الفصل الثالث :

مخاطر نظم العمليات المصرفية الإلكترونية ومبادئ إدارة المخاطر

أولا: مخاطر العمليات الإلكترونية المصرفية[1]:

يصاحب تقديم العمليات المصرفية الإلكترونية مخاطر متعددة وقد أشارت لجنة بازل للرقابة المصرفية إلى أنه ينبغي قيام البنوك بوضع السياسات والإجراءات التي تتيح لها إدارة هذه المخاطر من خلال تقييمها والرقابة عليها ومتابعتها وأصدرت اللجنة خلال مارس 1998 ومايو 2001 مبادئ لإدارة هذه المخاطر شملت ما يلي:

(1) مخاطر التشغيل OPERATIONAL RISK:

تنشأ مخاطر التشغيل من عدم التأمين الكافي للنظم أو عدم ملائمة تصميم النظم أو إنجاز العمل أو أعمال الصيانة وكذا إساءة الاستخدام من قبل العملاء وذلك على النحو التالي:

(أ) عدم التأمين الكافي للنظم SYSTEM SECURITY:

تنشأ هذه المخاطر عن إمكانية اختراق غير المرخص لهم UNAUTHORIZED ACCESS لنظم حسابات البنك بهدف التعرف على المعلومات الخاصة بالعملاء واستغلالها سواء تم ذلك من خارج البنك أو من العاملين به بما يستلزم توافر إجراءات كافية لكشف وإعاقة ذلك الاختراق.

---

(1) راجع تفصيلاً:

Constantine Lymperpoulos & loannes E. chaniotakis "Branch employees ' perceptions towards implications of E- Banking in Greece "International Journal of Retail & Distribution Management vol 32, Number 6. 2004, p. p 302-311.

إن التعاملات على شبكة الإنترنت تتم بين أفراد مجهولين لبعضهم ويمكن أن ينتحل هؤلاء الأفراد شخصيات أخرى وبالتالي ترتفع نسبة المخاطرة وإمكانية حدوث عمليات قرصنة، وإمكانية الدخول على مواقع المؤسسات المصرفية على الشبكة بواسطة قراصنة الإنترنت لمعرفة أسرار العملاء وحساباتهم، خاصة بالنسبة للشخصيات العامة الذين يهتم الكثيرون بمعرفة أسرارهم الخاصة.

فطبقًا للإحصائيات بلغت الخسائر الناجمة عن جرائم الكمبيوتر 100 مليون دولار أمريكي في عام 1999 في الولايات المتحدة الأمريكية وحدها.

(ب) عدم ملائمة تصميم النظم أو إجراء الصيانة الدورية اللازمة للنظام:

وهي تنشأ من إخفاق النظم أو عدم كفاءتها (بطيء الأداء SLOW-DOWN) لمواجهة متطلبات المستخدمين وعدم السرعة في حلّ المشاكل المتعلقة بالنظم والصيانة الخاصة بها وخاصة إذا تم الاعتماد على مصادر فنية من خارج البنوك لتقديم الدعم الفني.

وكذلك ظهور مشاكل نتيجة أخطاء في البرمجة مما قد يؤدي إلى تسرب معلومات عن الحسابات المصرفية للعملاء إلى حسابات عملاء آخرين، وهو ما يؤدي آلة فقدان مصداقية البنك في عالم الخدمات المالية الإلكترونية، بالإضافة إلى ظهور بعض المشكلات الفنية التي يمكن أن تصيب أجهزة الكمبيوتر والتي من شأنها أن تؤثر على ثقة العملاء في بنوك الإنترنت.

ج – إساءة الاستخدام من قبل العملاء ويحدث ذلك نتيجة عدم إحاطة العملاء بإجراءات التأمين الوقائية Security Precautions أو السماح لعناصر إجرامية بالدخول إلى حسابات العملاء أو القيام بعمليات غسيل الأموال باستخدام معلومات العملاء الشخصية.

