البنك المركزي الأردني

الدليل الإرشادي للحوسبة السحابية

(Cloud Computing Guideline)

March, 2018

فهرس المحتويات

المقدمة

شهد القطاع المالي والمصرفي في الآونة الأخيرة تطوراً كبيراً في مجال تكنولوجيا المعلومات والاتصالات واستخدامها لتقديم الخدمات المالية والمصرفية وحيث أن جميع الشركات ومؤسسات المال والأعمال في العالم تسعى دوماً إلى الإستفادة من هذه التكنولوجيا في تقليل تكلفة أعمالها وزيادة أرباحها توجهت هذه المؤسسات الى الإستفادة من أطراف خارجية تعمل على توفير العديد من المصادر اللازمة للشركات لإدارة وتقديم خدماتها وذلك عن طريق وصول مستخدمي هذه التكنولوجيا إلى جميع التطبيقات والخدمات من أي مكان وفي أي زمان عبر شبكة الانترنت وبشكل يضمن ديمومتها وهو ما يعرف بتكنولوجيا الحوسبة السحابية.

تقدم هذه التكنولوجيا العديد من الفوائد إلا أنها قد تزيد من حجم المخاطر على الشركات، مثل المخاطر الإستراتيجية، ومخاطر السمعة، ومخاطر الامتثال، والمخاطر التشغيلية التي تنشأ عن عجز الأطراف الخارجية عن تقديم الخدمة على المستوى المتفق عليه، أو حدوث اختراقات أمنية مما يستدعي من الشركات تبني إطار سليم وسريع الإستجابة لإدارة هذه المخاطر والإستفادة بأكبر قدر ممكن من هذه التكنولوجيا.

يتناول هذا الدليل توضيح لمفهوم تكنولوجيا الحوسبة السحابية والخصائص الأساسية لها ونماذج النشر ونماذج الخدمة المتعلقة بها وارشادات حول بعض القضايا الهامة والواجب على المؤسسات النظر فيها بعناية عند استخدامها لهذه التكنولوجيا ومنها حوكمة الحوسبة السحابية وإدارة مخاطرها واستمرارية اعمالها والضوابط والآليات المستخدمة لحماية بياناتها لاستخدامها بشكل آمن وفعال.

كما تضمن هذا الدليل ملحق خاص بالتعليمات والتعاميم الصادرة عن البنك المركزي الأردني والمتعلقة بعمليات الإسناد الخارجي في ضوء وجوب الالتزام التام بهذه التعليمات والتعاميم من قبل البنوك المرخصة والعاملة في المملكة كون أن تكنولوجيا الحوسبة السحابية تقع ضمن عمليات الاسناد الخارجي للتسهيل على البنوك الرجوع إليها.

النطاق والأهداف

في ضوء سعي البنك المركزي الأردني في مواكبة الممارسات الدولية الفضلى التي تعكس بأثرها الإيجابي على مكونات النظام المالي الأردني وصولاً إلى تحقيق الاستقرار المالي وتعزيز متانة القطاع المالي والمصرفي في تقديم أعماله واتاحة خدماته بشكل آمن وكفؤ وفعال؛ يأتي هذا الدليل الإرشادي لتنظيم استخدام تكنولوجيا الحوسبة السحابية من قبل البنوك والمؤسسات المالية وشركات الصرافة وشركات التمويل الأصغر وشركات المعلومات الائتمانية الخاضعة لإشراف ورقابة البنك المركزي الأردني بما يحقق أهدافها ضمن مستوى مناسب من الأمن والحماية ومساعدتها في فهم تكنولوجيا الحوسبة السحابية ومخاطرها لاستخدامها بشكل آمن وفعال.

المصطلحات

يكون للكلمات والعبارات التالية حيثما وردت في هذا الدليل المعاني المخصصة لها أدناه وتعتمد التعاريف الواردة في قانون البنك المركزي وقانون المعاملات الإلكترونية وقانون البنوك وأية تعليمات أخرى ذات العلاقة صادرة عن البنك المركزي حيثما ورد النص عليها في هذا الدليل ما لم تدل القرينة على غير ذلك:

الشركة	:	البنك أو البنك الإسلامي أو المؤسسة المالية أو شركة الصرافة أو شركة المعلومات الائتمانية أو شركة التمويل الأصغر.
الإدارة التنفيذية العليا	:	تشمل مدير عام الشركة أو المدير الإقليمي ونائب المدير العام أو نائب المدير الإقليمي ومساعد المدير العام أو مساعد المدير الإقليمي والمدير المالي ومدير العمليات ومدير إدارة المخاطر ومدير الخزينة (الاستثمار) ومدير الامتثال بالإضافة لأي موظف في الشركة له سلطة تنفيذية موازية لأي من سلطات أي من المذكورين ويرتبط وظيفياً مباشرةً بالمدير العام.
العميل (Customer)	:	كل شخص طبيعي أو اعتباري يحصل على خدمات مالية من الشركة.
مستخدم السحابة (Cloud Consumer)	:	الجهة التي تطلب وتستخدم المصادر والخدمات المتوفرة على السحابة.
مزود السحابة (Cloud Provider)	:	الجهة التي توفر مصادر و خدمات السحابة والأنشطة اللازمة لتوفير هذه الخدمات وضمان ايصالها إلى مستخدم السحابة.
تكنولوجيا الحوسبة السحابية (Cloud Computing Technology)	:	نموذج لتمكين الوصول الشبكي من أي مكان وبشكل مناسب وعند الطلب إلى مجموعة مشتركة من مصادر الحوسبة القابلة للإعداد (مثل الشبكات والخوادم ووسائط التخزين والتطبيقات والخدمات) لدى مزود السحابة.
البنية التحتية للسحابة (Cloud Infrastructure)	:	مجموعة من المكونات المادية والبرمجيات مثل الخوادم ووسائط التخزين والشبكات وبرامج المحاكاة الافتراضية اللازمة لدعم متطلبات الحوسبة السحابية.

اتفاقية مستوى الخدمة السحابية (Cloud Service Level Agreement)	:	اتفاقية تعاقدية بين مزود السحابة والشركة يتم فيها تحديد متطلبات الشركة ومستوى الخدمة والضمانات التي يقدمها مزود السحابة بشأن توافرية الخدمات وأداءها ومستويات الدعم لها.
تقييم المخاطر (Risk Assessment)	:	قياس وتحديد احتمالية حدوث المخاطر وشدتها وتوقع مقدار تأثيرها على الشركة.
إدارة التغيير (Change Management)	:	إدارة وضبط وتوثيق أي تغيير يتم إجراؤه على أي من الخدمات المسندة لمزود السحابة.
ضوابط الوصول/النفاذ (Access Control)	:	القواعد والآليات المستخدمة للسماح باستخدام ونفاذ الأشخاص المخولين فقط إلى أصول المعلومات وبما يتوافق وطبيعة مسؤولياتهم.
تصنيف المعلومات (Information Classification)	:	تحديد مستوى الحساسية المناسب للمعلومات التي يتم إنشاؤها أو تغييرها أو نقلها أو تعديلها أو حفظها على أية وسائل كانت وبأية تقنيات ممكنة، اعتماداً على المخاطر المترتبة عن الاطلاع والاستخدام غير المشروع لتلك المعلومات.
التعافي (Recovery)	:	مجموعة الاجراءات التي يتم اتخاذها واتباعها لإعادة الأعمال في الشركة الى وضعها الطبيعي وإعادة تشغيل موارد التكنولوجيا المعتمد عليها في تشغيل عمليات الشركة إلى ما كانت عليه قبل وقوع الحدث.
عمليات المسح (Vulnerability Scanning)	:	آلية تستخدم لتحديد خصائص الانظمة و نقاط الضعف المرتبطة بها.
اختبارات الاختراق (Penetration Testing)	:	اختبار يحاول فيها المقيمون المختصون بالبحث عن الثغرات الامنية والتحايل على الخصائص الأمنية لأنظمة المعلومات والضوابط الامنية واستغلالها لمحاولة اختراق تلك الانظمة من خارج او داخل الشركة لمعرفة مدى فعالية الضوابط الأمنية المستخدمة من قبل الشركة لحماية أنظمتها.

زمن التعافي المستهدف (RTO)	اقصى وقت مسموح به لإعادة تشغيل الخدمة أو العملية بعد حدوث الانقطاع للخدمة.
نقطة الاسترجاع المستهدفة (RPO)	العمر الأقصى المسموح للبيانات التي قد تفقد عند استعادة الخدمة بعد حدوث انقطاع.

الفصل الأول: تكنولوجيا الحوسبة السحابية

1.1 تمهيد

تعتبر تكنولوجيا الحوسبة السحابية نموذج لتمكين الوصول الشبكي من أي مكان وبشكل مناسب وعند الطلب إلى مجموعة مشتركة من المصادر المادية (Physical Resources) أو الإفتراضية (Virtual Resources) مثل الشبكات والخوادم ووسائط التخزين والتطبيقات والخدمات التي يمكن توفيرها بسرعة واستخدامها بأقل جهد. ويتكون هذا النموذج من خمس خصائص أساسية (Essential Characteristics)، وثلاثة نماذج خدمة (Service Models)، وأربعة نماذج للنشر (Deployment Models).

1.2 الخصائص الأساسية (Essential Characteristics)

- **خدمة ذاتية بناء على الطلب (On-Demand Self-Service)**: خاصية تمكن مستخدم السحابة من طلب خدمات تخزين ومعالجة حسب الحاجة وتلقائياً بهدف التقليل من الحاجة الى التفاعل المباشر مع مزود السحابة.
- **وصول واسع الى الشبكة (Broad Network Access)**: يتضمن الوصول الشبكي من أي مكان إلى مصادر مزود السحابة عن طريق منصات الشركة مثل: الهواتف الجوالة والأجهزة اللوحية وأجهزة الحاسوب المحمولة ومحطات العمل.
- **تجميع المصادر (Resource Pooling)**: يتم تجميع مصادر الحوسبة المختلفة من قبل مزود السحابة لخدمة العديد من مستخدمي السحابة باستخدام نموذج (Multi-tenant model) مع تخصيص مصادر مادية وافتراضية مختلفة بشكل ديناميكي وإعادة تخصيصها وفقاً لطلب مستخدم السحابة دون الحاجة لسيطرة مستخدم السحابة أو معرفته للموقع المحدد للمصادر الموفرة له من قبل مزود السحابة مع الاحتفاظ بحقه في تحديد الموقع على مستوى معين (على سبيل المثال البلد أو مركز البيانات).
- **مرونة سريعة (Rapid Elasticity)**: يمكن توفير الإمكانات وقدرات المعالجة على السحابة بشكل مرن وتلقائي وامكانية ضبط حجم المصادر المستخدمة بما يتناسب مع حجم العمل المطلوب من قبل مستخدم السحابة حيث تكون القدرات المتاحة غير محدودة ويمكن تخصيصها في أي وقت من خلال العقود المبرمة بين مستخدم ومزود السحابة.

- **الخدمة المقاسة (Measured Service)**: يمكن التحكم تلقائياً في استخدام مصادر السحابة وتحسين ومراقبة استخدامها وتدقيقها وعمل تقارير بخصوص ذلك، وبالتالي توفير الشفافية لكل من مزود ومستخدم السحابة على أن يتحمل المستخدم التكلفة حسب المصادر المطلوبة.

1.3 نماذج الخدمة (Service Models)

- **البرمجيات كخدمة Software as a Service (SaaS)**: نموذج لتوزيع البرامج وإتاحتها لمستخدم السحابة عبر الشبكة بحيث تكون التطبيقات مستضافة من قبل مزود السحابة دون الحاجة إلى تنصيب أو تشغيل التطبيقات على أجهزة المستخدم حيث يتمكن من استخدام التطبيقات التي تعمل على البنية التحتية الخاصة بالمزود ويمكن للمستخدم الوصول إلى تلك التطبيقات من خلال أجهزة مختلفة وعن طريق واجهة معينة مثل واجهة متصفح الويب أو البرنامج، وعمل اعدادات محدودة على تلك التطبيقات دون أن يقوم مستخدم السحابة بإدارة أو التحكم في البنية التحتية للسحابة.
- **المنصة كخدمة Platform as a Service (PaaS):** تقدم المنصة بيئة حوسبة متكاملة بما في ذلك نظام التشغيل وبيئة تنفيذ لغات البرمجة وقواعد البيانات وخوادم الويب لتمكين مستخدم السحابة من تطوير وتشغيل التطبيقات الخاصة به ونشر تطبيقاته على البنية التحتية للسحابة والتحكم بإعداداتها دون أن يقوم المستخدم بإدارة أو التحكم في البنية التحتية للسحابة.
- **البنية التحتية كخدمة Infrastructure as a Service (IaaS):** يتم توفير أجهزة الحاسوب المادية أو الافتراضية والمصادر الأخرى مثل الشبكات ووسائط التخزين من قبل مزود السحابة لدعم العمليات الخاصة بمستخدم السحابة حيث يكون المستخدم قادر على نشر وتشغيل بعض البرامج مثل أنظمة التشغيل والتطبيقات، ولا يقوم المستخدم بإدارة أو التحكم في البنية التحتية للسحابة، ولكن يمكنه التحكم في أنظمة التشغيل والتخزين والتطبيقات المنشورة، وربما سيطرة محدودة على بعض مكونات الشبكات (مثل الجدران النارية).

1.4 نماذج النشر (Deployment Models)

- **السحابة العامة (Public Cloud):** يتم توفير البنية التحتية للسحابة للاستخدام المفتوح العام وقد تكون مملوكة أو تدار أو تشغل من قبل مؤسسة تجارية أو أكاديمية أو حكومية أو مجموعة منها وتكون البنية التحتية للسحابة موجودة في مقر تابع لمزود السحابة. ومن الممكن أن تخزن البيانات التابعة

لمستخدم السحابة في مواقع غير معروفة له ومن الممكن ألا يتم استرجاعها بسهولة وقد تخزن البيانات الخاصة بمستخدم السحابة مع بيانات مستخدم آخر على نفس السحابة.

- **السحابة المجتمعية (Community Cloud):** يتم توفير البنية التحتية للسحابة للاستخدام الحصري من قبل مجتمع معين من مستخدمي السحابة من الشركات التي تتشارك بنفس الاهتمامات مثل مهماتها ومتطلباتها الأمنية وسياساتها واعتبارات الامتثال لديها. وقد تكون مملوكة أو تدار أو تشغل من قبل واحدة أو أكثر من الشركات في ذلك المجتمع أو طرف ثالث أو مزيج منها، وهي أكثر تكلفة من السحابة العامة حيث يتم توزيع التكلفة على عدد من مستخدمي السحابة مقابل مستوى أعلى من الالتزام والخصوصية والأمن وقد تكون موجودة داخل أو خارج مواقع تلك الشركات، وقد تخزن البيانات الخاصة بكل شركة مع البيانات الخاصة بمنافسيها على نفس السحابة المجتمعية.
- **السحابة الخاصة (Private Cloud):** يتم توفير البنية التحتية للسحابة للاستخدام الحصري من قبل مجموعة من مستخدمي السحابة قد تكون مملوكة أو تدار أو تشغلها المجموعة أو طرف ثالث أو كلاهما. وقد تكون البنية التحتية للسحابة داخل مقر المجموعة (On-premises) أو خارج مقر المجموعة (Off-premises)، وتعتبر السحابة الخاصة من اقل نماذج النشر خطورة الا أن الخدمات المقدمة من خلالها قد لا تكون مرنة كما هي في السحابة العامة.
- **السحابة الهجينة (Hybrid Cloud):** تتكون البنية التحتية للسحابة من اثنين أو أكثر من نماذج النشر سواء كانت السحابة خاصة أو مجتمعية أو عامة وتعتبر كيان مستقل ولكنها مرتبطة معاً بتقنية موحدة تمكن البيانات والتطبيقات من الانتقال فيما بينها، وقد ينشأ عن ذلك مخاطر بسبب دمج أكثر من نموذج للنشر وهنا يقع على عاتق مستخدم السحابة مسؤولية تصنيف المعلومات ليتم تخزينها على نموذج النشر الخاص بها، ويبين الجدول رقم (1) ادناه مقارنة بين نماذج النشر المختلفة.

جدول 1: مقارنة بين نماذج النشر المختلفة

نموذج النشر	مدير البنية التحتية للسحابة	مالك البنية التحتية للسحابة	موقع البنية التحتية للسحابة	يمكن الوصول إليها واستخدامها من قبل
العامة (Public)	مزود السحابة	مزود السحابة	خارج مقر مستخدم السحابة	أي مستخدم للسحابة
الخاصة (Private) / المجتمعية (Community)	مستخدم أو مزود السحابة	مستخدم أو مزود السحابة	خارج أو داخل مقر مستخدم السحابة	جهات موثوقة
الهجينة (Hybrid)	مستخدم و مزود السحابة	مستخدم و مزود السحابة	خارج و/أو داخل مقر مستخدم السحابة	جهات موثوقة وغير موثوقة

1.5 الجهات الفعالة في السحابة (Cloud Actors)

تتمثل الجهات التي تتشارك في العمليات و/أو المهام المتعلقة بالحوسبة السحابية سواء كانت شركات أو اشخاص بشكل فعال في السحابة بما يلي:

1. **مستخدم السحابة (Cloud Consumer)**
2. **مزود السحابة (Cloud Provider)**
3. **وسيط السحابة (Cloud Broker):** يعمل كوسيط بين مستخدم ومزود السحابة ويساعد مستخدمي السحابة في اختيار وادارة خدمات الحوسبة السحابية المختلفة والمقدمة من قبل المزود بالإضافة الى توفير خدمات اضافية للمستخدم. وتشمل الخدمات المقدمة من خلال وسيط السحابة ما يلي:

- **الوساطة (Intermediation):** يقوم الوسيط على تعزيز خدمة معينة من خلال تحسينها وتوفير خدمات ذات قيمة مضافة للمستخدمين، ويمكن أن يكون التحسين متمثل بإدارة الوصول إلى خدمات الحوسبة السحابية، وإدارة الهوية، وتعزيز الأمن، وما إلى ذلك.

- **التجميع (Aggregation):** يقوم الوسيط على جمع ودمج خدمات متعددة في خدمة واحدة أو أكثر من الخدمات الجديدة وتوفيرها لمستخدم السحابة، كما يوفر الوسيط البيانات وتكامل الخدمات ويضمن حركة البيانات الآمنة بين مستخدم ومزودي السحابة.
- **الموازنة (Arbitrage):** تشبه خدمة التجميع إلا أن الخدمات المجمعة ليست ثابتة حيث أن الوسيط لديه المرونة في اختيار الخدمات من أكثر من مزود للسحابة.

4. **مدقق السحابة (Cloud Auditor):** يقوم مدقق السحابة بمراقبة أداء الخدمات السحابية والضوابط الأمنية التي تنفذ على السحابة للتحقق من الامتثال للسياسات الأمنية الخاصة بالحوسبة السحابية.
5. **ناقل السحابة (Cloud Carrier):** يقوم ناقل السحابة بنقل الخدمات السحابية والبيانات بين مستخدمي ومزودي السحابة على أن يتحمل مزود السحابة مسؤولية إعداد اتفاقية مستوى الخدمة السحابية مع ناقل السحابة لضمان ايصال البيانات والخدمات الى مستخدم السحابة ضمن المستوى المتفق عليه.

1.5.1 العلاقة بين الجهات الفعالة في الحوسبة السحابية

- يمكن لمستخدم السحابة طلب خدمات الحوسبة السحابية من مزود السحابة مباشرة أو عن طريق وسيط السحابة وفي حال تم التعامل مع وسيط السحابة فعلى مستخدم السحابة الأخذ بعين الاعتبار أن وسيط السحابة ينطبق عليه ما ينطبق على مزود السحابة في حال تم التعاقد معه.
- يقوم مدقق السحابة بإجراء عمليات تدقيق مستقلة عن الجهات الفعالة الأخرى وجمع المعلومات اللازمة لذلك.
- هناك أدوار محددة لكل من مزود ومستخدم السحابة عند استخدام نماذج الخدمة المختلفة كما هو مبين في الجدول رقم (2).

جدول 2: الأدوار المختلفة لكل من مزود ومستخدم السحابة عند استخدام نماذج الخدمة الثلاث

نموذج الخدمة	أنشطة مستخدم السحابة (Cloud Consumer Activities)	أنشطة مزود السحابة (Cloud Provider Activities)
البرمجيات كخدمة (SaaS)	استخدام التطبيقات المتوفرة على السحابة لإجراء العمليات الخاصة بنطاق عمله.	يثبت ويدير ويحافظ على ويدعم التطبيقات المتوفرة لديه والخاصة بمستخدم السحابة على البنية التحتية للسحابة لديه.
المنصة كخدمة (PaaS)	تطوير واختبار ونشر وادارة التطبيقات المستضافة على منصة السحابة.	تخصيص وإدارة البنية التحتية للسحابة وتوفير أدوات التطوير والنشر والإدارة لمستخدمي السحابة.
البنية التحتية كخدمة (IaaS)	• إنشاء/تثبيت وإدارة ومراقبة خدمات البنية التحتية للسحابة الخاصة به. • التحكم في الأجهزة الافتراضية (Virtual Machines) التي يتم استخدامها على السحابة من حيث أنظمة التشغيل والتخزين والتطبيقات التي تم نشرها على مستوى تلك الأجهزة.	تقديم وإدارة المعالجة المادية والتخزين والشبكات وبيئة الاستضافة والبنية التحتية للسحابة لمستخدمي السحابة.

الفصل الثاني: إرشادات حول استخدام تكنولوجيا الحوسبة السحابية

2.1 تمهيد

في هذا الفصل تم وضع ارشادات حول حوكمة الحوسبة السحابية وسياسة الشركة (مستخدم السحابة) في استخدام تكنولوجيا الحوسبة السحابية والعقود والاتفاقيات المبرمة بين الشركة ومزود السحابة وحماية أمن البيانات وإدارة المخاطر وإدارة التغيير وقياس أداء مزود السحابة والإشراف عليه بالاضافة إلى مراقبة السجلات والأحداث الأمنية وإدارة الوصول واستمرارية العمل وخطط الانهاء المتعلقة بترتيبات الاستعانة بمزود السحابة، وذلك بهدف حماية الشركات من المخاطر التي قد تتعرض لها عند استخدام تكنولوجيا الحوسبة السحابية.

2.2 حوكمة الحوسبة السحابية

تعد الحوكمة الفعالة عند استخدام تكنولوجيا الحوسبة السحابية ضرورية لتوجيه عمليات الإدارة واتخاذ القرارات للاستفادة من خدمات الحوسبة السحابية وفقاً لاحتياجات الشركة وبالشكل الأمثل. وينبغي أن تكون استراتيجية حوكمة الحوسبة السحابية في الشركة واضحة لمزود السحابة لتمكين التعاون فيما بينهم من حيث الأداء التشغيلي وحل المشاكل ومشاركة القرارات فيما يخص إدارة المخاطر المرتبطة بالخدمات المسندة إلى مزود السحابة حيث يتم تحديد مهام ومسؤوليات المجلس والإدارة التنفيذية العليا مع الأخذ بعين الإعتبار ما يلي:

- أن يتولى المجلس أو من يفوض من لجانه اعتماد سياسة الحوسبة السحابية للشركة ومتابعة تطبيقها.
- أن تتولى الإدارة التنفيذية العليا المسؤوليات والمهام التالية كل بحسب موقعه:
  - وضع هيكل فعال للحوكمة وعمليات إدارة مخاطر الاستعانة بخدمات الحوسبة السحابية بشكل سليم.
  - ضمان وضع سياسة الحوسبة السحابية والإشراف على تنفيذها ومراجعتها وتحديثها بشكل دوري وكلما دعت الحاجة الى ذلك.
  - الموافقة على الاتفاقيات المبرمة بين الشركة ومزود السحابة.
  - التأكد من إجراء التقييم والعناية الواجبة لمزودي السحابة قبل الدخول في أي اتفاق معهم.
  - مراجعة نتائج تقييم المخاطر لجميع اتفاقيات الاستعانة بخدمات الحوسبة السحابية استناداً إلى إطار تقييم المخاطر الذي يقره مجلس الإدارة.

- مراجعة تقارير التقييم الدوري لأداء مزود السحابة.
- ضمان وضع خطط للتعافي من الكوارث استناداً إلى سيناريوهات التعطل والاختراق والأعمال التخريبية الواقعية والمحتملة، واختبارها بشكل دوري.
- ضمان وجود آلية مناسبة للمراقبة المستمرة لمزود السحابة وفقا لشروط وأحكام اتفاقية مستوى الخدمة السحابية بين الشركة ومزود السحابة.
- التأكد من قيام الجهات المعنية في الشركة بمراجعة جميع الأنشطة والخدمات المسندة لمزود السحابة وإخطار مجلس الإدارة بانتظام عن المخاطر التي قد تنشأ عن ذلك.

2.3 سياسة الحوسبة السحابية

ينبغي على الشركة وضع سياسة للحوسبة السحابية ومراجعتها وتحديثها بشكل دوري على أن تتضمن بالحد الأدنى ما يلي:

- الخدمات والعمليات والبيانات المراد إسنادها إلى مزود السحابة وتصنيفها حسب أهميتها ودرجة حساسيتها لتكون مرجع يتم الإستناد إليه عند الاستعانة بخدمات الحوسبة السحابية وتتحمل الشركة مسؤولية تصنيفها.
- نموذج النشر الأنسب (سحابة عامة، خاصة، مجتمعية، هجينة) ونموذج الخدمة الأنسب (IaaS, SaaS, PaaS) للخدمات والعمليات المراد إسنادها بالاعتماد على:
  - نوع الخدمة وتصنيف المعلومات والعمليات المراد إسنادها لمزود السحابة.
  - تقييم مستوى المخاطر المتعلق بها.
- آلية حفظ البيانات الخاصة بالشركة وأماكن تخزينها وآلية التخلص منها ومعالجتها وتناقلها مع أنظمة مزود السحابة.
- الضوابط الأمنية الواجب اتباعها عند التعامل مع أي مزود سحابة.
- أسس التقييم والعناية الواجبة لمزودي السحابة قبل الدخول في أي اتفاق معهم.
- المتطلبات والنتائج المتوقعة من الاستعانة بمزودي السحابة في أداء العمليات بما يتوافق مع المتطلبات والتغيرات في بيئة العمل.
- العلاقة بين العمليات الداخلية للشركة والعمليات المراد نقلها إلى أنظمة مزود السحابة.
- آلية لضمان التوافق والترابط بين الخدمات المختلفة والمسندة لأكثر من مزود سحابة.

- ضوابط لحماية بيانات العملاء والإفصاح للعميل في حال تم إسناد أي بيانات شخصية خاصة به إلى مزود السحابة وذلك بما يتوافق مع القوانين والتعليمات ذات العلاقة.
- الحدود الدنيا من الشروط الواجب توافرها في الاتفاقيات المبرمة مع مزود السحابة.
- آليات الرقابة والتدقيق للخدمات المسندة لمزود السحابة.

2.4 إدارة المخاطر

على الشركة تحديد وإدارة أي مخاطر قد تنتج عن الاستعانة بخدمات الحوسبة السحابية مع الأخذ بعين الاعتبار ما يلي:

- تضمين مخاطر الاستعانة بخدمات الحوسبة السحابية ضمن إطار تقييم المخاطر الشامل للشركة وتوثيقه وتحديثه باستمرار على أن يتضمن بالحد الأدنى ما يلي:
  - تحديد دور مزود السحابة في استراتيجية عمل الشركة.
  - وضع إجراءات شاملة لتغطية متطلبات الربط مع مزود السحابة لتحديد وتخفيف المخاطر الأساسية.
  - تقييم قدرة مزود السحابة على توظيف معايير عالية لأداء الخدمة بما يضمن تقديم الخدمة بكفاءة عالية.
  - تحليل تأثير الاستعانة بخدمات الحوسبة السحابية على ملف المخاطر الشامل للشركة.
  - تقييم الاعتبارات الخاصة بالقوانين السارية وأحكام إنفاذ القانون بالإضافة إلى الاستقرار السياسي والأمني لبلد مزود السحابة بما في ذلك القوانين المتعلقة بحماية البيانات.
  - تحديد المخاطر المالية والتشغيلية والقانونية على الشركة وسمعتها في حال فشل مزود السحابة بأداء العمليات على النحو المطلوب.
  - تقييم المخاطر الأمنية الشاملة المرتبطة بالخدمة المسندة لمزود السحابة وتحديد دور ومسؤولية الشركة ومزود السحابة في إدارتها وتحديد الخطوات اللازم اتباعها للتخفيف منها وتوثيق هذا التقييم.
- وضع معايير أداء رئيسية لمراقبة مستوى المخاطر المتعلقة بالاستعانة بخدمات الحوسبة السحابية (Key Risk Indicators) للتأكد من عدم تجاوز المخاطر المقبولة (Risk Appetite) ودرجة تحمل المخاطر.

- تحديد أفضل الممارسات الحالية في استخدام تكنولوجيا الحوسبة السحابية، بما في ذلك متطلبات إدارة أمن المعلومات، والمخاطر السيبرانية، والقواعد التنظيمية ذات الصلة.
- مراقبة المخاطر وتحديد الإجراءات التي قد تتخذ في حال فشل مزود السحابة في تقديم الخدمات على المستوى المتفق عليه.
- تحديد الأثر على عملاء الشركة في حال فشل مزود السحابة في أداء الخدمة أو انتهاك سرية بياناتهم.
- إدارة المخاطر الأمنية المرتبطة بتخزين البيانات وتشغيل التطبيقات الخاصة بالشركة على أنظمة مزود السحابة.
- مراقبة مخاطر التركز الناشئة عن الاعتماد على مزود سحابة واحد لجميع الخدمات المنوي إسنادها لمزود السحابة والنظر في الإجراءات التي ستتخذ في حال فشل المزود بأداء العمليات على النحو المطلوب.

2.5 العقود والاتفاقيات بين الشركة ومزود السحابة

ينبغي على الشركة التأكد من أن العقد/العقود المبرمة بينها وبين مزود السحابة تتسق مع سياسة الحوسبة السحابية المعتمدة لدى الشركة مع الأخذ بعين الاعتبار أن تتضمن العقود بالحد الأدنى ما يلي:

- اسم مزود السحابة واسم الشركة الأم له - إن وجدت - وعنوان عمله وكامل معلومات الاتصال الخاصة به.
- الأنشطة والخدمات المراد اسنادها للمزود.
- مدة العقد.
- التزام مزود السحابة بسرية وخصوصية وأمن بيانات الشركة.
- التزام مزود السحابة بخطط استمرارية الأعمال لدى الشركة.
- إجراءات التدقيق والرقابة على مزود السحابة.
- معايير الأداء والتشغيل والتحكم الداخلي وإدارة المخاطر.
- اتفاقية مستوى الخدمة السحابية ومتطلبات أداء مزود السحابة.
- الادوار والمسؤوليات لكلا الطرفين.
- اجراءات تسوية وحل النزاعات.

- آلية رفع التقارير للشركة.
- القانون المطبق الذي يحكم العقد.
- الترتيبات القانونية والتنظيمية الواجب على مزود السحابة الالتزام بها.
- متطلبات ومسؤوليات الدعم الفني والصيانة.
- الشروط الجزائية في حال فشل مزود السحابة في تقديم خدمات الحوسبة السحابية.
- أن يسمح العقد بالتجديد والتفاوض لتمكين الشركة من الاحتفاظ بمستوى مناسب من الرقابة على ترتيبات الاستعانة بمزود السحابة.
- الحفاظ على سرية وأمن المعلومات وملكية بيانات الشركة واتخاذ الإجراءات اللازمة لمنع اطلاع أو وصول أي شخص أو أي جهة أخرى على البيانات دون أخذ الموافقة المسبقة على ذلك.
- التزام مزود السحابة بإبلاغ الشركة عن أي تغييرات مهمة مقترحة على العقود أو الخدمات المتعاقد عليها التي قد تؤثر على قدرة المزود على الوفاء بمسؤولياته وأخذ موافقة الشركة عليها. وأن يتم الاتفاق مسبقاً على فترة الابلاغ عن هذه التغييرات للسماح للشركة بإجراء تقييم للمخاطر للنظر في آثار التغييرات المقترحة قبل اجراء التغيير الفعلي وعمل اختبار لهذه التغييرات.
- تحديد الموقع الجغرافي لأماكن حفظ بيانات الشركة وأخذ موافقة الشركة عند قيام مزود السحابة بتغيير أماكن العمل أو مراكز البيانات والعمليات الخاصة بالخدمات المسندة الى السحابة.
- الاتفاق على المتطلبات الأمنية والتشغيلية لضمان كفاية وفعالية السياسات والممارسات الأمنية، بما في ذلك الظروف القائمة التي يحق لكل طرف فيها تغيير تلك المتطلبات.
- إلزام مزود السحابة بالتعاون مع أي طرف ثالث تتعاقد معه الشركة إذا كان نطاق عمل هذا الطرف يتقاطع مع نطاق الخدمات المسندة للمزود.
- في حال تعاقد المزود مع طرف ثالث فيما يتعلق بالخدمة المسندة للمزود يجب ابلاغ الشركة فوراً وطلب موافقتها وإبقاء المزود مسؤولاً عن تقديمه للخدمة، وفعالية الضوابط المتفق عليها في العقد المبرم بينهما بما في ذلك المتطلبات الأمنية والتشغيلية.
- تحديد آليات الإبلاغ والتراسل وإجراءات التصعيد المعتمدة وضمان وجود إشعارات فورية من قبل مزود السحابة للشركة عن أي مخالفات أو أحداث أخرى ناشئة عن أي خلل في خدمات الحوسبة السحابية والإجراءات المتخذة و/أوالمقترحة من المزود لمعالجة الخلل.

- بنود تتيح للبنك المركزي القيام بمهامه الإشرافية وتلزم مزود السحابة بأي متطلبات وتعاميم وتعليمات صادرة عن البنك المركزي تتعلق بالخدمات المسندة الى المزود.
- ينبغي أن ينص العقد بوضوح على الحالات التي يكون فيها للطرفين الحق في إنهاء العقد، ومن الحالات التي يحق للشركة إنهاء العقد فيها على سبيل المثال لا الحصر:
  - حدوث خرق للأمن أو السرية.
  - عدم قيام مزود السحابة بإخطار الشركة عن الأحداث الأمنية التي قد تؤثر على عمل الشركة.
  - عدم قدرة مزود السحابة على أداء الخدمة المتعاقد عليها ضمن المستوى المتفق عليه.
  - تغيير الملكية لمزود السحابة.
  - اعسار مزود السحابة ودخوله في التصفية.
  - خضوع مزود السحابة للحجز القضائي سواء في البلد أو في مكان آخر.
- عدم وضع أي قيود أوعقبات في العقد قد تعرقل الإنهاء الفوري للعقد في حال رغبة الشركة بذلك.

2.5.1 اتفاقية مستوى الخدمة السحابية (Cloud Service Level Agreement)

تعتبر اتفاقيات مستوى الخدمة السحابية بين الشركة ومزود السحابة من أهم العناصر في إدارة خدمة الحوسبة السحابية حيث أن الطبيعة المعقدة والمتغيرة لتكنولوجيا الحوسبة السحابية تستلزم وسائل متطورة لإدارة اتفاقيات مستوى الخدمة لضمان جودة الخدمة المتفق عليها بين الشركة والمزود، حيث تحتاج الشركة إلى اتفاقية مستوى الخدمة السحابية لتحديد متطلبات أداء للخدمات السحابية، وتحتوي هذه الاتفاقيات بالحد الأدنى ما يلي:

- نوعية الخدمة ومستوى أداءها وضوابط الأمن المطلوبة.
- مستوى توافرية الخدمة المسندة للمزود وتكامليتها وسريتها وضوابط الوصول المطبقة عليها.
- آلية فصل بيانات المزود عن بيانات الشركة والبيانات المرتبطة بالخدمة المسندة للمزود.
- آلية حفظ ومعالجة البيانات الخاصة بالشركة وعملائها.
- آلية النسخ الاحتياطي والاحتفاظ بالسجلات.
- آلية التعافي من الكوارث وخطط الطوارئ.
- تفاصيل البنية التحتية والمعايير الأمنية التي يتعين الحفاظ عليها من قبل المزود ومراجعة الامتثال لها.
- الفحص الدوري لمزود السحابة للتأكد من امتثاله لمستوى أداء الخدمة والمعايير الأمنية المتفق عليها.

2.6 الإشراف على مزود السحابة

إسناد الشركة بعض خدماتها لمزود السحابة لا يعني نقل الشركة مسؤوليتها للمزود بل تتحمل الشركة المسؤولية الكاملة عن الخدمة المسندة للمزود بموجب التشريعات النافذة والتعليمات الصادرة عن البنك المركزي، وعليه ينبغي على الشركة القيام بما يلي:

- إعلام البنك المركزي عند التعاقد مع أي مزود للسحابة.
- تحديد مهام الإشراف والرقابة المستمرة من قبل الشركة على الخدمة وضمان حصول موظفي الشركة على ما يكفي من التدريب والمهارات والموارد للإشراف على هذه الخدمات واختبارها.
- الحق في اجراء زيارة ميدانية إلى مقر عمل المزود ولا ينبغي تقييد هذا الحق، وذلك حسب الاتفاق المسبق بين الطرفين.
- وضع اجراءات تتيح للبنك المركزي القيام بمهامه الإشرافية بما في ذلك:
  - ضمان أن تكون جميع بيانات الشركة وخدمات الحوسبة السحابية متاحة للمراجعة أو التفتيش من قبل البنك المركزي وفي أي وقت.
  - الحصول على أي سجلات أو وثائق أو بيانات أو معلومات يراها البنك المركزي ضرورية والمتعلقة بأعمال الشركة التي تم إسنادها الى مزود السحابة.
  - الوصول إلى أي تقرير أو نتائج تدقيق تم عملها من قبل مدققين خارجيين أو داخليين يتم تعيينهم من قِبل الشركة أو مزود السحابة ذات علاقة بالخدمة المسندة.

2.7 أمن البيانات

إن الحفاظ على أمن البيانات من أهم القضايا التي يجب على الشركة ضمانها عند الإستعانة بمزود السحابة نظراً للطبيعة الموزعة لبيئة الحوسبة السحابية لذا يجب الأخذ بعين الإعتبار الإجراءات والضوابط الواجب اتباعها لحماية البيانات عند نقلها ومعالجتها وتخزينها واتلافها وعليه ينبغي على الشركة القيام بما يلي:

- التأكد من توفر متطلبات الحماية الفيزيائية لمراكز البيانات التابعة لمزود السحابة.
- اعتماد تصنيف محدد للبيانات وذلك حسب حساسيتها حيث ان الشركة ملزمة بتحمل مسؤولية تصنيفها للبيانات مع ضرورة قيامهم بإجراء مراجعة دورية لهذا التصنيف.

- تحديد البيانات التي سيتم نقلها للسحابة بالإستناد الى تصنيف المعلومات المعتمد لدى الشركة مع الأخذ بعين الاعتبار المخاطر المترتبة على وضع البيانات المصنفة كحساسة على السحابة العامة أو الهجينة.
- التأكد من تزويد الشركة بما يفيد فصل البيانات الخاصة بالشركة عن بيانات مستخدم سحابة آخر أو بيانات المزود.
- تحديد الجهة المسؤولة عن أخذ نسخ احتياطية من البيانات وآلية وأماكن تخزينها.
- اتخاذ الخطوات المناسبة للتخفيف من المخاطر الأمنية المترتبة على نقل البيانات على السحابة.
- تحديد طبيعة ونطاق المخاطر الناتجة عن فقدان البيانات الخاصة بالشركة والتقليل من تلك المخاطر من خلال:
    - توزيع البيانات والتطبيقات في أماكن متعددة.
    - الالتزام بأفضل الممارسات في استمرارية الأعمال والتعافي من الكوارث.
- أن تخضع البيانات (سواء المخزنة أو المتناقلة) والنسخ الاحتياطية من هذه البيانات وخاصة الحساسة منها إلى ضوابط التشفير المناسبة ومنها ما يلي:
    - وضع سياسات وإجراءات مفصلة لتنظيم مفاتيح التشفير من حيث انشائها وتخزينها واستخدامها وايقافها وانتهاء صلاحيتها وتجديدها وأرشفتها ومراجعتها بشكل دوري.
    - مراجعة التفاصيل المتعلقة بخوارزميات التشفير وطول مفاتيح التشفير وتدفقات البيانات على نحو ملائم من قبل متخصصين لتحديد نقاط الضعف المحتملة.
    - ضمان أن المفاتيح السرية المستخدمة في التشفير يتم إنشاؤها وإدارتها بشكل آمن، على سبيل المثال أجهزة HSM (Hardware Security Model).
    - التأكد من وجود الضوابط المناسبة لإدارة مفاتيح التشفير والشهادات الرقمية.
    - وضع تجهيزات أمنية كافية مثل وحدة أمن الأجهزة وغيرها من الأدوات المستخدمة للتشفير على شبكات آمنة منفصلة للتحكم في الوصول اليها بعناية بحيث لا يمكن الوصول إليها من الشبكات الفرعية (Subnets) التي قد تستخدمها شركات أخرى تتعامل مع مزود السحابة أو التي قد يستخدمها موظفي المزود.
    - أن تكون مفاتيح التشفير المستخدمة لتشفير بيانات الشركة فريدة ومخصصة فقط لبيانات الشركة وألا يتم استخدامها لبيانات شركات أخرى تتعامل مع المزود.

- في حال استخدام عملية الترميز(Tokenization) والتي تهدف الى تقليل كمية البيانات خاصة الحساسة منها والتي تقوم الشركة بمشاركتها مع مزود السحابة وضمان أن الأطراف المصرح لها فقط هي التي يمكنها الوصول الى بيانات الشركة عند الاستعانة بمزود السحابة ينبغي مراعاة ما يلي:
  - إجراء تقييم دقيق للمخاطر وخاصة المتعلقة بالحلول المستخدمة لعملية الترميز وتحديد الخصائص الفريدة المستخدمة للوصول إلى البيانات.
  - التأكد من عدم قدرة مزود السحابة على استرجاع البيانات التي تم ترميزها من خلال وصوله الى النظام الخاص بالترميز.
- إجراءات معالجة الانتهاكات وغيرها من الأحداث ذات التأثير السلبي على خدمات الحوسبة السحابية.
- إجراء اختبارات الاختراق (Pentration Tests) للأنظمة الخاصة بالخدمات المسندة الى مزود السحابة وبالأخص أنظمة التشغيل على البيئة الإفتراضية للسحابة بشكل دوري وبالتعاون مع المزود نظراً لتعرضها إلى الكثير من المخاطر بسبب تشارك مستخدمي السحابة للمكونات المادية.
- إجراء عمليات المسح (Vulnerability Scanning) بشكل دوري على الأنظمة والبرمجيات الخاصة بالخدمات المسندة لمزود السحابة للكشف عن نقاط الضعف ومعالجة الثغرات وبالتنسيق مع المزود بشكل استباقي لتجنب احتمال تعرض تلك الأنظمة للخطر.

2.8 إدارة الوصول

2.8.1 إدارة وصول المستخدم وفصل الواجبات

عندما يكون لدى مزود السحابة إمكانية الوصول إلى وإدارة الأنظمة أو البرمجيات الخاصة بالخدمة المسندة إليه، ينبغي على الشركة الأخذ بعين الإعتبار ما يلي:

- التأكد من تطبيق مزود السحابة لسياساتها المتبعة في إدارة الوصول.
- الفصل بين واجبات مستخدمي الأنظمة والبرمجيات خاصة للأدوار الحرجة والحساسة.
- تسجيل وصول المستخدمين إلى الأنظمة أو البرمجيات في سجلات الوصول التابعة لمزود السحابة ومراجعتها سنويا على الأقل.

- التحكم في الوصول إلى الخدمة والحسابات العامة وحسابات مديري الأنظمة التابعة للشركة والموجودة عند مزود السحابة من خلال وجود ضوابط إدارة وصول المستخدمين وخاصة ذوي الامتيازات العليا وتسجيل الأنشطة التي تتم على تلك الأنظمة لمراجعتها.
- ينبغي ألا يكون للمطورين التابعين لمزود السحابة أي حق في الوصول إلى البيئة الحية للشركة والموجودة على السحابة.

2.8.2 الوصول الفعال إلى البيانات

من الضروري أن تكون الشركة قادرة على الوصول بشكل فعال إلى بياناتها المرتبطة بالخدمات المسندة الى مزودة السحابة والموجودة على البنية التحتية للسحابة، لذا ينبغي على الشركة القيام بما يلي:

- التأكد من إمكانية الوصول إلى البيانات على النحو المتفق عليه مع مزود السحابة.
- ضمان عدم وجود قيود على عدد طلبات الشركة للوصول إلى البيانات أو الحصول عليها.
- ضمان عدم تخزين البيانات في الدول والأماكن التي قد تمنع وصول الشركة الفعال إلى البيانات الخاصة بها.

2.9 مراقبة الأحداث الأمنية والسجلات

لغايات مراقبة الأحداث الأمنية التي قد تتعرض لها الخدمات المسندة الى مزود السحابة، على الشركة التأكد من وجود آليات الكشف المناسبة في الشبكة والأنظمة والتطبيقات لدى المزود لتحليل الأنشطة التي يمكن أن تؤثر على أمن واستقرار الخدمة المسندة. وتحتفظ الشركة عادة بسجلات توثق فيها الأحداث التي تقع على بياناتها وتطبيقاتها وكون أن السجلات المتعلقة بالخدمة موجودة عند المزود ينبغي على الشركة ضمان حصولها على صلاحيات وصول غير مقيدة إلى هذه السجلات وعليه يترتب على الشركة ما يلي:

- توفير ما يلزم لمراقبة وتحليل السجلات المتعلقة بالخدمات المسندة بشكل تلقائي.
- مراجعة سجلات الأحداث بشكل مستمر حسب تصنيف أهمية الحدث وتوثيق ذلك.
- مراجعة سجلات الدخول والتدقيق عليها والاحتفاظ بها للتأكد من دخول المستخدمين المخولين فقط إلى البيانات.
- ضمان الحصول على سجلات الأحداث الأمنية لكافة الخدمات المسندة لمزود السحابة.

2.10 إدارة استمرارية العمل

على الشركة أخذ التدابير المناسبة لضمان استمرارية عملها المرتبط بالخدمات المسندة الى مزود السحابة في حال حدوث أي كارثة أو فشل أو انقطاع مفاجئ في تلك الخدمات وعلى أن تشمل هذه التدابير على الأقل ما يلي:

- وضع خطة استمرارية العمل والتعافي من الكوارث لها وفحصها بالتعاون مع المزود والاتفاق معه عند التعاقد فيما يخص متطلبات وإلتزامات المزود والمتعلقة بالتخطيط لإستمرارية الأعمال على أن يشمل ذلك: زمن التعافي المستهدف (RTO) ونقطة الاسترجاع المستهدفة (RPO).
- التأكد من أن فريق إدارة الأزمات التابع للشركة يدرك تماماً خطة التعافي من الكوارث الخاصة بالمزود.
- النظر في احتمال وأثر الانقطاع غير المتوقع للخدمات المسندة على استمرارية أعمال الشركة.
- التأكد من حفظ نسخ احتياطية للبيانات والبرمجيات في موقع بديل وفحص استرجاع النسخ الاحتياطية للبيانات.
- وضع خطة طوارئ توثق فيها الشركة مزود بديل للمزود الحالي والاجراءات التي ينبغي اتباعها في حال فسخ العقد المبرم مع المزود الحالي بشكل مفاجئ أو عدم تمكنه من الوفاء بالتزاماته لأي سبب كان.

2.11 إدارة التغيير

يمكن حدوث بعض المخاطر عند إجراء تغييرات على بيئة الحوسبة السحابية ولتفادي تلك المخاطر ينبغي على الشركة مراعاة يلي:

- الاتفاق والترتيب مع مزود السحابة على الأسلوب المتبع لإخطارها بالتغييرات التي تطرأ على بيئة الحوسبة السحابية وقدرتها على مراجعة تلك التغييرات للتسهيل على الشركة الإشراف على تلك التغييرات.
- ضمان الرقابة على التغييرات الرئيسية التي يمكن أن تؤثر على استقرار وأمن بيئة التشغيل في السحابة وكشف التغييرات الخاطئة أو غير المصرح بها.

- الاتفاق مع مزود السحابة فيما يخص إجراءات إدارة التغيير والتي تشمل إجراءات طلب التغيير وإجراءات الموافقة عليه والإبلاغ عنه وإجراءات الطوارئ والتغييرات القياسية والأدوار والمسؤوليات الخاصة بإدارة التغيير.
- تحديد كيفية إجراء اختبار التغييرات التي تمت الموافقة عليها.

2.12 سيادة البيانات

- قبل أن تضع الشركة بياناتها في بلد مزود السحابة يجب على الشركة النظر فيما يلي:
  - المتطلبات التنظيمية لبلد المزود.
  - الظروف السياسية والاقتصادية والاجتماعية لبلد المزود.
  - العلاقات الدبلوماسية والسياسات الحكومية والمتطلبات القانونية في بلد المزود.
  - الأحداث والكوارث التي قد تحد من قدرة المزود على تقديم خدماته.
- على الشركة عدم الدخول في ترتيبات الاستعانة مع مزودي السحابة في الدول التي تسمح قوانينها بالوصول الفوري والإجباري إلى المعلومات والبيانات الخاصة فيها.
- على الشركة وضع متطلبات ملزمة تعاقدياً تطلب من مزود السحابة بإخطارها لاتخاذ الإجراءات المناسبة من قبلها في حال تم إلزامه قانونياً في بلد مركز البيانات بالإفصاح عن البيانات الخاصة بالشركة إلى طرف ثالث وذلك لضمان حماية بيانات الشركة.

