Sultanate of Oman
Information Technology Authority

e.oman

إطار حوكمة الحوسبة السحابية

قسم الحوكمة والمعايير

المصادقة والتوزيع:

	الاسم	المنصب	تاريخ الإصدار
الاعداد	عامر جميل	استشاري حوكمة تقنية المعلومات	2017
التصديق			
الاعتماد	اللجنة التوجيهية		

قائمة التوزيع	
أ.	هيئة تقنية المعلومات
ب.	جميع الوحدات الحكومية المعنية
ج.	النشر على شبكة الإنترنت

سجل مراجعة المسند:

رقم الإصدار	التاريخ	القائم على المستند	الملاحظات
1.0	2017	عامر جميل	إصدار المستند

الفهرس

الأشكال التوضيحية

1. نظرة عامة

يقدم هذا المستند إطار عمل لتبني خدمات الحوسبة السحابية بنماذجها وخدماتها المتنوعة، ويتناول قائمة ببعض المزايا والتحديات والمخاطر التي قد تنجم نتيجة تبني الحوسبة السحابية ذات الصلة بالوحدات الحكومية في سلطنة عمان. يعرض إطار العمل التوجيهات التنظيمية والتقنية والبيئية لتبني خدمات الحوسبة السحابية. تحتاج الوحدات الحكومية – مع تبنيها للحوسبة السحابية – إلى أن تكون على دراية بالآثار القانونية والتأكد من أن مقدم خدمات الحوسبة السحابية متوافق مع الصلاحيات والقوانين والسياسات المعمول بها داخل سلطنة عمان.

1.1. الغرض

يهدف إطار عمل خدمات الحكومة الإلكترونية في عمان إلى تعزيز تقديم الخدمات الحكومية بما يتماشى مع رسالة عمان الرقمية، ويهدف إطار العمل إلى وضع ضوابط لتقليل معدل المخاطر إلى أدنى حد ممكن وتقديم مبادرات تقنية المعلومات بشكل أفضل. كما أن إطار العمل هذا يهدف إلى تحديد المبادئ التوجيهية بُغية تبني خدمات الحوسبة السحابية كجزء من رسالة عُمان الرقمية. ويشمل ذلك عملية تحديد وتقييم المخاطر، ووضع الاستراتيجيات اللازمة لتقديم المساعدة في العمليات المتعلقة بالبنية الاساسية السحابية وحمايتها وكذلك وضع الآليات اللازمة لضمان تنفيذ الاستراتيجيات على النحو المرجو.

أ. يقدم إطار العمل هذا تعريف حول الحوسبة السحابية لمختلف أصحاب المصلحة داخل الوحدات الحكومية وعملية تبني الحوسبة السحابية كخدمة لمختلف الوحدات في سلطنة عمان.

ب. يقدم إطار العمل الإرشادات اللازمة وكذلك يساعد الوحدات على تحديد نموذج الحوسبة السحابية المناسب لهم بناءً على معايير معينة من شأنها أن تساعد الوحدات على إجراء مقارنة بين تقنية المعلومات الحالية وخدمات الحوسبة السحابية.

ج. يقدم إطار العمل مقومات الجاهزية وقابلية تبني خدمات الحوسبة السحابية، والتي ينطبق بعضها على أي برنامج بينما ينطبق البعض الآخر على خدمات الحوسبة السحابية بصفة خاصة. تم تبني هذه المقومات من إطار عمل المجالات التكنولوجية والتنظيمية والبيئية (TOE). ويُشير إطار عمل المجالات التكنولوجية والتنظيمية والبيئية (TOE) هذا إلى نظرية (فرضية) على مستوى المؤسسة توضح إمكانية تأثير الثلاثة مقومات المختلفة في مجال أعمال الشركة على قرارات تبني الخدمات.

1.2. الفئات المستهدفة

يرد أدناه قائمة الفئات المستهدفة لإطار عمل تبني خدمات الحوسبة السحابية.

أ. الوحدات الحكومية في سلطنة عمان التي ترغب في النظر في تبني الحوسبة السحابية وتريد معرفة المزايا والتحديات والمخاطر المرتبطة بخدمات الحوسبة السحابية.

ب. جميع شركاء الوحدات الحكومية الذين قد لا يستفيدون بشكل مباشر من إطار العمل ولكنهم قد يهتمون بمعرفة المزيد عن خدمات الحوسبة السحابية.

2. العوامل البيئية

تعمل الحكومات في جميع أنحاء العالم على تعزيز فكرة تقديمها للخدمات والخدمات الإلكترونية بأفضـــل طريقة ممكنة لتنفيذ الأعمال اليومية وبصـفة خاصـة في المكاتب الحكومية التي تتواصـل مباشـر مع المواطنين. كما أنه مع توافر خدمات الحوسـبة السحابية، فهناك فرصة كبيرة لتسريع عمليات تطوير تطبيقات الحكومة الإلكترونية ونشرها، وتعزيز سرعة الأداء في تخصيص ونشر تقنية المعلومات والاتصالات (ICT) لتلبية متطلبات العمل المحددة، مع زيادة كفاءة تقنية المعلومات والاتصالات الحكومية في نفس الوقت (من خلال إعادة الاستخدام وقابلية التوسع في تقديم الخدمة).

تتمثل أهداف الوحدات العمانية في تبني استراتيجية الحوسبة السحابية فيما يلي:

أ. الاستخدام الأمثل للبنية الاساسية.