(2) مخاطر السمعة REPUTATIONAL RISK:

تنشأ مخاطر السمعة في حالة توافر رأى عام سلبي تجاه البنك، الأمر الذي قد يمتد إلى التأثير على بنوك أخرى نتيجة عدم مقدرة البنك على إدارة نظمه بكفاءة أو حدوث اختراق مؤثر فيه.

(3) المخاطر القانونية LEGAL RISK:

تقع هذه المخاطر في حالة انتهاك القوانين أو القواعد أو الضوابط المقررة خاصة تلك المتعلقة بمكافحة عمليات غسيل الأموال، أو نتيجة عدم التحديد الواضح للحقوق والالتزامات القانونية الناتجة عن العمليات المصرفية الإلكترونية، ومن ذلك عدم وضوح مدى توافر قواعد لحماية المستهلكين في بعض الدول، أو لعدم المعرفة القانونية VALIDITY لبعض الاتفاقيات المبرمة باستخدام وسائل الوساطة الإلكترونية.

(4) المخاطر الأخرى مثل:

ارتفاع تكاليف جذب عملاء جدد للمعاملات المصرفية من خلال الإنترنت، لذا فقد بدأت بنوك الإنترنت في التراجع عن تقديم خدماتها المجانية للعملاء في ظل تزايد النفقات وتراجع الإيرادات ومن أمثلة هذه البنوك wingspan bank. Com.

لم تصل البنوك الإلكترونية حتى الآن لفهم واضح لمتطلبات عملائها وكيفية تحقيق هذه المتطلبات على مواقعها بالشكل الأمثل، مما يعني أن هناك حلقة مفقودة بين متطلبات العملاء كما تراها هذه البنوك وبين الاستجابة الواقعية لها.

صعوبة الاعتماد على الإنترنت فقط كوسيلة لتقديم الخدمات المصرفية، فحتى الآن لا تستطيع هذه البنوك أن تحل محل البنوك التقليدية تمامًا، وذلك نظرًا لما أثبتته الدراسات عن أهمية الوجود المادي لهذه البنوك حيث إن العملاء يفضلون الحصول على خدمة بها تفاعل شخصي أكثر من الحصول على خدمة تلائم ظروفهم ولمدة 24 ساعة بالإضافة إلى عامل الأمان الذي يوفره لهم التواجد المادي للبنك الذي يتعاملون معه.

تعد عمليات الإيداع إحدى المشاكل التي يواجهها عملاء بنوك الإنترنت، فعلى عكس عمليات الإيداع المباشر التي تتم من خلال البنوك التقليدية يضطر عميل بنك الإنترنت لإرسال المبالغ التي يريد إيداعها بالبريد، فإذا كان العميل يقوم بعمليات إيداع نقدي بشكل متكرّر فقط تصبح هذه المشكلة ذات وزن كبير بالنسبة له.

وهنا تأتي أهمية وضع استراتيجية عامة للبنك تحدد الأهداف المرجوة من إدخال العمل

المصرفي الإلكتروني وطرق تحقيق ذلك وضمان عملية التنفيذ بشكل سليم وأمن بعيدًا عن المخاطر التي تحيط بالعمل المصرفي الإلكتروني.

الأمن المعلوماتي لأنظمة المعلومات :

يعد التطور السريع في تكنولوجيا المعلومات والانتشار الواسع للنظم والبرامج الصديقة وتطور ووسائل تخزين المعلومات وتبادلها بطرق مختلفه أو ما يسمى نقل البيانات عبر الشبكة من موقع لآخر أدى إلى أن تكون هذه المعلومات عرضة للاختراق لذلك أصبحت هذه التقنية سلاحا ذو حدين تحرص المنظمات على إقتناءه وتوفير سبل الحماية له . إن موضوع الأمن المعلوماتي يرتبط ارتباطا وثيقا بأمن الحاسوب فلا يوجد أمن للمعلومات إذا لم يراعى أمن الحاسوب ، وفي ظل التطورات المتسارعة في العالم والتي أثرت على الإمكانات التقنية المتقدمة المتاحة والرامية إلى خرق منظومات الحاسوب بهدف السرقة أو تخريب المعلومات أو تدمير أجهزة الحاسوب ، كان لا بد من التفكير الجدي لتحديد الإجراءات الدفاعية والوقائية وحسب الإمكانات المتوفرة لحمايتها من أي اختراق أو تخريب ، ومن هنا تظهر مهمة جديدة ومسؤولية كبيرة أمام إدارة نظم المعلومات في المنشأة وهي ضرورة توفير الوسائل والأساليب اللازمة لضمان استمرارية عمل هذه النظم بشكل صحيح والتخطيط الدقيق لمواجهة جميع الأخطار التي يمكن أن تؤدي إلى تعطلها أو توقفها عن العمل، وفي حال حدوث ذلك، التمكن من إعادة تشغيلها بأسرع وقت ممكن، وتسمى هذه الوظيفة الهامة والضرورية جدا حماية وأمن نظم المعلومات، وتهدف هذه الوظيفة إلى حماية الموارد المحوسبة من الأخطار والتهديدات المقصودة وغير المقصودة التي يمكن أن تؤدي إلى عمليات غير ، مسموح بها مثل تعديل أو انكشاف أو تخريب البيانات أو البرامج.

أولا : مفهوم الأمن المعلوماتي

يعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيات إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال ، فهو مجموعة

من التدابير الوقائية المستخدمة في المجالين الإداري والفني لحماية مصادر البيانات من أجهزة وبرمجيات وبيانات من التجاوزات أو التداخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلسل أو الإجراءات الخاطئة المستخدمة من قبل إدارة المصادر المعلوماتية ، فضلا عن إجراءات مواجهة الأخطار الناتجة عن الكوارث الطبيعية المحتملة التي تؤدي إلى فقدان بعض المصادر كلاً أو جزءًا ، ومن ثم التأثير على نوع ومستوى الخدمة المقدمة.

ثانيا : مراحل تطور مفهوم الأمن المعلوماتي

إن مفهوم الأمن المعلوماتي مر بمراحل تطويرية عدة أدت إلى ظهور ما يسمى بأمنية المعلومات ، ففي الستينات كانت الحواسيب هي كل ما يشغل العاملين في أقسام المعلومات ، وكان مفهوم الأمنية يدور حول تحديد الوصول أو الإطلاع على البيانات من خلال منع الغرباء الخارجيين من التلاعب في الأجهزة لذلك ظهر مصطلح أمن الحواسيب والذي يعني حماية الحواسيب وقواعد البيانات ، ونتيجة للتوسع في استخدام أجهزة الحاسوب وما تؤديه من منافع تتعلق بالمعالجة للحجوم الكبيرة من البيانات ، تغير الاهتمام ليمثل السيطرة على البيانات وحمايتها . وفي السبعينات تم الانتقال إلى مفهوم أمن البيانات ورافق ذلك استخدام كلمات السر البسيطة للسيطرة على الوصول للبيانات إضافة إلى وضع إجراءات الحماية لمواقع الحواسيب من الكوارث واعتماد خطط لخزن نسخ إضافية من البيانات والبرمجيات بعيدا عن موقع الحاسوب ، وفي مرحلة الثمانينات والتسعينات ازدادت أهمية استخدام البيانات ، وساهمت التطورات في مجال تكنولوجيا المعلومات بالسماح لأكثر من مستخدم للمشاركة في قواعد البيانات ، كل هذا أدى إلى الانتقال من مفهوم أمن البيانات إلى أمن المعلومات ، وأصبح من الضروري المحافظة على المعلومات وتكاملها وتوفرها ودرجة موثوقيتها ، حيث أن الإجراءات الأمنية المناسبة يمكن أن تساهم في ضمان النتائج المرجوة وتقلص اختراق المعلومات والتلاعب بها ، وفي ظل انتشار أنظمة الذكاء الإصطناعي وازدياد معدلات تناقل البيانات بسرعة الضوء أو التفاعل بين المنظومات والشبكات وصغر حجم أجهزة الحاسوب المستخدمة قد يكون أمن المعرفة هو الخطوة القادمة بعد أمن المعلومات.

ثالثا : الأخطار التي يمكن أن تتعرض لها أنظمة المعلومات المعتمدة على الحاسب

تعتبر المخاطر المقصودة أشد خطرا على أداء فعالية النظم وتزداد تلك الخطورة في النظم الإلكترونية . وتكمن خطورة مشاكل أمن المعلومات في عدة جوانب منها تقليل أداء الأنظمة الحاسوبية، أو تخريبها بالكامل مما يؤدي إلى تعطيل الخدمات الحيوية للمنشأة، أما الجانب الآخر فيشمل سرية وتكامل المعلومات حيث قد يؤدي الإطلاع والتصنت على المعلومات السرية أو تغييرها إلى خسائر مادية أو معنوية كبيرة

ويمكن تصنيف المخاطر من وجهات نظر مختلفة إلى عدة أنواع:

أولا: من حيث مصدرها

- **مخاطر داخلية:**

حيث يعتبر موظفي المنشآت هم المصدر الرئيسي للمخاطر الداخلية التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية وذلك لأن موظفي المنشآت على علم ومعرفة بمعلومات النظام وأكثر دراية من غيرهم بالنظام الرقابي المطبق لدى المنشأة، ومعرفة نقاط القوة والضعف ونقاط القصور لهذا النظام ويكون لديهم القدرة على التعامل مع المعلومات والوصول إليها من خلال صلاحيات الدخول الممنوحة لهم، ولذلك فإن موظفي الشركة غير الأمناء يستطيعون الوصول للبيانات وإمكانية تدميرها أو تحريفها أو تغييرها

- **مخاطر خارجية:**

وتتمثل في أشخاص خارج المنشأة ليس لهم علاقة مباشرة بالمنشأة مثل قراصنة المعلومات والمنافسين الذين يحاولون اختراق الضوابط الرقابية والأمنية للنظام بهدف الحصول على معلومات سرية عن المنشأة أو قد تتمثل في كوارث طبيعية مثل الزلزال والبراكين والفيضانات والتي قد تحدث تدمير جزئي أو كلي للنظام في المنشاة

ثانيًا : من حيث المتسبب بها

- **مخاطر ناتجة عن العنصر البشري**

و هي التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات أو خلال عمليات البرمجة أو الاختبار أو التجميع للبيانات أو أثناء إدخالها إلى النظام ، أو في عمليات

تحديد الصلاحيات للمستخدمين ، وتشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن وسلامة نظم المعلومات في المنظمات .

- **مخاطر ناتجة عن العنصر الغير بشري**

و هذه تشمل الزلازل والعواصف والفيضانات والأعاصير والمشاكل المتعلقة بأعطال التيار الكهربائي والحرائق إضافة إلى المشاكل القائمة في تعطل أنظمة التكييف والتبريد وغيرها ، وتؤدي هذه الأخطار إلى تعطل عمل هذه التجهيزات وتوقفها لفترات طويلة نسبيا لإجراء الإصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات .

ثالثا : من حيث أساس العمدية:

- مخاطر ناتجة عن تصرفات متعمدة مقصودة.
- مخاطر ناتجة عن تصرفات غير متعمدة غير مقصودة.

رابعًا : من حيث الآثار الناتجة عنها:

- مخاطر ينتج عنها أضرار مادية.
- مخاطر فنية ومنطقية.