2.13 خطة الإنهاء

يجب أن يكون لدى الشركة خطة محددة وموثقة للتأكد من قدرتها على إنهاء اتفاقيات الاستعانة بخدمات الحوسبة السحابية دون تعطل في تقديم خدماتها أو تأثر امتثالها للتعليمات والتشريعات الصادرة عن البنك المركزي، لذا على الشركة القيام بما يلي:

- وضع خطط وترتيبات إنهاء يتم فهمها وتوثيقها وفحصها بشكل كامل ودوري وبالتعاون بين الشركة ومزود السحابة.
- تحديد آلية الإنتقال إلى مزود السحابة البديل أو العودة إلى نظام الشركة والحفاظ على استمرارية الأعمال.

- آلية محددة لاسترجاع وحذف البيانات الخاصة بالشركة وجميع السجلات والوثائق من أنظمة مزود السحابة عند إنهاء العقد مع مزود السحابة أينما كان قد تم تخزينها بما في ذلك مواقع النسخ الاحتياطي وكذلك وسائط تخزين البيانات عبر الإنترنت.
- مراقبة المخاطر والنظر في الإجراءات التي قد تتخذ في حال توقف مزود السحابة عن العمل.
- وضع ترتيبات خاصة لضمان الحصول على بيانات الشركة أو نقلها لمزود بديل في حال عدم وفاء المزود بالتزاماته أو إنهاء العقد معه أو لأي سبب كان وإلزام المزود الحالي بالتعاون مع المزود البديل أو الشركة لاتمام عملية النقل.

الفصل الثالث: المعايير الخاصة بالحوسبة السحابية

نظراً للتحديات التي تواجهها الشركات والتي قد تعيق تبنيها لتكنولوجيا الحوسبة السحابية ومن أجل تمكين الشركات من استخدام هذه التكنولوجيا بطريقة آمنة تقلل من تعرضها للمخاطر الناجمة عن ذلك؛ على الشركات اتخاذ كافة التدابير اللازمة لحمايتها من تلك المخاطر من خلال استخدام المعايير الأمنية الشائعة في جميع أنحاء العالم التي تدعم تكنولوجيا الحوسبة السحابية والتي يمكن من خلالها المحافظة على سرية وأمن البيانات عند الإستعانة بمزود السحابة، وتقدم هذه المعايير العديد من الفوائد ومنها:

- تعزيز توافقية أنظمة الشركة مع أي أنظمة أخرى مما يجعل الانتقال من مزود سحابة إلى آخر أبسط.
- ضمان اتباع الشركات ومزودي السحابة أفضل الممارسات بهذا الخصوص.
- تعتبر المعايير وسيلة فعالة تمكن الشركات من المقارنة بين مزودي السحابة لاختيار المزود الأنسب.
- يتيح استخدام المعايير مسارا أسهل للامتثال التنظيمي.

وهناك العديد من المعايير الخاصة بأمن تكنولوجيا الحوسبة السحابية والتي تم نشرها مؤخراً، بما في ذلك ISO/IEC 27017 و ISO/IEC 27018، التي توفر إرشادات أكثر تفصيلاً لكل من الشركات ومزودي السحابة. بالإضافة إلى ذلك، هناك عدد من المعايير العامة لتكنولوجيا المعلومات التي يمكن تطبيقها عند استخدام تكنولوجيا الحوسبة السحابية حيث أن هذه المعايير ليست محددة للحوسبة السحابية بشكل خاص، ولكنها عامة بحيث يمكن تطبيقها على بيئة الحوسبة السحابية لذا ينبغي على الشركة ومزود السحابة إعطاء الأهمية لهذه المعايير حيث تقدم هذه المعايير توجيهات وتوصيات وبشكل تفصيلي لكل من الشركة والمزود ونخص بالذكر المعايير التالية مصنفة حسب عدة مواضيع كما هو مبين ادناه في جدول رقم (3).

جدول 3 : أهم المعايير المستخدمة في مجال تكنولوجيا الحوسبة السحابية

الموضوع	المعايير
الحوكمة وإدارة المخاطر والامتثال	• COBIT • ISO/IEC 20000 • SSAE 16 or ITIL depending on type of workload • ISO/IEC 27001 and ISO/IEC 27002 • ISO/IEC 27017 & ISO/IEC 27018 • ISO/IEC 38500 – IT Governance • Cloud Security Alliance (CSA) Cloud Controls Matrix • National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
العمليات التشغيلية و التجارية	• SSAE 16 • ISO/IEC 27000
إدارة الادوار	• LDAP, SAML 2.0, OAuth 2.0, WS-Federation, OpenID Connect, SCIM • XACML • PKCS, X.509, OpenPG
حماية البيانات و المعلومات	• HTTPS, SFTP, VPN using IPSec or SSL • OASIS KMIP • US FIPS 140-2
سياسات الخصوصية	• ISO/IEC 27018
أمن وحماية الشبكات	• ISO/IEC 27033 or FIPS199/200 standards

الضوابط الأمنية على البنية التحتية	• ISO/IEC 27002 • ISO/IEC 27017 & ISO/IEC 27018
شروط الأمان في اتفاقية مستوى الخدمة	• ISO/IEC 19086 • ISO/IEC 27004:2009, TM Forum TR 178, NIST Special Publication 800-55, CIS Consensus Security Metrics V1.1.0, and ENISA Procure Secure • CWE list • CSA STAR registry • PCI DSS • FedRAMP program
عمليات الإنهاء	• ISO/IEC 19086

ملحق تعليمات وتعاميم البنك المركزي

تم تجميع التعليمات والتعاميم الصادرة عن البنك المركزي فيما يتعلق بالإسناد الخارجي للبنوك المرخصة والعاملة في المملكة وذلك لتنظيم عملية الاستعانة بخدمات الحوسبة السحابية في المملكة.

1. **تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (2016/65) تاريخ 2016/10/25**

- المادة (3/ج) : "على البنوك عند توقيع اتفاقيات إسناد (Outsourcing) مع الغير لتوفير الموارد البشرية و الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات بهدف تسيير عمليات البنك التأكد من إلتزام الغير بتطبيق بنود هذه التعليمات بشكل كلي أو جزئي بالقدر الذي يتناسب مع أهمية وطبيعة عمليات البنك والخدمات والبرامج والبنية التحتية المقدمة قبل و أثناء فترة التعاقد، وبما لا يعفي المجلس والإدارة التنفيذية العليا من المسؤولية النهائية لتحقيق متطلبات التعليمات بما في ذلك متطلبات التدقيق الواردة في المادة(9) أدناه، وتعتبر فترة نفاذ التعليمات أو فترة التعاقد المدة الزمنية الواجب خلالها توفيق أوضاع الشركات المتعاقد معها حاليا بالخصوص أيهما أسبق."
- المرفق رقم (6) من التعليمات (منظومة السياسات) سياسة التعهيد (Outsourcing):

"اعتماد سياسة عامة للإستعانة بالموارد بشكل عام وبموارد تكنولوجيا المعلومات بشكل خاص، تلك الموارد سواء المملوكة للبنك (In-sourcing) أو المملوكة للغير (Outsourcing) تراعي التعليمات والأنظمة والقوانين وتحاكي أفضل الممارسات الدولية المقبولة بهذا الخصوص، وتأخذ بعين الاعتبار مكان العملية الإنتاجية (On-site, Off-site, Near-site, Off-shore)، وتأخذ بعين الاعتبار وتراعي متطلبات مراقبة مستوى الخدمات (Service Levels) وتفعيل حق التدقيق (Audit Right) من قبل اطراف ثالثة محايدة موثوقة وتحقيق متطلبات استمرارية العمل و ضوابط الحماية اللازمة لتلبية متطلبات السرية والمصداقية بالإضافة لمتطلبات الكفاءة والفعالية في استغلال الموارد."

