لجنة الرقابة على المصارف
مصرف لبنان

بيروت في ٢٠١١/١٠/٢٧

تعميم رقم ٢٧٢
موجّه إلى المصارف والمؤسسات المالية ومؤسسات الوساطة المالية

الموضوع: أمان أنظمة تكنولوجيا المعلومات لدى المصارف
والمؤسسات المالية ومؤسسات الوساطة المالية

بالاستناد الى تعميم مصرف لبنان الأساسي رقم ١٢٣ تاريخ ٢٠٠٩/٨/٢١ المتعلّق بخطة استمرار التشغيل أثناء وبعد حدوث كارثة، وعطفاً على تعميم لجنة الرقابة على المصارف رقم ٢٢٢ تاريخ ٢٠٠٠/٨/١٨ المتعلّق بالتوجيهات العامة المختصة بالقواعد التنظيمية لأمان تكنولوجيا المعلومات، يُطلب من جميع المصارف والمؤسسات المالية ومؤسسات الوساطة المالية اتخاذ الإجراءات التالية:

المادة الأولى : في حال اعتماد أنظمة أو برامج معلوماتية جديدة

تتمّ عملية اعتماد أنظمة أو برامج معلوماتية جديدة (Central or Branch systems) بشكل أساسي، وفق ما يلي:

١. اختيار الأنظمة الجديدة وفق استراتيجية معلوماتية لأنظمة تكنولوجيا المعلومات تنطلق من الاستراتيجية العامة لنشاطات المصرف أو المؤسسة وتتوافق مع طبيعة ومتطلبات العمل لناحية ماهية المعلومات وهيكليتها.

٢. وضع مستند بمواصفات البرنامج أو النظام المطلوب إنجازه وذلك بعد إجراء الدراسات المناسبة لحاجات ومتطلبات العمل في هذا الشأن.

٣. اعتماد منهجية محدّدة لمراحل تنفيذ مشاريع الأنظمة والبرامج الجديدة (Systems Development Life Cycle SDLC) تتوافق مع المعايير العلمية والتقنية العالمية المعمول بها.

٤. احتواء عقود تنفيذ المشاريع لبنود تضمن عملية تطوير واستمرارية الأنظمة والبرامج المستحدثة، وذلك إما عن طريق الاستحواذ على البرامج الأم (Source Programs) أو اللجوء إلى اتفاق لوضع نسخة عن هذه الأنظمة والبرامج لدى طرف ثالث (Escrow Agreement) وتحديثها كلّما تطلب الأمر.

٥. وضع جدول بالمتسلمات (Deliverables) مع تواريخ تسلّمها على أن يتضمّن كحدّ أدنى:
- تواريخ إنجاز المراحل التنفيذية الأساسية لكل مشروع.
- الأنظمة والبرامج والمتفرعات (Additional scripts) من أجهزة وبرامج مساعدة (Utilities) أو محيطة (Interfaces) المطلوب إعدادها أو تنفيذها.
- برنامج تدريب الجهاز البشري المخوّل استلام الأنظمة والبرامج المستحدثة.
- برنامج الاختبارات، بحسب نوع كل اختبار مرفقاً بالمتطلبات التقنية والعملية والتقييمية لحسن إتمامه.
- آلية وأسس اختبارات القبول (Acceptance Testing) التي على أساسها يتمّ قبول البرامج طبقاً للمواصفات العملانية (Functionalities) والتقنية (Technical / System) الموضوعة.

٦. تَسلُّم المصرف أو المؤسسة مستندات الأنظمة والبرامج، وأهمّها مستندات الاستعمال، مستندات التشغيل التقنية، مرجع للمشاكل والالتباسات وطريقة معالجتها (Troubleshooting)، وكذلك المستندات التي تتيح فهم وتعديل البرامج الأم (Source Program) إذا تضمّنها عقد التنفيذ.

٧. التشديد على إنجاز اختبارات مركّزة ومستفيضة قبل التوقيع على القبول بصورة نهائية على أن يتمّ لحظ معايير الجودة (Performance) والأمان (Vulnerability ensuring software security) والثبات (Robustness ensuring the stability of the application over time) ، وعلى أن تشمل تحديداً:
- اختبارات تقنية (Technical Test).
- اختبارات عملانية (Functional Tests).
- اختبارات لدورة العمل الكاملة (Integration Test).
- اختبارات الضغط والسعة (Capacity and Stress Tests).
- اختبارات القبول النهائية التي يُجريها المستعملون بصورة أساسية (User Acceptance Test).

٨. توثيق جميع المستندات العائدة لإنجاز المشروع من دراسات وملفات تنفيذ وخطط اختبارات وخطط وضع النظام أو البرامج الجديدة في الخدمة الفعلية وذلك تسهيلاً لأعمال التدقيق والمراجعة.

٩. تزويد لجنة الرقابة على المصارف بالمعلومات المتعلّقة بكلٍّ من المراحل التالية أدناه، وذلك وفق الاستمارة المرفقة (ITSACQ01, Excel Sheet):

أ) <u>مرحلة أولى</u> : عند اتخاذ القرار باعتماد أنظمة معلوماتية رئيسية جديدة (تحديد طريقة الإنجاز والجهة المُكلّفة التنفيذ والروزنامة المُقررة).

ب) <u>مرحلة ثانية</u> : عند تحديد تواريخ وضع الأنظمة أو البرامج المستحدثة في الخدمة الفعلية، إبلاغ لجنة الرقابة على المصارف بهذه التواريخ على أن يتمّ الإبلاغ في حال الأنظمة الرئيسية (Core and Branch Systems) قبل ثلاثة أشهر على الأقل من أول تاريخ وضع فعلي مرفقاً بخطط وضع هذه الأنظمة موضع التطبيق وبسُبُل الاحتياط لأي تعثّر يُمكن أن يطرأ بعد وضعها في الخدمة الفعلية (parallel run or eventual reverse migration or specific support procedures).

ج) <u>مرحلة مستجدة</u> : عند اللجوء إلى تعديلات أساسية تتناول خطط أو ماهية أو تواريخ إطلاق هذه الأنظمة والبرامج، تزويد لجنة الرقابة على المصارف بالتعديلات التي تطرأ.

المادة الثانية: حالات إبلاغ لجنة الرقابة على المصارف عن حوادث إرباك الأنظمة المعلوماتية والتشغيلية الرئيسية الناتجة عن عوامل داخلية أو خارجية

بهدف توفير الدعم والمساعدة في حالات التعثّر أو الإرباك التي قد تطال نشاطات أو خدمات المصرف أو المؤسسة وبهدف تفادي انتشارها، يجب إبلاغ لجنة الرقابة على المصارف بأي تعثّر أو إرباك في هذه الأنظمة مع مراعاة سريّة الإبلاغ، وذلك وفق الاستمارة المرفقة (ITSIRP01, Excel Sheet) على أن تتمّ عملية الإبلاغ كما يلي:

١. **تحديد حالات الإرباك**

يُقصد بحالات الإرباك أو التعثّر ما يلي:

أ) توقُّف أو تعثّر أساسي للأنظمة المعلوماتية نتيجة عطل في أحد مكوّناتها، أجهزةً أم برامج، بما فيها شبكات الاتصالات، هذا إذا نتج عنه مخاطر حصول أخطاء في البيانات والتقارير أو مخاطر مالية أو مخاطر سُمعة.

ب) عوارض أخطاء مُزمنة ومتكررة للنظام المعلوماتي وغير محدّدة السبب.

ج) عمليات تخريب داخلية مثل سرقة معلومات أو ملفات أو العبث بالبرامج.

د) خلو أحد المراكز الحسّاسة في هيكلية إدارة الأنظمة المعلوماتية بشكل يُعرّض الأنظمة لمخاطر إرباكات مختلفة (عدم ضمان دقة المعلومات، تأخير في صدور البيانات، الخ...).

ه) تعرّض الخدمات المصرفية او المالية المُتاحة على شبكات الانترنت لعوامل خارجية أو داخلية مسيئة (System Failure or Web Sites Attack).

و) عمليات أو محاولات الاختلاس التي تتعرّض لها أجهزة الصرّاف الآلي أو أجهزة نقاط البيع أو نظام بطاقات الدفع والائتمان.

ز) أية حالات أخرى يمكن أن تشكل مخاطر تشغيلية محقّقة وتدخل في نمط حالات الإبلاغ المشار إليها في البند الثاني أدناه.

٢. **تحديد حالات الإبلاغ**

يجب أن يتمّ الإبلاغ في الحالات التالية:

أ) في حال تَجاوَزَ التوقّف الكلي أو التعثّر الجزئي للعمليات الأساسية للزبائن أو للجهات الخارجية المتعاملة مع المصرف أو المؤسسة، إقفال اليومية وافتتاح اليوم التالي.

ب) في حال ظهور خطأ جذري ومنهجي يطاول ذمم العملاء أو التصريحات أو التقارير أو في حال ترتّب على خطأ ما مخاطر مالية أو مخاطر سمعة، وما لم يتمّ معالجته قبل افتتاح اليوم الذي يلي يوم اكتشافه.

ج) في حال الاختراقات التي تتعرّض لها الأجهزة أو الأنظمة، إن لأسباب داخلية أو خارجية (توقّف قسري جرّاء عوامل مختلفة، تعرّض الأنظمة لهجومات وباء أو برامج خبيثة، عمليات الاختلاس التي تطال أجهزة الصرّاف الآلي...) أو في حال تأثرت عمليات المصرف أو المؤسسة بأوضاع وحالات إرباك تطال مصارف أو مؤسسات أخرى تتعامل معها.

د) أية حالات أخرى تدخل مفاعيلها في نمط النقاط الثلاث السابقة.

٣. **آلية الإبلاغ**

تطلب لجنة الرقابة على المصارف إبلاغها من قِبَل جهة مخوّلة من إدارة المصرف أو المؤسسة بحالات الإرباك أو التوقف فور التأكّد من حدوثها بأية وسيلة متاحة ومن ثمّ تزويدها خلال ٢٤ ساعة من تاريخه بتقرير يشرح ماهية التوقّف أو الإرباك أو التعثر الحاصل وحجم الأضرار الناتجة عنه والمتوقّعة لحين الانتهاء من معالجته نهائياً، وذلك وفق الاستمارة (ITSIRP01).

المادة الثالثة: في قواعد التلزيم الخارجي (Outsourcing)

على المصارف والمؤسسات المالية ومؤسسات الوساطة المالية التي تلجأ إلى تلزيم إحدى خدماتها أو نشاطاتها أو مواردها البشرية أو المادية المتعلّقة بأنظمة تكنولوجيا المعلومات إلى إحدى الشركات المحلية أو الخارجية التي تُعرف بالشركات الملتزمة (Outsourcing Service Providers) مراعاة المبادئ الأساسية التالية:

١. إنّ مسؤولية المصرف أو المؤسسة المعنية تجاه مصرف لبنان ولجنة الرقابة على المصارف وهيئة التحقيق الخاصة وتجاه الزبائن وجميع الجهات المتعاملة مع المصرف أو المؤسسة، تبقى قائمة بمفاعيلها كافة في حال تم تلزيم، بشكل أولي أو ثانوي، الخدمات الواجب القيام بها.

٢. يجب أن يرتكز قرار التلزيم على دراسات مبيّنة لصوابية الخيار المتّخذ على أن يتمّ توثيق هذه الدراسات تسهيلاً لأعمال المراجعة والتدقيق.

٣. يجب أن يراعي اختيار الشركة الملتزمة معايير الكفاءة والخبرة والملاءة والنزاهة وأن يتمّ وفق دفتر شروط واضح وشامل.

٤. على المصرف أو المؤسسة مراقبة سلامة أداء الشركة الملتزمة وتقييمها دورياً واتخاذ الإجراءات المناسبة لتصحيح أي خلل في تنفيذ عقد التلزيم عند الحاجة، بما فيه اللجوء إلى إنهائه طوعاً.

٥. وضع أسس واضحة لاختيار الشركة الملتزمة المناسبة وفق المعايير التالية:
أ) اختيار الشركات المرشّحة لالتزام الخدمة وفق دفتر شروط واضح وشامل (RFP).
ب) دراسة وضعية الشركة الملتزمة، مالياً وإدارياً وتقنياً، وخبرتها في تقديم الخدمة المطلوبة.
ج) تضمين دفتر الشروط، ولاحقاً العقود التي تستتبعها، البنود التي تضمن التزام الشركات الملتزمة بتقديم الخدمة وفق متطلبات تعاميم ومذكرات مصرف لبنان ولجنة الرقابة على المصارف وهيئة التحقيق الخاصة.

٦. تضمين عقود التلزيم البنود التي تشير إلى التدابير التالية:
أ) في حال تمّ اللجوء إلى تلزيم ثانوي (Subcontracting) يجب إخضاعه لشروط التلزيم الأولي بكل مندرجاته القانونية والإجرائية والرقابية.
ب) تفصيل شروط تسيير الخدمة بشكل جيّد ومضمون (Service Level Agreement).
ج) التزام الشركة المعنية بسريّة وخصوصية المعلومات.
د) التزام الشركة المعنية بمتطلبات الأمان بحسب تعاميم مصرف لبنان ولجنة الرقابة ذات الصلة.
ه) قيام الشركة الملزِّمة بإجراء التقييم الدوري لجودة الخدمة المقدّمة لها ومستوى أدائها بشكل يسمح باستباق أي خلل مُمكن ومحاسبة الشركة الملتزمة من جراء الخروج عن مستوى الأداء المُتفَق عليه.
و) تحديد المفاعيل التعاقدية لتدنّي مستوى الخدمة أو التدني الخطير لمستوى أو فعالية الشركة بشكل عام.
ز) تحديد شروط إنهاء عقد التلزيم وترتيبات استعادة الخدمة من قِبَل المؤسسة الملزِّمة.
ح) الالتزام بتسهيل عمل لجنة الرقابة على المصارف لجهة إجراء الرقابة الميدانية لمتطلبات الخدمة في مركز الشركة الملتزمة والاطلاع على قواعد المعلومات العائدة للخدمة الملزَّمَة.

٧. اتخاذ التدابير المناسبة لضمان استمرارية الخدمة في حال توقّف تقديمها من قِبَل الشركة الملتزمة وذلك وفقاً لاتفاقية محددة لإنهاء عقد التلزيم (Escrow Agreement upon source programs and Exit Strategies)، وبالتالي وضع خطط متابعة العمل التي تُمكّن من استعادة تسيير الخدمة داخلياً بشكل طبيعي وميسّر.

المادة الرابعة: تقارير جودة الأنظمة المعلوماتية وقواعد قياسها

يجب على المصارف والمؤسسات المالية ومؤسسات الوساطة المالية إعداد تقارير وافية حول جودة الأنظمة والبرامج وتكليف جهة ملمّة لتقييم جودة البرامج وقواعد المعلومات (Quality Assurance & Quality Control) على أن تقوم بشكل أساسي، بما يلي:

١. التأكد من استلام البرامج من مورّديها بشكل يراعي معايير الجودة (Quality Assurance) لجهة إنشاء البرامج ومطابقتها لدفتر شروط واضح ومفصّل.
٢. الاطلاع المباشر على جودة التنفيذ لجهة شموليته ومطابقته لمقاييس الجودة الموضوعة.
٣. تقييم مدى طواعية البرامج وسهولة استعمالها من قبل الموظفين ومدى استيعابهم لها بشكل لا يترك أي التباس أو تناقض في تفسيرها أو فهمها عند استعمالهم لها.
٤. التأكد من قدرة البرامج على استيعاب التطوير الذي يمكن أن يتطلّبه العمل على المدى المتوسط والطويل ومدى قابليتها للتعديلات التي تستجدّ.
٥. تقييم فعالية الأنظمة المعتمدة للخدمات المطلوبة بالنظر للمدّة الزمنية والكلفة المُترتّبة التي يتطلبها تنفيذ هذه الخدمات.
٦. التأكّد من توفّر وكفاية المستندات لحسن إدارة الأنظمة والبرامج وسهولة تعديلها وفق ما جاء في البند ٦ من المادة الأولى أعلاه.
٧. رفع تقارير دورية للإدارة العليا للمصرف أو المؤسسة حول جودة أداء الأنظمة والبرامج الأساسية المعتمدة (Quality Control) وتقييم مدى ملاءمتها لطبيعة العمل بالنظر لاستراتيجية وخطط المصرف أو المؤسسة.
٨. التأكّد من وجود البرامج الأم بمتناول المصرف أو المؤسسة (Source Programs) أو لدى طرف ثالث (Escrow Agreement) وفق ما جاء في البند ٤ من المادة الأولى أعلاه، وذلك حفاظاً على استمرارية هذه البرامج في حال عدم تمكّن الطرف المورّد من متابعة تقديمها وصيانتها بالشكل المعهود.

إن اللجنة تدعوكم لتحميل النسختين الالكترونيتين للاستمارتين (ITSACQ01 – ITSIRP01) المذكورتين أعلاه من الموقع الالكتروني للجنة : www.bccl.gov.lb على أن يتمّ تزويدها بها على أسطوانة (CD-Rom) مع نسخة مطبوعة منها وموقّعة بحسب الأصول المتّبعة كلّما استجّد وضعٌ يتطلب ذلك بحسب ما هو مبيّن في التعميم.

عن لجنة الرقابة على المصارف

الرئيس

أسامة مكداشي

لتحميل الإستمارة ITSACQ01 الضغط هنا
لتحميل الإستمارة ITSIRP01 الضغط هنا

ITSACQ01	إستمارة ITSACQ01 التصريح عن مشروع اعتماد أنظمة وبرامج معلوماتية جديدة أو مستحدثة		
رقم المصرف / المؤسسة		إسم المصرف / المؤسسة	
طبيعة التصريح		التسمية المعتمدة للمشروع	
المنتج (Product Name)			
النظام التشغيلي/ قاعدة المعلومات			
رح مقتضب للمشروع			
دوى المشروع			
الجهة المنفّذة (Developer)		داخلية /خارجية /مشتركة	
دير المشروع			

تاريخ إطلاق تنفيذ المشروع dd/mm/yyyy	تاريخ المتوقّع لإنجاز المشروع dd/mm/yyyy	تاريخ الوضع في الخدمة الفعلية dd/mm/yyyy	لمدة الإحترازية بعد الوضع في الخدمة الفعلية (أشهر) (e.g. Parallel Run)	مدة كفالة المنفّذ (أشهر)

ح مقتضب لمنهجية الإختبارات المزمع إجراؤها للنظام الجديد أو المعدّل
شرح مقتضب لعملية وضعه في الخدمة (مرحلياً كلّياً إشراك كل العاملين في المؤسسة أو فريق متخصص...)
ح للخطة الإحترازية في حال تعثّر النظام الجديد أو المعدّل بعد وضعه في الخدمة الفعلية

تاريخ التصريح	أسم المسؤول عن التصريح	رتبة المسؤول عن التصريح	الإمضاء

ITSIRP01	إستمارة ITSIRP01للإبلاغ عن إرباك أو توقف الأنظمة المعلوماتية والتشغيلية الرئيسية

رقم المصرف / المؤسسة		اسم المصرف / المؤسسة	

تصنيف الحالة حسب اللائحة		تاريخ حصول الإرباك	

شرح لحالة الإربك أو التوقّف

شرح تداعيات الإرباك أو التوقف على حسابات العملاء، الزبائن، الموظفين، الجهات الأخرى الخارجية...

شرح تداعيات الإرباك أو التوقف على حسابات الميزانية والتقارير الداخلية والخارجية(التقارير المرسلة إلى مصرف لبنان ولجنة الرقابة على المصارف وهيئة التحقيق الخاصة)

شرح تداعيات الإرباك أو التوقف لناحية الخسائر المادية والمالية المحققة

تقدير الخسائر المادية والمالية الإجمالية المتوقّعة لحين المعالجة النهائية الإرباك أو التوقف(مقدّرة بالعملة اللبنانية أو الأجنبية)

شرح الخطة الموضوعة للمعالجة النهائية

تاريخ المتوقّع لإنجاز المعالجة			
الجهة المُكلّفة بالمعالجة		داخلية /خارجية /مشتركة	

تاريخ الإبلاغ dd/mm/yyyy	أسم المسؤول عن الإبلاغ	رتبة المسؤول عن الإبلاغ	الإمضاء