خامسا : المخاطر على أساس علاقتها بمراحل النظام:

- مخاطر المدخلات.
- مخاطر التشغيل.
- مخاطر المخرجات.

رابعًا : الحماية من الأخطار :

تعتبر عملية الحماية من الأخطار التي تهدد أنظمة المعلومات من المهام المعقدة والصعبة والتي تتطلب من إدارة نظم المعلومات الكثير من الوقت والجهد والموارد المالية وذلك للأسباب التالية :

1. العدد الكبير من الأخطار التي تهدد عمل نظم المعلومات .
2. توزع الموارد المحوسبة على العديد من المواقع التي يمكن أن تكون أيضا متباعدة .
3. وجود التجهيزات المحوسبة في عهدة أفراد عديدين في المنظمة وأحيانا خارجها .
4. صعوبة الحماية من الأخطار الناتجة عن ارتباط المنظمة بالشبكات الخارجية .

5. التقدم التقني السريع يجعل الكثير من وسائل الحماية متقادمة من بعد فترة وجيزة من استخدامها.
6. التأخر في اكتشاف الجرائم المحوسبة مما لا يتيح للمنظمة إمكانية التعلم من التجربة والخبرة المتاحة.
7. تكاليف الحماية يمكن أن تكون عالية بحيث لا تستطيع العديد من المنظمات تحملها .

هذا وتقع مسؤولية وضع خطة الحماية للأنشطة الرئيسية على مدير نظم المعلومات في المنظمة على أن تتضمن هذه الخطة إدخال وسائل الرقابة التي تضمن تحقيق ما يلي :

- الوقاية من الأخطار غير المتعمدة .
- إعاقة أو صنع الأعمال التخريبية المتعمدة .
- اكتشاف المشاكل بشكل مبكر قدر الإمكان .
- المساعدة في تصحيح الأعطال واسترجاع النظام .

و يمكن تصميم نظام الرقابة ضمن عملية تطوير نظام المعلومات ويجب أن يركز هذا النظام على مفهوم الوقاية من الأخطار ، ويمكن أن يصمم لحماية جميع مكونات النظام بما فيها التجهيزات والبرمجيات والشبكات .

خامسًا : العناصر الأساسية لنظام الأمن المعلوماتي:

إن النظام الأمني الفعال يجب أن يشمل جميع العناصر ذات الصلة بنظام المعلومات المحوسبة ويمكن تحديد هذه العناصر بما يلي :

(1) منظومة الأجهزة الإلكترونية وملحقاتها :

إن أجهزة الحواسيب تتطور بشكل بالمقابل هناك تتطور في مجال السبل المستخدمة لاختراقها مما يتطلب تطوير القابليات والمهارات للعاملين في أقسام المعلومات لكي يستطيعوا مواجهة حالات التلاعب والعبث المقصود في الأجهزة أو غير المقصود .

(2) الأفراد العاملين في أقسام المعلومات :

يلعب الفرد دورا أساسيا ومهما في مجال أمن المعلومات والحواسيب وله تأثير فعال في أداء عمل الحواسيب بجانبيه الإيجابي والسلبي ، فهو عامل مؤثر في حماية الحواسيب

والمعلومات ولكن في الوقت نفسه فإنه عامل سلبي في مجال تخريب الأجهزة وسرقة المعلومات سواء لمصالح ذاتية أو لمصالح الغير ، إن من متطلبات أمن الحواسيب تحديد مواصفات محددة للعاملين ووضع تعليمات واضحة لاختيارهم وذلك للتقليل من المخاطر التي يمكن أن يكون مصدرها الأفراد إضافة إلى وضع الخطط لزيادة الحس الأمني والحصانة من التخريب ، كما يتطلب الأمر المراجعة الدورية للتدقيق في الشخصية والسلوكية للأفراد العاملين من وقت لآخر وربما يتم تغيير مواقع عملهم ومحاولة عدم احتكار المهام على موظفين محدودين .

