لفهم وادراك خطورة وأهمية هذا الموضوع ومن ثم السعي الى الاستجابة السليمة من خلال تطوير السياسات والاجراءات التي تكفل حماية أمنية معلوماتها. اذ حذر احد التقارير من أن معلومات المنظمة تعد بمثابة "الذهب " في عصر ثورة المعلومات على النحو الذي يتوجب على الادارات أن تدرك أهمية وكيفية حمايتها بأسلوب مشابه لحماية الجواهر الثمينة.

3- شمولية الموضوع وعدم اقتصاره على منظمة دون أخرى، إذ أن جميع المنظمات تعتمد على المعلومات في تسيير انشطتها المختلفة عليه فأن مشكلات أمنية المعلومات ستؤثر عليها جميعا دون استثناء .

2- المقصود بأمن المعلومات:

1 – هي المحافظة على متاحية المعلومات وسلامتها وسريتها وملكيتها والاستفادة منها.

2 – هي المحافظة على المعلومات من تداخل استخدامها أو تخريبها أو استخدام معلومات مضللة أو تحريفها أو استبدالها أو سوء تفسيرها أو الغاؤها أو سوء استخدامها أو الفشل في استخدامها أو الوصول اليها أو اظهارها أو مراقبتها أو نسخها أو سرقتها.

3 – هي معالجة جميع الخروقات المذكورة في التعريف الثاني أعلاه قانونيا بشكل ناجح من قبل مالك هذه المعلومات بوصف هذه الخروقات انتهاكا لحقوق المالك.

4 – هي الوظائف التي تهدف الى حماية المعلومات والتي تشتمل على التجنب، المنع، الكشف، الاعاقة، التطفيف، النقل ، التحويل ، الاسترجاع، التصحيح، والاقرار.

5 – هي الاجراءات التي تحقق الحماية والتي يجب توجيهها من خلال الوفاء بالمعايير المحددة في اطار التشخيص السليم للسلبيات والتهديدات .

6 – هي الحماية الدقيقة والتي غالبا ما تنجز من خلال صياغة ضوابط واضحة ومحددة بشكل سليم للمراقبة الامنية وتطبيقها بفاعلية في اطار استخدام مجموعة من القواعد الرقابية كارشادات .

رابعا: الرقابة على أمن المعلومات

3- طرق اختراق أمنية المعلومات:

1- التجسس التنافسي (الصناعي) : ويتمثل في الاطلاع غير المخول به على المعلومات فالتهديد الخطير الذي يواجه أمنية المعلومات هو الدخول(الوصول) غير المرخص اليها من قبل شخص ما ويعرف مثل هؤلاء الاشخاص عادة بمصطلح " المأجورين " (Hackers) وقد أحست منظمات كثيرة بوجودهم ، ويعزى السبب في ظهور مثل هذه الشريحة الى زيادة حدة المنافسة بين المنظمات ، قصر دورة حياة المنتجات ،انخفاض هامش الربح ، انخفاض ولاء العاملين ،

2 – سوء استخدام المعلومات .ويشيرالىالحالة التي تسخر وتوظف فيها المعلومات لتحقيق أهداف غير مشروعة أو في مجالات غير مسموح بها لتحقيق مصالحه الشخصية أو مصالح جهات أخرى حتى في الحالات التي يحق للمستفيد في الوصول الى هذه المعلومات ، ويحصل هذا الاختراق بسبب استغلال احد الافراد من قبل الشركات المنافسة من اجل المال او الرغبة في التجسس او بسبب طرد الفرد العامل ومن ثم قيامه بعرض معلوماته وكشف اسرار المنظمة واستراتيجيتها.

3- الإهمال : وهو يمثل الطريقة الاكثر شيوعا لاختراق المعلومات ويعزى السبب في ذلك الى اهمال الافراد العاملين وتهاونهم أو ضعف ادراكهم لاهمية الاحتفاظ بسرية المعلومات والعواقب الوخيمة المترتبة لاختراق أمنية المعلومات .الى جانب عدم معرفتهم المعلومات التي تحتاج الى الحماية ومن يمتلك الدافع الى سرقة هذه المعلومات من داخل المنظمة وخارجها وكيف يمكن كشفه وإيقافه في الوقت المناسب.

4- تدمير المعلومات من خلال استخدام الفايروسات التي شغلت المتخصصين في السنوات الاخيرة بسبب اتساع مخاطرها وسهولة انتشارها والأضرار الكبيرة المترتبة عليها والتي تشتمل علىمهاجمة البيانات والمعلومات والبرامج واتلافها وحذفها وتعديلها جذريا من خلال تشويهها وتحريفها وادخال معلومات غير صحيحة ، حذف الملفات واعادة تسميتها وتغيير تواريخ الملفات المخزونة ، فضلا عن ايقاف الحاسب عن العمل او ابطاء تشغيله وتقليص السعة التخزينية . وتجدر الاشارة هنا الصعوبة حصر وتعداد جميع أنواع الفايروسات المستخدمة حاليا في اختراق أمنية المعلومات وذلك لتعددها وتنوعها وتزايد انتشارها باضطراد فضلا عن تطور صيغها وأشكالها باستمرار .

رابعا: الرقابة على أمن المعلومات

4- آليات تعزيز أمن المعلومات: