



الرقم : ٩٩٤٣ / ١/١٠

التاريخ : ١٤٣٥/٨/٢١ هـ

الموافق : ٢٠١٤/٨/١٧ م

تعميم إلى البنوك المرخصة

لاحقا لتعليمات خطة استمرارية العمل رقم (٢٠٠٦/٢٧) تاريخ ٢٠٠٦/٣/٣٠، وإلى تعميمنا رقم (١٠٧٤٠/١/١٠) تاريخ ٢٠١٣/٨/٢٨ والذي تم بموجبه قيامكم بتكليف مدقي حساباتكم لفحص مدى اعتمادية خطة استمرارية العمل الخاصة بخدمة المقاصة الإلكترونية، وأكد على ما يلي:

١. الإلتزام بأحكام تعليمات خطة استمرارية العمل رقم (٢٠٠٦/٢٧) تاريخ ٢٠٠٦/٣/٣٠، وقراءة البنود أدناه ضمن الفهم العام لأحكام التعليمات.

٢. مراعاة الأولوية في حماية موجودات البنوك وعملياتها اعتمادا على أهميتها النسبية في معرض التخطيط لضمان استمرارية العمليات الحرجة، وعلى رأسها الحفاظ على سلامة العنصر البشري ضمن خطط منظمة للتعافي من الكوارث بحيث تكون خاضعة للتحديث والفحص والتدريب المستمر.

٣. رصد الموازنات اللازمة لبناء وتشغيل وفحص وديمومة خطط استمرارية العمل ضمن إطار التخطيط الاستراتيجي الشامل للبنوك.

٤. توثيق خطط استمرارية العمل بما في ذلك آليات اتخاذ القرار، وقواعد تصنيف الحوادث، والخيارات المختلفة الممكن اتباعها كاستراتيجيات للتعافي وإجراءاتها، ومهام الفرق المختلفة الواجب مشاركتها، وقوائم الاتصالات الهاتفية لرؤساء وأعضاء الفرق والموظفين ومزودي الخدمات، وإجراءات الإخلاء بما في ذلك تحديد نقاط التجمع.

٥. تنظيم خطط استمرارية العمل من خلال إيجاد الهياكل التنظيمية الهرمية واللجان التوجيهية وتضمين وثائق الوصف الوظيفي بمسؤوليات محددة تضمن ديمومة واعتمادية وصلاحية تلك الخطط، وعلى أن تتولى جهة مركزية (إدارة المخاطر واللجان التوجيهية المتعلقة بها) المسؤولية النهائية في إخراج تلك الخطط بالتنسيق والتعاون مع كافة الوحدات التنظيمية المعنية.

٦. شمول برامج المدقق الداخلي والمدقق الخارجي على آليات تضمن الرقابة والمتابعة المستمرة لخطط استمرارية العمل.

٧. الالتزام بنشر الوعي بمفاهيم وأهداف خطط استمرارية العمل ضمن إطار الثقافة العامة لإدارة المخاطر، وتدريب كافة الموظفين وعلى وجه الخصوص الأفراد المشاركين بسيناريوهات واستراتيجيات التعافي بشكل مستمر على الواجبات والمسؤوليات المنوطة بهم تجاه تلك الخطط بما يضمن تحقيقها لأهدافها واعتماديتها.

٨. أن لا يتجاوز الزمن المستهدف لإعادة التشغيل (RTO) (Recovery Time Objective) للخدمات الحرجة ساعتين، وتوفير الموارد البشرية والتكنولوجية المختلفة الأصلية والبديلة المعتمد عليها واللازمة للتشغيل والحفاظ على توافرية تلك الخدمة، واعتبار خدمة المقاصة الإلكترونية والخدمات المماثلة الأخرى من ضمن الخدمات الحرجة بموجب خطط استمرارية العمل.

