المحور الخامس: المخاطر التي يتعرض لها نظام المعلومات المحاسبي وأساليب الرقابة

1 – المخاطر التي تتعرضلها موارد المشروع المخاطر : هذه المخاطر **متنوعة** منها:

- خطر **اختلاس** أموال المشروع النقدية أو العينية من قبل القائمين على حيازتها أو استخدامها.
- خطر تحقق **خسائر ناجمة عن العمليات الجارية** التي يكون منشؤها الإهمال أو ضعف كفاءة الإدارة أو قرارات خاطئة ناجمة عن خطأ في المعلومات المستخدمة في اتخاذ القرارات.
- خطر تحقق **خسائر نتيجة عوامل خارجية** تؤدي إلى تلف أصول المشروع وفقدانها. من هذه العوامل: الزلازل والحرائق والفياضانات وغيرها.
- **خطر ضياع بعض الفرص** على المشروع كعدم الاستفادة من فرص ائتمانية ممنوحة من قبل الموردين والبنوك نتيجة للإهمال أو السمعة غير الحسنة للإدارة. كذلك الأمر في حال عدم الاستفادة من فرصة التعامل مع بعض العملاء المتميزين بملاءتهم المالية وانتظام أعمالهم واتساعها.
- خطر **التعرض للمخالفات القانونية**، نتيجة لمخالفات القوانين والأنظمة النافذة الناظمة لعمل المشروع أو المرتبطة بالأنشطة التي يمارسها.
- خطر **الغش والاحتيال:** يقصد بالاحتيال التضليل المقصود وتزوير الحقائق لدفع جهة ما للتنازل عن حق أو لدفع هذه الجهة للقيام بعملٍ ما، كشراء أصل مثلاً. أما الغش فهو نتيجةٌ للاحتيال ويحدث عندما يتم التنازل عن الحق أو القيام بالتصرف كنقل الملكية مثلاً.

المخاطر المذكورة تنشأ إذاً من **مصادر** مختلفة منها:

- تفويض غير مناسب للصلاحيات أو تجاوز الصلاحيات الممنوحة.
- غياب أو ضعف سياسات المشروع أو عدم الالتزام بهذه السياسات.
- إهمال الواجبات
- سوء الائتمان
- عدم الاحتياط لخسائر محتملة
- أخطاء في المعلومات المعتمدة لدى اتخاذ القرارات
- ضعف كفاءة الإدارة والعاملين
- غياب الإجراءات المكتوبة والواضحة
- مخالفة القوانين والأنظمة

إن المخاطر المذكورة قد تؤدي إلى تحقيق خسائر مالية للمشروع، يمكن أن تتسبب بدورها في تهديد وجود المشروع أحياناً. الخسائر المالية تأخذ أشكالا مختلفة منها: زيادة التكلفة، انخفاض الإيرادات، فقدان بعض الأصول، الخ.

– أهداف الرقابة الداخلية: تهد ف الرقابة الداخلية إلى حماية أصول المشروع من المخاطر المذكورة ومن آثارها كما تهدف إلى تنميةِ هذه الأصول. هذه الأهداف هي:

- ضمان مشروعية العمليات.
- ضمان سلامة تنفيذ العمليات ودقتها.
- ضمان سير العمليات طبقاً للسياسات والبرامج والخطط المحددة.
- ضمان إنتاج وتقديم معلومات صحيحة ودقيقة وموثقة وفي الوقت المناسب.

– ضمان تنمية وتطوير الموارد الاقتصادية المتاحة للمشروع.

إن بلوغ هذه الأهداف وترجمتها على أرض الواقع يوجب على الإدارة استخدام وسائل وأساليب رقابية، ورسم إجراءات رقابية تكون أكثر التصاقاً بخطوات ومراحل إنجاز الأعمال في المشروع. هذه الأساليب والوسائل والإجراءات لا يمكن تحديدها ورسمها بعيداً عن الأهداف المذكورة، إذ أن تحقيق كل هدف يحتاج إلى إجراءات خاصة به.

ركز المفهوم التقليدي لنظم الرقابة الداخلية على كونها إجراءات تعمل على حماية أصول المنظمة، والتأكد من الدقة الحسابية للبيانات المحاسبية المسجلة بالدفاتر . أما المفهوم المعاصر للرقابة الداخلية فإنه يركز على كونها "خطة التنظيم والطرق والإجراءات والأساليب التي تضعها إدارة المنظمة" بهدف:

– المحافظة على أصول المنظمة.
– ضمان صحة ودقة المعلومات المحاسبية وزيادة درجة الاعتماد عليها.
– تحقيق الكفاءة التشغيلية لكافة جوانب النشاط في المنظمة.
– التحقق من التزام العاملين في المنظمة بالسياسات الإدارية التي تضعها الإدارة.

يقوم الضبط الداخلي على توزيع السلطات والأعمال على العاملين في المشروع بشكل يضمن فصل الأعمال المتعارضة وتقسيم العمل على مجموعة أشخاص لينجز كل منهم جزء من العمل بحيث يراقب أحدهم عمل من سبقه في إنجاز العمل. وبذلك تتحقق الرقابة التلقائية خلال إنجاز العمل. في مجرى هذه الرقابة تجري أعمال المقارنة والمطابقة للمستندات بحيث يتم التحقق من مدى صحة المستندات وشرعيتها ودقتها لحظة إنجاز العمل وقبل معالجة البيانات التي تحملها في نظام المعلومات المحاسبي. يقوم الضبط الداخلي أولاً على أركان أساسية أهمها:

– تحديد الصلاحيات والمسؤوليات.
– فصل الأعمال المتعارضة.
– تقسيم العمل.
– توثيق المستندات ومطابقتها قبل اعتمادها واستخدام بياناتها.