- مرفق رقم (8) الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات، الاستضافة وضوابط الأمن المادي والبيئي (Physical and Environmental Security) لغرف الخوادم الرئيسية وغرف الاتصالات والتزويد بالكهرباء، توفير ضوابط الأمن المادي والبيئي بالحد الأدنى حسب ما يلي:
  - "يراعي أن تتواجد الغرف وأن يكون تصميم البنية التحتية للبناية بعيدة ومحمية عن تهديدات فيضانات وتسربات المياه والصرف الصحي المحتملة، سواء أسفل البناء أو في نهايته بالقرب من

الأسطوح أو أي مكان آخر معرض لذلك. كما أن مساحة الغرف يجب أن تكون كافية وتلبي احتياجات البنك الحالية وتأخذ بالاعتبار التوسع المستقبلي المحتمل.

- يجب أن يكون مكان الغرفة والبناية بشكل عام غير محدود الوصول (سواء بطبيعة الموقع الجغرافي أو بموجب الاتفاقيات التعاقدية الحصرية) من قبل شركات الاتصالات كافة ومن مزودين متنوعين.
- يجب ان تتمتع غرف الخوادم الرئيسية وغرف الاتصالات مثل (Routers, Switches, etc.) وغرف تزويد الكهرباء بالحماية المادية والبيئية بحيث تكون محاطة بجدران مسلحة بدون شبابيك ومعزولة من حيث التأثيرات الكهرومغناطيسية التي تؤثر سلبا على بيانات أجهزة الكمبيوتر، ومخدومة بمدخل احتياطي محكم لاستخدامه من قبل الأفراد عند الطوارئ، ويجب أن تكون الغرفة من حيث التصميم مخدومة بمداخل الكهرباء وأجهزة مكافحة الحريق (مثل FM 200) بحسب المواصفات العالمية والمحلية بهذا الخصوص، كما يجب أن تكون على أرضية مرفوعة (Raised Floor)، ويجب أن تحتوي على كواشف للدخان والمياه والحرارة والرطوبة بدرجة حساسية عالية، كما يجب توفير المراقبة التلفزيونية المسجلة والتبريد الموزع على كافة مساحة الغرفة بشكل عادل لحماية الأجهزة من الحرارة والرطوبة المرتفعة، مع توفير أجهزة لسحب الغبار من الغرفة، وأن يكون الدخول محكم ومراقب بحث يمنع غير المخولين من ذلك، مع مراعاة عدم وضع أي إشارات تدل الغير على مكان تواجد تلك الغرف الحساسة في البنك بدون مرافقين مخولين.
- يجب تزويد غرف الخوادم وغرف الاتصالات بمدخل كهرباء متعدد المصادر وأن يكون التحويل بينها بشكل أوتوماتيكي، أي توفير بطاريات (UPS) بالإضافة إلى مولدات كهرباء بالقدرة الكافية لتشغيل أجهزة وعمليات البنك (الحساسة على الأقل) في حال انقطاع مصدر الكهرباء الرئيسي.
- يجب الأخذ بالاعتبار متطلبات الدفاع المدني ودائرة المواصفات والمقاييس الأردنية (حيثما تطلب الأمر ذلك).
- كل ما ذكر أعلاه أيضا على غرف الخوادم والاتصالات والكهرباء البديلة (Disaster Recovery Sites)."

2. تعميم بخصوص تعليمات خطة استمرارية العمل رقم (9943/1/10) تاريخ 2014/8/17

- المادة (11): "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."

- المادة (12): "أن تراعي سياسات التعهيد والاستعانة بخدمات الغير (Ousourcing 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، وتضمين العقود والاتفاقيات الموقعة مع المزودين لتعكس هذه المتطلبات، ومخاطبة المزودين الحاليين لتوفيق أوضاعهم تلبية لذلك."

3. تعليمات أنظمة الضبط والرقابة الداخلية رقم (2007/35) تاريخ 2007/6/10

- المادة(9/هـ): "جودة الخدمات المقدمة من قبل الاطراف الخارجية وآلية تقديمها من حيث المحافظة على شروط السرية والدقة والتوافر والتكاملية(المصداقية)، وبحيث يتم ضبط هذه الشروط من خلال اتفاقيات أصولية موثقة. "

4. تعميم بخصوص مبادئ إدارة مخاطر العمل المصرفي الإلكتروني رقم (3344/1/10) تاريخ 2005/3/21

- المادة (أولاً/3): "على مجلس الإدارة والإدارة العليا العمل على إنشاء نظام وآلية لإدارة خدمات الجهات الخارجية (Outsourcing relationships) المتعاقد معها بغرض دعم عملية تقديم خدمات العمل المصرفي الإلكتروني والاستمرار في تطوير ذلك."

5. تعليمات ممارسة البنوك لأعمالها بوسائل إلكترونية رقم (2001/8) تاريخ 2001/7/26

- المادة (7): "ضرورة تنظيم الاتفاقيات المبرمة بين البنك وأي من الشركات الخادمة والمزودة والداعمة بما لا يتعارض مع أحكام السرية المصرفية، وبما يضمن أمن النظم والمعلومات."

المراجع

1. **ABS Cloud Computing Implementation Guide 1.1 For The Financial Industry in Singapore**, The Association of Banks in Singapore, 2 Aug 2018.
2. **Banking on Cloud (A discussion paper by the BBA and Pinsent Masons),** BBA Cloud Working Group, 5 December 2016.
3. **NIST Cloud Computing Standards Roadmap**, NIST Cloud Computing Standards Roadmap Working Group, NIST Cloud Computing Program, July 2013.
4. **NIST Guidelines on Security and Privacy in Public Cloud Computing**, National Institute of Standards & Technology Gaithersburg, MD, United States , 2011
5. **Australian Government Cloud Computing Policy Smarter ICT Investment**, Australian Government, Department of Finance, Version 3.0, October 2014
6. **International Standard ISO/IEC 17788 First edition 2014-10-15**, ISO/IEC 17789, 2014
7. **Cloud Security Policy for Government Agencies,** Qatar National Information Assurance, 2014
8. **Practical Guide to Cloud Computing Version 2.0,** Cloud Standard Customer Council, April, 2015
9. **Cloud Security Standards "What to Expect & What to Negotiate Version 2.0",** Cloud Standard Customer Council, 2016.
10. **Security for Cloud Computing Ten Steps to Ensure Success Version 2.0 March**, Cloud Standards Customer Council, 2017
11. **Security Guidance for Critical Areas of Focus in Cloud Computing V3.0,** Cloud Security Alliance

12. **PCI DSS Cloud Computing Guidelines,** Cloud Special Interest Group PCI Security Standards Council, February 2013
13. **Best Practices for Security in Cloud Adoption by Indian Banks**, Members of The Open Group Security Forum, March 2015
14. **How Cloud is Being Used in the Financial Sector: Survey Report**, CSA, March 2015
15. **Towards a Generic Value Network for Cloud Computing**, Markus Böhm*, Galina Koleva, Stefanie Leimeister, Christoph Riedl, and Helmut Krcmar, 2010
16. **Secure Use of Cloud Computing in the Finance Sector / Good practices and recommendations,** European Union Agency for Network and Information Security, December 2015.
17. **A Reference Guide to Cloud Computing Dimensions: Infrastructure as a Service Classification Framework,** Jonas Repschlaeger, Stefan Wind, Ruediger Zarnekow, Klaus Turowski, 2012
18. **Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,** CSA, December 2009
19. **Cloud Computing-Software as Service,** Gurudatt Kulkarni, Jayant Gambhir, Rajnikant Palwe, March, 2012
20. **FG 16/5 - Guidance for firms outsourcing to the 'cloud' and other third- party IT services,** FCA, July 2016.
21. **Framework for Risk Management in Outsourcing Arrangements by Financial Institutions,** State Bank of Pakistan, 2017
22. **Circulaire Cloud Computing,** De Nederlandsche Bank, 2012
23. **Cloud Computing: Business Benefits with Security,** Governance and Assurance Perspectives/ISACA, 2009
24. **Outsourcing in Financial Services,** Basel Committee on Banking Supervision, February 2005

25. **Guidelines on Outsourcing,** Monetary Authority of Singapore, 27 JUL 2016
26. **Guidelines on Business Continuity Planning,** Monetary Authority of Singapore, June 2003
27. **Public Consultation on Guidance on Outsourcing,** Response to Feedback Received, July 2016
28. **سبل الإفادة من تطبيقات الحوسبة السحابية في تقديم خدمات المعلومات بدولة الإمارات العربية المتحدة،** كلية الدراسات الإسلامية والعربية بدبي، 2014/3