(3) البرمجيات المستخدمة في تشغيل النظام :

تعتبر البرمجيات من المكونات غير المادية وعنصر أساس في نجاح استخدام النظام ، لذلك من الأفضل اختيار حواسيب ذات أنظمة تشغيل لها خصائص أمنية ويمكن أن تحقق حماية للبرامج وطرق حفظ كلمات السر وطريقة إدارة نظام التشغيل وأنظمة الاتصالات ، إن أمن البرمجيات يتطلب أن يؤخذ هذا الأمر بعين الاعتبار عند تصميم النظام وكتابة برامجه من خلال وضع عدد من الإجراءات كالمفاتيح والعوائق التي تضمن عدم تمكن المستفيد من التصرف خارج الحدود المخول بها وتمنع أي شخص من إمكانية التلاعب والدخول إلى النظام وذلك من خلال أيضا تحديد الصلاحيات في مجال قراءة الملفات أو الكتابة فيها ، ومحاولة التمييز بين اللذين يحق لهم الإطلاع وحسب كلمات السر الموضوعة ، وهناك أسلوبان للتمييز إما عن طريق البرمجيات أو استخدام الأجهزة المجفرة .

(4) شبكة تناقل المعلومات :

تعتبر شبكة تناقل المعلومات المحلية أو الدولية ثمرة من ثمرات التطورات في مجالات الاتصالات كما أنها سهلت عملية التراسل بين الحواسيب وتبادل واستخدام الملفات ، ولكن من جهة أخرى إتاحة عملية سرقة المعلومات أو تدميرها سواء من الداخل كاستخدام الفيروسات أو من خلال الدخول عبر منظومات الاتصال المختلفة ، لذلك لا بد من وضع إجراءات حماية وضمان أمن الشبكات من خلال إجراء الفحوصات المستمرة لهذه المنظومات وتوفير الأجهزة الخاصة بالفحص ، كما أن نظم التشغيل المستخدمة والمسؤولة عن إدارة الحواسيب يجب أن تتمتع بكفاءة وقدرة عالية على الكشف عن التسلل إلى الشبكة وذلك من

خلال تصميم نظم محمية بإقفال معقد أو عن طريق المجفرات وربطها بخطوط الاتصال والتي هي عبارة عن استخدام الخوارزميات الرياضية أو أجهزة ومعدات لغرض تجفير تناقل المعلومات أو الملفات .

(5) مواقع منظومة الأجهزة الإلكترونية وملحقاتها :

يجب أن تعطى أهمية للمواقع والأبنية التي يحوي أجهزة الحواسيب وملحقاتها ، وحسب طبيعة المنظومات والتطبيقات المستخدمة يتم اتخاذ الإجراءات الاحترازية لحماية الموقع وتحصينه من أي تخريب أو سطو وحمايته من الحريق أو تسرب المياه والفيضانات ، ومحاولة إدامة مصدر القدرة الكهربائية وانتظامها وتحديد أساليب وإجراءات التفتيش والتحقق من هوية الأفراد الداخلين والخارجين من الموقع وعمل سجل لذلك .

مبادئ إدارة المخاطر وأمن المعلومات RISK MANAGEMENT:

تشتمل إدارة المخاطر على التقييم والرقابة والمتابعة وذلك على النحو التالي:

(1) تقييم مخاطر Assessing Risk:

ويشمل التقييم ما يلي:

أ- تحديد المخاطر التي قد يتعرض لها البنك، ومدى تأثيرها عليه.

ب- وضع حدود قصوى لما يمكن للبنك أن يتحمله من خسائر نتيجة التعامل مع هذه المخاطر.