غير أن توافر هذه الأركان يستوجب توافر عدد كبير من العاملين في المشروع ، وهذا يعني ارتفاع تكاليف الرقابة بحيث يصعب على المشروعات المتوسطة أو الصغيرة تحملها. لذلك فإن الضبط الداخلي لا ينطبق إلا في المشروعات الكبيرة.

ينصب الضبط الداخلي على كافة الأعمال التي تجري في المشروعات سواءً منها العمليات الإنتاجية أو المالية أو المحاسبية أو غيرها. وبالتالي فهو يختص برقابة العمليات الإنتاجية والمحاسبية على حدٍ سواء ليشكل تطبيقه داخل نظام المعلومات المحاسبية ما يعرف بالرقابة المحاسبية الداخلية التي تهدف إلى: حماية العمليات المحاسبية ونتائجها (بدءاً من إعداد المستند الأولي مروراً بمرحلة إدخال البيانات ثم تشغيلها وإعداد المعلومات لتقديمها للمستخدمين)، وإلى ضمان سير هذه العمليات طبقاً للتفويض المحدد للصلاحيات والمسؤوليات ، بحيث يمكن بلوغ الدقة وانتظام الأعمال كما هو مرسوم لها. وهذا بدوره يضمن صحة Reification المعلومات المحاسبية.

تستخدم وسائل كثيرة لتحقيق الضبط الداخلي منها ما يخص العاملين ومنها ما يخص آليات العمل وكيفية إنجاز الأعمال. فيما يلي أمثلة على وسائل الضبط الداخلي:

- تحديد المسؤوليات والصلاحيات لكل شخص أو فرد بشكل واضح.
- لايجوز لموظف أو جهة واحدة إنجاز عملية بكاملها (فصل الأعمال المتعارضة).
- تقسيم العمل على مجموعة أشخاص بحيث يراقب أحدهم عمل ما أنجزه الآخر ثم يكمل العمل وهكذا.
- كتابة التعليمات والتوجيهات بشكل واضح.
- اختيار الأفراد وتدريبهم ومحاسبتهم.
- تبديل مهام الأفراد بين الفترة والأخرى
- مطابقة المستندات والتحقق منها عند إنجاز العمل وقبل معالجة بياناتها ، مثل مطابقة كشوف المصرف مع الدفاتر، أو مطابقة كشف الموردين مع حساب الموردين.
- الترقيم المسبق للمستندات.
- إعداد التقارير الدورية للوقوف على ما أُنجز من عمل ومن مستوى الأداء.
- اعتماد سياسات واضحة محددة، كسياسات البيع ومنح الحسم التجاري وحسم تعجيل الدفع وغير ذلك.
- تحديد آليات إنجاز العمل واعتماد دورات مستندية ثابتة وواضحة لكل نشاط.

أما وسائل الضبط الداخلي في العمليات المحاسبية داخل النظام والتي تسمى **بالرقابة المحاسبية الداخلية** فإنه يمكن الإشارة إلى ما يلي كأمثلة عليها:

- فصل الأعمال المحاسبية عن باقي أنواع الأعمال.
- استخدام حسابات المراقبة الإجمالية.
- استخدام القيد المزدوج.
- إعداد موازين مراجعة دورية
- مطابقة المستندات الواردة من خارج المشروع مع الدفاتر (مثل كشوف المصرف والموردين).
- استخدام دليل حسابات واضح.
- وجود توصيف محدد وموثق لآلية إنجاز العمل المحاسبي.

2 -أثر تكنولوجيا المعلومات في الرقابة الداخلية:

إن مصادر الخطر المذكورة تختلف وتتنوع من مشروع لآخر باختلاف عوامل كثيرة، أهمها سوء التنظيم. فالمشروع المنظم تنظيماً جيداً، وتديره إدارة علمية خبيرة، ويعمل فيه عاملون أكفاء، ويعتمد على نظام معلومات محاسبي جيد ومتين يكون أقل عرضة للمخاطر المذكورة من المشروعات الأخرى الأقل كفاءة وتنظيماً.

كما أنه كلما قلّ العمل اليدوي في المشروع كلما ضعفت أيضاً مصادر الخطر. ففي المشروعات التي تستخدم التكنولوجيا الحديثة ونظم المعلومات الآلية تقل فيها المخاطر الناجمة عن سوء الائتمان وعدم الكفاءة وعدم الالتزام

بالسياسات وعن الإهمال أو عن الأخطاء في المعلومات. هذا بخلاف المشروعات التي تعتمد على العمل اليدوي في إنجاز الأعمال. غير أن استخدام الوسائل التقنية الحديثة لا يعني عدم وجود أخطاء لأن استخدام هذه الوسائل يحمل معه **مصادر أخرى للخطر**. من هذه المصادر:

- اتخاذ إجراءات غير سليمة أو غير مناسبة لتطوير النظم وتغيير البرامج المستخدمة.
- حيازة المشروع لتجهيزات حواسب وبرمجيات حاسوبية لا تحقق احتياجات المشروع.
- عدم قدرة الحاسب على اكتشاف الأخطاء عند إدخال البيانات ومعالجتها.
- دخول غير مصرّح به إلى الحاسب وبرمجياته وملفاته.
- اختراق النظام من خلال قنوات الاتصال.
- استخدام الحاسب لارتكاب عمليات غير نظامية.
- عدم اكتشاف الأخطاء عند تحديث الملفات أو قواعد البيانات.
- ضياع أو تعديل قواعد البيانات المحاسبية.
- المغالاة في تكاليف وصيانة تشغيل الحاسوب.

على الرغم من أن الهدف من الرقابة الداخلية لم يختلف ما بين النظم التقليدية والنظم الحديثة لتشغيل ومعالجة البيانات بشكل عام، إلا أن التغيرات التي حدثت في أساليب تجميع وتشغيل البيانات والتقرير عن المعلومات استوجبت إحداث تغييرات في طبيعة الوسائل والإجراءات الرقابية المستخدمة في النظم الالكترونية. وبشكل عام يمكن دراسة العوامل التي أدت إلى حدوث تغيرات في طبيعة الوسائل والإجراءات الرقابية نتيجة تأثير تطورات تكنولوجيا المعلومات من خلال ما يلي:

– التشغيل المركزي للبيانات:

في ظل التشغيل اليدوي يتم تقسيم تشغيل البيانات بين الموظفين المتواجدين في أقسام مختلفة من المنظمة، مما يوفر فرصة لإمكانية الرقابة المهنية الناتجة عن تقسيم العمل بين عدة أشخاص تقارن نتائج عملهم مع بعضها البعض، كأن يتم الفصل بين عمليات إعداد حسابات الأستاذ المساعد عن العمليات المتعلقة بإعداد حسابات الأستاذ العام، مما يوفر فرصة لاستخدام عمل الشخص الثاني للرقابة على عمل الشخص الأول أو بالعكس.

أما في ظل التشغيل الالكتروني للبيانات، يؤدي استخدام أسلوب المعالجة المركزية إلى تجميع البيانات وتراكم العمليات من مختلف أقسام الم نظمة في قسم الحاسب ، مما يؤثر على الرقابة المهنية الموجودة في النظام التقليدي.

وعموماً، يظل الفصل بين الواجبات أحد أبرز مبادئ الرقابة الداخلية سواء في النظم اليدوية أو النظم الالكترونية، إلا أن هذا الفصل في النظم الالكترونية يكون بين الوظائف المرتبطة بالتعامل مع البيانات وتشغيلها، مثلاً الفصل بين وظيفة البرمجة ووظيفة إدخال البيانات .

– طبيعة وسائط التخزين:

على الرغم من أن وسائط التخزين الالكترونية تقدم العديد من المزايا لنظام المعلومات ومستخدميه، إلا أن طبيعة هذه الوسائط قد توفر فرصة لحدوث مشاكل متعددة، ومن أبرز هذه المشاكل:

- صغر حجم وسائط التخزين قد يمكن من سهولة سرقة البيانات.
- سهولة التعديل على البيانات المخزنة يمكن أن يوفر فرصة لتغيير محتوى البيانات التي تخزنها المنظمة أو حذفها بشكل نهائي دون ترك آثار مادية.
- قد يوفر الوصول إلى البيانات من مواقع بعيدة من خارج المنظمة، الفرصة لأطراف غير مصرح لها من داخل أو من خارج الدخول إلى نظم المنظمة وإجراء تغيرات عليها.

لذلك يجب توفير إجراءات رقابية لحماية البيانات المخزنة من الوصول غير المصرح إليها و توفير نسخ احتياطية من البيانات الهامة، إضافة إلى توفر إمكانية استرداد البيانات عند حذفها أو تعديلها بشكل غير نظامي أو غير قانوني.

– تغيير طبيعة الوثائق التقليدية:

تعتبر الوثائق التقليدية أحد أدلة الإثبات في عملية الرقابة والتحقق من العمليات، فالمستندات التقليدية الورقية تقدم أدلة إثبات لما تقوم به المنظمة من عمليات، ويمكن الاعتماد على تدفق هذه المستندات والوثائق وحركتها بين أقسام المنظمة والأطراف التي تتعامل معها، عند فحص العمليات والرقابة عليها من خلال ما يعرف بمسار المراجعة Audit Trial.

يختلف الوضع في ظل التشغيل الالكتروني للبيانات، حيث قد يؤدي الإدخال والتشغيل الالكتروني واستخدام تبادل البيانات الكترونياً إلى فقد مسار المراجعة للعمليات، وفقدان أثر المستندات وحركتها ضمن المنظمة أو مع الأطراف الأخرى. ولذلك يجب أن تتضمن الإجراءات الرقابية في التشغيل الالكتروني للبيانات ما يعوض عن فقد أو إمكانية فقدان مسار المراجعة.

– اختلاف طريقة المعالجة:

توفر تكنولوجيا المعلومات تماثل عملية المعالجة من خلال استخدام برنامج واحد لتشغيل جميع البيانات، وهذا ما يختلف عن تشغيل البيانات في ظل النظام التقليدي حيث يقوم عدة أشخاص بمعالجة البيانات، ولذلك يتم في النظام التقليدي التركيز على فحص عينة كبيرة من العمليات لاكتشاف الأخطاء في إدخال وتشغيل البيانات. أما في ظل التشغيل الالكتروني للبيانات، يجب التركيز على فحص النظام الذي يقوم بالمعالجة، لفترات زمنية مختلفة، كما يتم التركز على فحص عملية واحدة، إذ يمكن أن يبين ذلك أن جميع العمليات الأخرى المماثلة صحيحة أو غير صحيحة، حيث يقوم برنامج واحد بمعالجة جميع هذه العمليات المتماثلة.

– افتقار الحاسب إلى الحكم الشخصي:

يفتقر الحاسب إلى الحكم المنطقي على العمليات التي يقوم بها نظام المعلومات، فيقوم الحاسب بتنفيذ العمليات من خلال مجموعة من التعليمات والبرامج التي تفتقر إلى الحكم المنطقي الذي يمكن أن يتوفر لدى العنصر البشري. فيمكن مثلاً أن ينتج عن معالجة البيانات الكترونياً أن عمر الموظف يبلغ 7 سنوات، أو أن الشهر 40 يوم، ولذلك يتم وضع مجموعة من الضوابط والمحددات في نظام المعلومات للحكم على مدى قبول المدخلات أو عمليات التشغيل أو حتى المخرجات، وذلك في إطار الرقابة على التطبيقات، من خلال التحقق والتنقيح والكمال وغيرها من الإجراءات .

يعتمد أثر الحاسب الآلي المباشر على النظام المحاسبي والمخاطر المرتبطة به بشكل عام على ما يلي :

- مدى استخدام النظم المباشرة في معالجة التطبيقات المحاسبية.
- نوع وأهمية المعاملات التي تتم معالجتها.
- طبيعة الملفات والبرامج التي تستخدمها التطبيقات.

من العوامل التي قد تقلل من مخاطر الأخطاء التي تحدث نتيجة استخدام النظم المباشرة ما يلي :

- إدخال البيانات عند أو بالقرب من النقطة التي تنشأ فيها المعاملات يقلل من مخاطر عدم تسجيل المعاملات.
- التصحيح الفوري وإعادة إدخال المعاملات غير الصحيحة يقلل من المخاطرة بأن هذه المعاملات لن يتم تصحيحها وإعادة تقديمها بسرعة.
- إدخال البيانات من قبل أفراد يفهمون طبيعة المعاملات ذات العلاقة يقلل من التعرض للخطأ مقارنة بإدخالها من قبل أفراد ليسوا على معرفة بطبيعة المعاملات.
- معالجة البيانات بشكل فوري يقلل من مخاطرة معالجتها في الفترة المحاسبية الخطأ.
- التوثيق والتصريح اللذان يحدثان عند أو بالقرب من النقطة التي تنشأ فيها المعاملات، يقللان من مخاطر انتحال الشخصية أو الوصول غير المصرح به إلى البيانات أو التلاعب بها.

– عدم اكتمال مسار المراجعة:

يعتبر ضمان مسار جيد للمراجعة من أبرز أساليب الرقابة الوقائية، حيث يشير مسار المراجعة الجيد إلى إمكانية تتبع العمليات المحاسبية بداية من المستند الأصلي لنشوء المعاملة وحتى وجودها في التقرير النهائي، حيث يمكن للمنظمة التعرف على العمليات التي قامت بها، واكتشاف الأخطاء والتلاعب الذي قد يحدث في نظام المعلومات المحاسبية.

في النظام التقليدية يمكن ضمان مسار لمراجعة العمليات التي تقوم بها المنشأة، إلا أن استخدام تكنولوجيا المعلومات والتبادل الإلكتروني للبيانات قد يؤدي إلى فقد مسار مراجعة العمليات، فالمستندات قد تنشأ

آليا وتعالج البيانات بدون تدخل العناصر البشري، مما قد يؤدي إلى فقد المستندات التي تثبت مسار العمليات وتبينه.

عموماً يمكن استخدام سجلات المعاملات في النظم الالكترونية لتحديد مسار المراجعة في نظم التشغيل المباشر للبيانات خاصة في ظل عدم وجود مستندات أولية، فسجل المعاملة يقوم بحصر كافة العمليات التي تم تشغيلها في نظام الحاسب، ويحتوي هذا السجل على كافة البيانات التي تم إدخالها واختبارها، فيتضمن عادة رقم الجهاز الطرفي الذي تم إدخال البيانات منه، قيمة العملية، ورقم العملية الكودي.

3- أساليب الرقابة العامة على نظم المعلومات الحاسوبية:

تتضمن أساليب الرقابة العامة مجموعة من الإجراءات والسياسات التي تتبناها المنظمة بهدف توفير بيئة رقابية آمنة، إذ تتعرض هذه الأساليب إلى النظام بشكل عام، وليس إلى جزء خاص من الإدخال أو المعالجة أو المخرجات. ويمكن التعرض لأبرز أساليب الرقابة العامة فيما يلي:

- الفصل بين الوظائف:

يعتبر الفصل بين الوظائف من أبرز إجراءات الرقابة الداخلية التي يجب أخذها بالحسبان عن تصميم ووضع نظام رقابة داخلية فعّال، ويقصد هنا بالفصل بين الوظائف ذات العلاقة، بحيث لا يجمع موظف واحد بين حيازة الأصل وسلطة تسجيل العمليات المتعلقة بهذا الأصل، كمثل وظيفة مسك دفاتر أو سجلات النقدية ووظيفة أمين الصندوق، فإذا لم يتحقق مثل هذا الفصل سيكون بإمكان الشخص الذي يحوز كلا الوظيفتين سرقة النقدية والتلاعب ببيانات النقدية في السجلات بشكل يجعلها متطابقة مع قيمها الفعلية المحرفة.

ويعتبر الفصل بين الوظائف من الإجراءات التي تتبع في كلا النظامين التقليدي والحاسوبي، إلا أنه يجب مراعاة اختلاف طبيعة الوظائف المرتبطة ببعضها البعض في حال استخدام النظم الحاسوبية، فهناك وظائف جديدة تتعلق بإدخال ومعالجة البيانات وتطوير وتصميم البرامج، ومن أبرز الوظائف التي يجب الفصل بينها:

- إصدار مستندات المصدر.
- التصريح بمستندات المصدر.
- إدخال البيانات إلى النظام.
- معالجة البيانات التي تم إدخالها.
- تغيير البرامج والبيانات.
- استخدام أو توزيع المخرجات.
- تعديل أنظمة التشغيل.

في ظل استخدام النظم الحاسوبية، يجب التركيز على فصل الوظائف بين الأقسام إضافة إلى الفصل بين الوظائف في قسم الحاسب نفسه، وذلك كما يلي:

- **فصل الوظائف بين الأقسام:**

يجب أن لا يملك الأفراد العاملون في قسم معالجة البيانات حق الوصول إلى الأصول المادية، أو سلطة اعتماد وإجازة العمليات، بمعنى آخر الفصل بين وظيفة المحاسبين ووظيفة المبرمجين، فيجب عدم إجراء تعديلات على الملفات الرئيسية أو ملفات المعاملات إلا بعد موافقة قسم المحاسبة.

– فصل الوظائف داخل قسم الحاسب:

أ – الفصل بين وظائف تطوير البرامج والأنظمة ووظائف تشغيل البيانات، حيث تتعلق وظائف تطوير الأنظمة والبرامج بتحليل وتصميم ووضع البرامج وتوثيق العديد من التطبيقات، أما وظائف تشغيل الحاسب فتتضمن إدخال البيانات وتشغيلها لتقديم المخرجات. بحيث يؤدي الفصل بين هاتين الوظيفتين إلى عدم توفير الفرصة لمعدي البرامج لإدخال بيانات وهمية، أو لمشغلي الأجهزة لإعداد برامج تمكنهم من معالجة البيانات بطريقة تتضمن الاحتيال أو الغش والتلاعب.

ب – الفصل بين وظيفة تشغيل البرامج ووظيفة البرمجة، إذ أن معرفة المبرمج بتفاصيل البرنامج المعد من قبله يجعله قادراً على التلاعب بالإجراءات الرقابية.

ت – الفصل بين وظيفة البرمجة ووظيفة مراجعة البرامج، بحيث لا يسمح للمبرمج بمراجعة البرامج المعدة من قبله.

- **الحماية المادية لمكونات النظام:**

تتعرض مكونات نظام المعلومات للسرقة أو التلف المادي أو الوصول غير المصرح به، ولذلك يجب على المنظمة توفير إجراءات لحماية التجهيزات المادية لنظام المعلومات، ومن إجراءات الحماية ما يلي:

– وضع التجهيزات في أمكان مغلقة ومحمية.

– استخدام أنظمة الإنذار للتنبيه عند فصل الحاسب أو نقله من مكانه.

– وضع سياسات تبين الإجراءات الملائمة الواجب إتباعها عند استخدام الحاسب خارج موقع المنظمة، أو السفر مع حاسب محمول.

– تشفير الملفات الرئيسية.

– وجود أساليب تحول دون حدوث التلف الذي قد ينتج من الكوارث الطبيعية والكوارث الأخرى كالحرائق.

- **الرقابة على نقل البيانات وتداولها:**

تمثل الرقابة على نقل البيانات وتداولها الكترونياً أحد أبرز الضرورات التي تتطلبها النظم الالكترونية والشبكات، حيث يوجد العديد من المخاطر التي تتعرض لها البيانات أثناء نقلها أو تداولها سواء داخل فروع المنظمة، أو بين المنظمة والأطراف التي تتعامل معها. وهناك العديد من الأساليب التي يمكن إتباعها للرقابة على نقل البيانات وتداولها، أبرزها ما يلي:

– التوثيق الالكتروني Electronic Authentication:

تعتبر عملية التعرف على العملاء والتحقق من هويتهم أحد طرق الرقابة. حيث أن طرق التوثيق التقليدية التي تعتمد على المستندات الورقية وطرق التوثيق الشخصية تخفض من سرعة وكفاءة العمليات الالكترونية، وقد تبنت المنظمات طرق توثيق بديلة تتضمن:

- كلمات المرور وأرقام التعريف الشخصي Personal Identification Numbers (PINs).
- الشهادات الرقمية Digital Certificates باستخدام البنية التحتية للمفتاح العمومي Public Key (PKI).
- مطابقات قواعد البيانات (مثلا: تطبيقات اكتشاف الغش).
- المحددات المترية Biometric Identifiers.

تختلف طرق التوثيق السابقة وفقا لمستوى الأمن والموثوقية التي تقدمها، كما تختلف وفقا لدرجة تعقيد بنيتها التحتية وتكاليفها. واختيار أياً من هذه الأساليب للاستخدام يجب أن يتوافق مع المخاطر المرتبطة بالمنتجات والخدمات التي تمكن هذه الأداة من الوصول إليها.

– التشفير Encryption:

يشمل التشفير تغيير البيانات إلى صيغة غير معروفة قبل نقلها، ومن خلال هذه الطريقة نعمل على ضمان عدم القدرة على تفسير وقراءة النص الأصلي عند اعتراض الرسالة، وتعرف البيانات المشفرة التي لا معنى لها بشكلها المشرف بأنها نص مشفر Cipher text، ويجب أن يرتبط بالتشفير فك التشفير، أو إعادة النص المشفر إلى صيغته الأصلية. وعموما هناك طرق متعددة من التشفير أبرزها ما يلي:

أ – طريقة المفتاح الخاص DES-Private Key Encryption:

وفقاً لهذه الطريقة يتم استخدام مفتاح واحد أو خوارزمية واحدة لتشفير النص وفك التشفير، ولهذا يعرف هذا النوع من التشفير في بعض الأحيان بأنه تشفير متماثل، وتستخدم عادة أشكال معروفة لتشفير البيانات تصدر عن هيئات متخصصة، تعرف بمعايير تشفير البيانات Data Encryption Standard.

وفي هذه الطريقة من التشفير يجب أن يكون مفتاح التشفير معروف لمرسل الرسالة ولمستقبلها.