٩. تطوير استراتيجيات ضمن إطار خطة شاملة للتعافي من الكوارث والحوادث المختلفة الخاصة بتكنولوجيا المعلومات والاتصالات، تلبي متطلبات خطة استمرارية العمل من حيث الزمن المستهدف لإعادة التشغيل (RTO) (Recovery Time Objective) للعمليات الحرجة المحددة بموجب تحليل الأثر على الأعمال (BIA) (Business Impact Analysis)، تتضمن على الأقل وبشكل خاص الأمور التالية:

أ. تجهيز موقع أصيل وآخر بديل لتشغيل موارد تكنولوجيا المعلومات في مكان مناسب يختلف من حيث احتمالية التعرض لنفس التهديدات التي يتعرض لها الموقع الأصيل، يشمل كل ما يلزم من موارد تكنولوجية على شكل خوادم وبرامج وبيانات وحلول حماية لنظم المعلومات ووسائل اتصالات وأجهزة حماية للوقاية من التهديدات المادية والبيئية.

ب. التنويع في استخدام خطوط الاتصالات، والاعتماد على أكثر من مزود خدمات واحد لهذا الغرض.

ج. اتباع الممارسات السليمة واستخدام الحلول المناسبة في إجراءات النسخ الاحتياطي بهدف الحفاظ على سرية وسلامة وتوفر تلك البيانات وفحصها من خلال استرجاعها للتأكد من اعتماديتها، وضرورة اتباع الممارسات السليمة من حيث عملية النقل والتخزين لوسائط النسخ الاحتياطي، وتفعيل الضوابط اللازمة بما في ذلك إجراءات الضبط والرقابة الثنائية في

الوصول لها، مع توفير متطلبات الحماية من الأحوال البيئية المحيطة والتبوع في أماكن التخزين والحفظ.

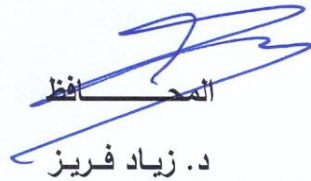
١٠. تطوير سيناريوهات لفحص خطط استمرارية الأعمال، والالتزام بإجراء تلك الفحوصات بشكل منتظم وتوثيق تلك الفحوصات وتحليلها وأخذ تغذية راجعة لتحسين أداء واعتمادية الخطط والتدريب على تنفيذها والعمل على تحديثها بشكل مستمر.

١١. مراعاة أن تتضمن الاتفاقيات الموقعة مع المزودين الخارجيين بخصوص الدعم الفني للخدمات بشكل عام والخدمات الحرجة بشكل خاص مسؤولياتها في توفير الدعم المطلوب ضمن شروط ملحقة بالاتفاقية (Service Level Agreement) (SLA) تضمن التوافرية بأعلى درجاتها وتفاصيلها في كافة الظروف وبما يتناسب مع متطلبات البنوك بحسب خطط استمرارية الأعمال لديها بهذا الخصوص.

١٢. أن تراعي سياسات التعهيد والاستعانة بخدمات الغير (Outsourcing Policies) لدى البنوك ضرورة توفر خطط لاستمرارية الأعمال لدى الغير معتمد عليها وبتأكيد دوري مستقل من جهة محايدة بشكل سنوي على الأقل، تضمن التوافرية والسرية لبيانات وعمليات البنوك لدى حدوث أي طارئ قد يؤدي لانقطاع تزويد تلك الخدمات، والعمل بهذه القاعدة كمعيار مهم عند اختيار المزودين للاستعانة بخدماتهم، وتضمن العقود والاتفاقيات الموقعة مع المزودين لتعكس هذه المتطلبات، ومخاطبة المزودين الحاليين لتوفيق أوضاعهم تلبية لذلك.

وختاماً أؤكد على ضرورة اتخاذ الإجراءات اللازمة لتصحيح نقاط الضعف الواردة ضمن تقارير مدققي حساباتكم الخارجيين بموجب تعميمنا المشار إليه أعلاه، وتولي كل من المدقق الداخلي والمدقق الخارجي مهام المتابعة المستمرة لذلك ضمن برامج التدقيق الدورية الاعتيادية، علماً بأننا سنقوم باتخاذ الإجراءات اللازمة للتأكد من قيامكم بالامتثال لتعليماتنا ولتقارير المدققين بهذا الخصوص.

وتفضلوا بقبول فائق الاحترام والتقدير،


المحافظ
د. زياد فريز