(2) الرقابة على التعرض للمخاطر Controlling Risk Exposures:

تشتمل هذه الرقابة على ستة مجالات على النحو التالي:

أ- تنفيذ سياسات وإجراءات التأمين بهدف: Implementing Security Policies and Measures

- تحديد شخصية المتعامل مع النظم.
- ضمان عدم إجراء تعديلات على رسائل العملاء أثناء انتقالها عبر القنوات.
- ضمان الحفاظ على سرية معاملات العملاء PRIVACY.

ويراعى في هذا المجال ما يلي:

1- إتباع سياسات وإجراءات تحقق تأمين الاتصالات من وإلى النظم لمنع أو الحد من اختراق غير المرخص لم للنظم أو إساءة استخدامها.

2- الرقابة على الدخول إلى النظم وتحديد شخصية المستخدمين.

3- حماية النظم من احتمالات القيام بممارسات غير مرخص بها من قبل العاملين بالبنك السابقين أو الجدد أو المؤقتين.

ب- تدعيم الاتصالات بين المستويات المختلفة بالبنك من مجلس إدارة وإدارة عليا وبين العاملين بشأن سلامة أداء النظم وتوفير التدريب المستمر للعاملين.

ج- استمرار تقديم وتطوير الخدمات.

د- وضع ضوابط للحد من المخاطر في حالة الاعتماد على مصادر خارج البنك لتقديم الدعم الفني.

وتشتمل هذه الضوابط على ما يلي:

- متابعة الأداء المالي ولتشغيلي لمقدم الدعم الفني.
- التأكد من توافر اتفاقيات تعاقدية مع مقدمي الدعم الفني تحدد التزامات الأطراف تفصيليًا.
- التأكد من مقدرة مقدمي الدعم الفني على توفير التأمين اللازم بما يتفق مع ما هو متبع داخل البنك في حالة تعرفهم على بيانات ذات حساسية تخص البنك، وذلك من خلال مراجعة سياساتهم وإجراءاتهم في هذا المجال.
- توفير ترتيبات طوارئ لتغطية احتمالات تغيير مفاجئ في مقدمي الدعم الفني.

هـ- إحاطة العملاء عن العمليات المصرفية الإلكترونية وكيفية استخدامها.

و- إعداد خطط طوارئ Contingency Planning.

ز- إعداد خطط طوارئ بديلة في حالة إخفاق النظم عن أداء الخدمات.

وذلك فيما يتعلق بما يلي:

- إعادة البيانات إلى الوضع الذي كانت عليه قبل الإخفاق.
- توفير قدرات بديلة لتشغيل البيانات.
- توفير عاملين لمواجهة الظروف الطارئة.
- اختيار نظم التشغيل البديلة Backup System بصفة دورية للتأكد من فاعليتها.
- توافر التأمين اللازم في حالة تنفيذ خطط الطوارئ وكذا توافر تعليمات لاستخدام هذه الخطط لدى مقدمي الدعم الفني.
- إبرام عقود بديلة مع مقدمي دعم فني متخصصين جدد في حالة إخفاق المقدمين الأساسيين.

(3) متابعة مخاطر Monitorig Risk:

تتمثل متابعة المخاطر في اختبار النظم وإجراء المراجعة الداخلية والخارجية وذلك على النحو التالي:

أ- إجراء اختبارات دورية للنظم والتي يكون من ضمنها.

ب- إجراء اختبار إمكان الاختراق Penetration Testing الذي يهدف إلى تحديد وعزل وتعزيز تدفق البيانات من خلال النظم وإتباع إجراءات لحماية النظم من المحاولات غير العادية للاختراق.

ج- إجراء مراجعة دورية من خلال النظم للتأكد من فاعلية التأمين والوقوف على مدى اتساقها مع سياسات وإجراءات التأمين المقررة.

د- إجراءات المراجعة الداخلية والخارجية إذ تسهم المراجعة الداخلية والخارجية في تتبع الثغرات وحالات عدم الكفاءة وتخفيض حجم المخاطر بهدف التحقق من توافر سياسات وإجراءات مطورة والتزام البنك بها.