ب – تشفير المفتح العام RAS- Public Key Encryption:

قد تكون التسمية الأكثر دقة لهذه الطريقة من التشفير هي بتشفير المفتاح الخاص والمفتاح العام، ووفقا لهذه الطريقة يتم استخدام مفتاحين أحدهما للتشفير وآخر لفك التشفير. حيث تقوم بعض المنظمات بتحديد مفتاح عام لعملائها لتشفير الرسائل التي يرسلونها، وتحتفظ بمفتاح خاص لفك الرسالة المشفرة لديها. وتتميز هذه الطريقة بأنه لو عُرِف أحد المفتاحين فإنه لا يمكن معرفة الآخر، وكلا المفتاحين له علامة رياضية معقدة لا يمكن معرفتها إلا من جانب المنظمة، والمفتاح الخاص لا يفترض أن يعرفه سوى صاحبه ويظل دائماً سراً عن الآخرين، أما المفتاح العام فيمكن معرفته لبعض الجهات المختصة ولا يقصد بقائه سراً.

– التوقيع الالكتروني:

يعتبر التوقيع الإلكتروني جزء صغير مشفر من بيانات يضاف إلى رسالة إلكترونية كالبريد الإلكتروني أو العقد الإلكتروني، ولا يعتبر هذا التوقيع رموز أو أرقام أو صورة للتوقيع العادي. إذ لا تُعدّ صورة التوقيع العادي بواسطة الماسح الضوئي Scanner توقيعاً رقمياً.

فالتوقيع الإلكتروني على رسالة ما عبارة عن بيانات مجتزأة من الرسالة ذاتها (جزء صغير من البيانات) يجري تشفيره وإرساله مع الرسالة، بحيث يتم التثبت من صحة الرسالة، ويتم التوقيع الإلكتروني (الرقمي) بواسطة برنامج كمبيوتر خاص لهذه الغاية ، وباستعماله فإن الشخص يكون قد وقع على رسالته تماما كما يوقع مادياً (في إطار الأوراق والوثائق الورقية)، ويستخدم التوقيع الرقمي على كافة الرسائل والعقود الإلكترونية.

<u>هناك نوعان شائعان من التواقيع الرقمية:</u>

أ – التوقيع المفتاحي أو التوقيع الكودي الرقمي:

وفقا لهذا النوع من التوقيع الالكتروني يتم تزويد الوثيقة الإلكترونية بتوقيع مشفر مميز Encrypted، يحدد هذا التوقيع الشخص الذي قام بتوقيع الوثيقة، والوقت الذي قام فيه بتوقيع ها، ومعلومات عن صاحب التوقيع. ويتم تسجيل التوقيع الرقمي بشكل رسمي عند جهات تعرف باسم (سلطة التوثيق) Certification Authority وهي طرف محايد مهمته التأكد من صحة ملكية التوقيع الرقمي للأشخاص الذين يقومون بتوقيع الوثائق الإلكترونية، حيث تتولى إصدار وثيق ة أو شهادة Certificate تمكن الشخص من التوقيع الإلكتروني على الوثائق الإلكترونية، ويزود هذا الشخص بعد إعطائه الشهادة (الوثيقة) بكلمة سر خاصة تمكنه من استخدام التوقيع الإلكتروني.

ب – التوقيع البيومتري أو التوقيع بالقلم:

يعتمد التوقيع البيومتري Biometric Signature (Pen-on) على تحديد نمط خاص تتحرك به يد الشخص الموقع أثناء التوقيع، إذ يتم توصيل قلم إلكتروني ب الحاسب ويقوم الشخص بالتوقيع باستخدام هذا القلم الذي يسجل حركات يد الشخص أثناء التوقيع كسمة مميزة لهذا الشخص ، حيث أن لكل شخص سلوكا معينا أثناء التوقيع. كما يدخل في التوقيع البيومتري البصمة الإلكترونية أيضا. ويتم تسجيل التوقيع البيومتري أيضا عند سلطة التوثيق كما هو الحال في التوقيع المفتاحي السابق.

– الرقابة على الوصول إلى البيانات (حماية البيانات):

يعتبر الوصول إلى البيانات من قبل أطراف غير مصرح لها من أبرز المشاكل التي تتعرض لها نظام المعلومات الالكترونية، إذ تتيح التكنولوجيا المعاصرة إمكانية الوصول إلى النظام والبيانات المخزنة من مواقع بعيدة عن النظام Remote Access. لذلك يجب على المنظمات تصميم واستخدام أساليب وإجراءات رقابية قوية

للسماح لمن له الحق بالوصول إلى البيانات، وتحديد حقوق هؤلاء بنوع العمليات التي يسمح لهم إجراؤها على البيانات.

تستخدم المنظمات العديد من الوسائل والإجراءات للرقابة على الوصول إلى البيانات، من أبرزها:

– استخدام كلمات المرور والتعريف الشخصي لتحديد من له الحق في الوصول إلى البيانات.

– ربط كل نوع من العمليات بمفتاح خاص لا يمكن القيام بالعملية بدون هذا المفتاح، وربط المفتاح بكلمة السر. حيث يمكن تحديد كلمات المرور على مستويات متعددة تحدد الوصول إلى البيانات ونوع العمليات المسوح للمستخدم القيام بها. مثلا يحدد المستوى الأولى على مستوى النظام والدخول إليه، ويحدد المستوى الثاني عند مستوى حق الوصول إلى الملفات، بينما يحدد مستوى ثالث عند مستوى الوصول إلى عناصر البيانات المخزنة وحق التعديل عليها.

– استخدام ملف المستخدم وجدول صلاحيات المستخدم، والتي تحدد مستوى الوصول إلى البيانات المسموح به للمستخدم ونوع العمليات المسموح له القيام بها.

– الرقابة على البيانات المخزنة:

تشكل البيانات مورداً هاماً للمنظمات لذلك يجب عليها حمايتها من التلف أو الضرر أو السرقة أو الوصول إليها بشكل غير مصرح به. هنا يجب على المنظمات تحديد وإتباع أساليب وإجراءات لحماية البيانات المخزنة من المخاطر التي قد تتعرض لها. من أبرز هذه الأساليب:

– عزل البيانات، إذ يجب عزل البيانات المهمة للمنظمة مثل الملفات المرجعية وتوثيق البرامج وحفظها في مكتبة خاصة لهذا الغرض.

– الاحتفاظ بنسخ إضافية عن الملفات الهامة والأساسية، وإجراء اختبارات دورية للتحقق من صلاحية هذه النسخ الإضافية.

– تحديد درجة لسرية البيانات، وتحديد نوع الحماية المطلوبة لكل نوع منها.

– توفير إمكانيات استرداد البيانات في حال فقدها لسبب طارئ مثل حدوث حريق.

من الأساليب التي يمكن إتباعها للرقابة على الوصول إلى البيانات الجدران النارية أو حوائط المنع Firewalls.

تشير الجدران النارية في مجال نظم المعلومات الحاسوبية إلى استخدام برمجيات ومعدات لعزل الشبكة الخاصة بالمنظمة عن محيطها. حيث تتولى هذه المكونات (الحوائط) القيام بالرقابة على الوصول إلى نظم المنظمة الداخلية أو شبكتها وفقاً لقواعد تحددها المنظمة.

–التوثيق Documentation:

يشير التوثيق إلى استخدام طرق نمطية لوصف وتحديد طبيعة عمل نظام المعلومات أو أجزاء منه، وقد أشار فصل سابق إلى طرق وأشكال التوثيق والخرائط والمخططات المستخدمة في توثيق نظام المعلومات المحاسبية.

يعتبر توافر معايير للتوثيق قضية مهمة للرقابة حيث يوفر التوثيق الجيد لعمل النظام مصدر موثوق به لتشغيل النظام أو عملياته ومراجعتها والتحقق من تشغيلها بالشكل المطلوب، كما يعتبر أداة مفيدة في مراجعة عمل النظام وتطويره مستقبلا.

ولعل أهمية التوثيق تبرز بشكل أكبر في إطار النظم الإلكترونية حيث تكون المستندات الكترونية، وقد تتم معالجة البيانات بشكل مباشر عند حدوث المعاملات، ولذلك يجب توفير توثيق جيد لعناصر متعددة من تشغيل ومعالجة البيانات الكترونياً، كما يلي:

– توثيق النظام، يمكن وضع خريطة تدفق للنظام كوسيلة توثيق ملائمة، تبين هذه الخريطة مدخلات النظام والعمليات التي تتم داخل النظام، ونوع المعالجة، من ثم المخرجات المقدمة ومواقع تخزين البيانات. ويعتبر توثيق النظام من مهمة محلل النظام.

– توثيق جميع البرامج، إذ يجب توثيق خطوات تشغيل البرامج، ويتم هذا التوثيق عادة من قبل المبرمجين المسؤولين عن وضع البرنامج وتعديله.

– توثيق البيانات من خلال تحديد عناصر البيانات التي تتضمنها قاعدة البيانات.

4– الرقابة على التطبيقات Applications Controls:

ترتبط أساليب الرقابة على التطبيقات بالمهام المؤداة من قبل نظم محددة، وتصنف إلى أساليب رقابية على: المدخلات، وعلى المعالجة، وعلى المخرجات.

الهدف من الرقابة على التطبيقات هو وضع إجراءات رقابية محددة على التطبيقات المحاسبية لتوفير تأكيد معقول بصحة اعتماد العمليات وتسجيلها، ومعالجتها في الوقت الملائم، وتقديم المخرجات المطلوبة في الوقت لمطلوب.

تعتبر غالبية أساليب الرقابة على التطبيقات أساليب رقابة وقائية، تصمم بهدف اكتشاف الأخطاء قبل تحويل البيانات المدخلة إلى عملية المعالجة، أو قبل معالجها أو حتى قبل تقديم المعلومات إلى مستخدميها. ولذلك يجب مراعاة وضع أساليب ملائمة وجيدة في مرحلة تصميم وتحليل النظام المحاسبي، ومن بين العوامل التي يجب مراعاتها في هذا المجال ما يعرف بالأهداف التشغيلية لأساليب الرقابة على التطبيقات والتي تتضمن:

– تحديد سلطة إجازة وإقرار العمليات.

– التأكيد على دقة البيانات وشموليتها.

- التأكيد على دقة عمليات المعالجة وشموليتها.
- التأكيد على التوقيت الملائم في الإدخال والمعالجة والمخرجات.
- توفير أساليب لحماية المدخلات والمعالجة والملفات.
- التحقق من الفعالية والتكلفة.

- الرقابة على المدخلات:

تهدف أساليب الرقابة على المدخلات إلى التحقق من صحة وشمولية واتساق البيانات المدخلة، وأنه تم إدخال البيانات المطلوب إدخالها، ولم يتم إدخال بيانات غير مطلوب إدخالها.

يجب أن تولي المنظمات أهمية كبيرة لأساليب الرقابة على المدخلات، حيث تؤثر جودة ودقة المدخلات على جودة ودقة المخرجات أو المعلومات الناتجة. ومن أبرز العوامل التي تبين أهمية الرقابة على المدخلات ما يلي:

- يسهل تصحيح البيانات التي يتم رفضها في مرحلة الإدخال، إذ يمكن الرجوع إلى المستندات الأصلية والتحقق من صحة هذه البيانات.
- لا يمكن لنظام المعلومات أن يقدم مخرجات جيدة ما لم تكن المدخلات جيدة.
- لا يمكن الاستمرار في تطبيق اختبارات الرقابة والتحقق على البيانات في جميع مراحل وتداولها ومعالجتها، ولذلك تصمم هذه الاختبارات بطريقة تقدم تأكيد معقول بأن هذه البيانات خالية من الأخطاء بعد مرحلة معينة.
- يجب التأكيد على دقة المدخلات وصحتها، بحيث يجب العمل على أن لا يستخدم نظام المعلومات بيانات غير دقيقة في المراحل الأخيرة من عملية المعالجة.

عادة ما يتم تجهيز الحاسب ببرامج اختباريه للتأكد من صحة ومعقولية البيانات المدخلة إلى النظام، بحيث لا يسمح بإدخال البيانات بشكل نهائي وتحويلها إلى عملية المعالجة إلا بعد اجتيازها لهذه الاختبارات، فيتم مقارنة البيانات المدخلة مع معايير محددة مسبقاً لملائمة البيانات.

تتم هذه الاختبارات عند مستويات الرموز والحقول والسجلات والملفات، كما يتم للتأكد من صحة نقل البيانات ومن صحة ودقة البيانات المنقولة. وذلك كما يلي:

- اختبارات التحقق Verification Tests:

- اختبارات التنقيح Edit Tests:

- اختبارات أخرى على المدخلات:

- الرقابة على المعالجة:

تعمل أساليب الرقابة على المعالجة إلى التأكد من شمولية عملية المعالجة للبيانات المطلوب معالجتها فقط، بحيث لا تترك بيانات مطلوب معالجتها بدون معالجة، ولا يتم معالجة بيانات غير مطلوب معالجة، إضافة إلى

التحقق من سلامة ودقة معالجة البيانات والبرامج المستخدمة من المعالجة. يمكن تحديد أهداف الرقابة على المعالجة الحاسوبية فيما يلي:

- التأكد من استخدام البرنامج المطلوب لعملية المعالجة.
- التأكد من معالجة الملفات المطلوب معالجتها.
- وجود ضوابط رقابية في برنامج المعالجة تمنع حدوث الأخطاء أثناء المعالجة.
- التأكد من صحة عمل برامج المعالجة والقيام بالصيانة الدورية لتأكيد ذلك.
- وجود اختبارات للتحقق من معقولية عملية المعالجة، ورفض العمليات التي تخرج عن حدود المعقولية.

تختلف الإجراءات الرقابية المستخدمة على المعالجة الحاسوبية وفقاً لدرجة استخدام الوسائل الآلية في المعالجة، ووفقاً لنوع المعالجة دورية أو مباشرة. ويمكن بشكل عام الإشارة إلى أبرز هذه الأساليب الرقابية فيما يلي:

- التأكد من سلامة وحدة المعالجة المركزية لمعالجة البيانات أمر ضروري لتفادي أخطاء المعالجة غير المتعمدة، ويتم ذلك من خلال برامج الصيانة Maintenance Programs الخاصة لهذا الغرض والتي تكون مكتوبة بلغة الحاسب، والتي تتولى القيام بعمليات الصيانة والاختبارات لأجهزة الحاسب بشكل دوري (أسبوعياً في الغالب).
- التأكد من شمولية وتكامل برامج الحاسب المستخدم في المعالجة، حيث يمكن استخدام اختبارات "ملفات توثيق البرامج Software Documentation" التي تشمل على وسائل توثيق النظام (مثل خرائط تدفق النظام والبرامج)، وذلك حتى يتمكن محلل النظام من وضع خطة شاملة لبرامج معالجة البيانات.
- اختبار صحة تشغيل البيانات:

هناك العديد من الاختبارات التي يمكن استخدامها في الرقابة على الإدخال والرقابة على المعالجة، فاختبار الترتيب المستخدم في الرقابة على الإدخال يلائم الرقابة على المعالجة الدورية، كما يمكن استخدام اختبارات المعقولية للرقابة على المعالجة.

- اختبارات الملفات والبرامج:

تعمل اختبارات الملفات والبرامج لضمان أن العمليات تم ترحيلها إلى الملفات الرئيسية الملائمة. ومن أبرز الاختبارات في هذا المجال:

أ -تزويد برامج التشغيل بإمكانية التحقق من هوية المستخدم (كلمة السر، الرقم التعريفي الشخصي، مفتاح إجراء العملية).

ب يجب وجود اختبارات ضمن برامج التشغيل بحيث ترفض التعامل مع المدخلات أو المخرجات غير الصحيحة.

ت استخدام اختبار المقابلة لضمان أن العمليات قد تم ترحيلها إلى السجل المناسب.

ث -التأكد من ملائمة برامج التشغيل على فترات دورية، وذلك من خلال تشغيل برامج اختباريه للتأكد من الوصول إلى النتائج المرجوة، كما يمكن إعادة تشغيل البرامج بالبيانات الفعلية مرة ثانية ومقارنة النتائج التي تم التوصل إليها سابقاً للتأكد من سلامة برامج التشغيل.

ج -تزويد برامج المعالجة بإمكانية رفض معالجة المدخلات إذا لم تكن تامة، مثلاً يرفض معالجة عملية مقبوضات نقدية إلا إذا تم إدخال رقم العميل.

- الرقابة على المخرجات:

تهدف أساليب الرقابة على المخرجات إلى التحقق من أن نتائج تشغيل البيانات كاملة ودقيقة، فهي تعمل على تقديم تأكيد معقول بما يلي:

- مراجعة نتائج تشغيل البيانات والتحقق من أن التغيرات التي حدثت في الملفات الرئيسية صحيحة.
- أن المعلومات الناتجة من النظام تعكس البيانات المخزنة في النظام.
- أنه تم تقديم المعلومات في الوقت الملائم.
- وصول المعلومات إلى الأطراف المصرح لهم بذلك.