ب. تسريع عمليات تطوير التطبيقات ونشرها.

ج. ســـهولة النســـخ للتطبيقات الناجحة عبر الوحدات المماثلة لتفادي الازدواجية في الجهود والتكلفة في تطوير تطبيقات مماثلة.

د. توفير التطبيقات المعتمدة وفقًا للمعايير الموحدة في مكان واحد.

يتعين على الوحدات في عُمان – مع الأخذ في الاعتبار أهداف تبني خدمات الحوســـبة الســـحابية – التمتع بالقدرة على تحقيق المزايا التجارية والتقنية الواردة أدناه:

أ. تحسـين بيئة التكامل داخل الوحدات من خلال تعزيز فكرة تقديم حل لمجموعة أوسـع من المسـتخدمين بدلاً من اقتصـار الخدمة على وحدة واحدة.

ب. إمكانية نشـر الممارسـات الموحدة والمتطلبات التنظيمية والقيود من خلال الحل السـحابي لجميع الوحدات بينما لا يزال بإمكان كل وحدة الاحتفاظ باستقلاليتها في نفس الوقت.

ج. الحصول على تعاون مُعزز من خلال حل الأعمال التعاوني المشترك.

د. زيادة التركيز على تقديم الخدمات دون الحاجة إلى القيام باستثمارات ضخمة في مجال تقنية المعلومات.

ه. وقت أسرع للتسويق لإطلاق خدمات جديدة.

و. انخفاض تكاليف التشغيل مع خفض تكاليف الأجهزة والبرامج والتراخيص.

ز. انخفاض تكاليف التطوير من حيث تطوير واستضافة الخدمات والقدرات الجديدة.

3. المبادئ التوجيهية

تشكل المبادئ التوجيهية لإطار عمل تبني خدمات الحوسبة السحابية أساسًا للسلوك. يجب أن تتبنى الوحدات الحوسبة السحابية مع الأخذ في الاعتبار استراتيجية الحوسبة السحابية أولاً. تركز استراتيجية الحوسبة السحابية أولاً على تقليل تكاليف تقنية المعلومات من خلال الاستفادة من مزايا استخدام البنية الاساسية والخدمات المشتركة. وستدفع الوحدات مقابل الموارد المستهلكة فقط. ويرد أدناه المبادئ التوجيهية لتبني الوحدات لخدمات الحوسبة السحابية.

أ. **التمكين**: يجب على الوحدات وضع خطط الحوسبة السحابية كعامل تمكين استراتيجي، وليس الاستعانة بمصادر خارجية أو منصات تقنية.

ب. **التكاليف والمزايا**: يجب على الوحدات تقييم مزايا تبني الحوسبة السحابية بناءً على الإلمام الشاملة لتكاليف الحوسبة السحابية مقارنةً بتكاليف حلول الأعمال لمنصات التقنية الأخرى.

ج. **المخاطر المؤسسية**: يجب أن تتبنى الوحدات منظور إدارة مخاطر المؤسسة (ERM) لإدارة تبني واستخدام الحوسبة السحابية.

د. **الكفاءة**: يجب على الوحدات التي تتبنى خدمات الحوسبة السحابية دمج النطاق الكامل للإمكانيات التي يوفرها مقدمي خدمات الحوسبة السحابية مع الموارد الداخلية لتوفير دعم فني شامل وحلول التسليم.

ه. **المساءلة**: يجب على الوحدات إدارة المسؤوليات من خلال تحديد المسؤوليات الداخلية ومسؤوليات مقدم الخدمة بوضوح.

و. **الثقة**: يجب أن تجعل الوحدات الثقة جزءًا أساسيًا من حلول الحوسبة السحابية، وبناء الثقة في جميع العمليات التجارية التي تعتمد على الحوسبة السحابية.

4. مقدمة في الحوسبة السحابية

إن الحوسبة السحابية هي نموذج للوصول إلى الخدمات (الأعمال أو التطبيقات) عبر الإنترنت والتي سيتم استضافتها إما في موقع خاص بجهة خارجية (مقدم الخدمة) أو في مركز بيانات الوحدات (الخدمات المدمجة). يمكن الوصول إلى هذه الخدمات (الخوادم والتطبيقات والتخزين وما إلى ذلك) على نطاق واسع عبر قنوات مختلفة (مكاتب العمل وأجهزة الكمبيوتر المحمولة والهواتف المحمولة والأجهزة اللوحية) من أي مكان، وإتاحتها عند الطلب. كما يتم توفير هذه الخدمات من خلال استخدام مجموعة من الموارد (الافتراضية أو المادية) والتي يمكن استخدامها من قبل جهات متعددة ويمكن تقليصها أو زيادتها حسب المتطلبات. وتخضع الخدمة إلى قابلية القياس (الحساب)، مما يعني أن الوحدات ستدفع مقابل الوقت الذي تم فيه استخدام الموارد فقط.

تعزز الحوسبة السحابية من إمكانية توفير الخدمات ويتم وصفها بخمس خصائص أساسية وثلاثة نماذج خدمة أولية وأربعة نماذج نشر، والتي يتم ذكرها بالتفصيل في أقسام أخرى.

الخصائص	نماذج الخدمة	نماذج النشر
الخدمة الذاتية عند الطلب	خدمات البرمجيّات (SaaS)	السحابة العامة
وصول واسع للشبكة	خدمات المنصّات السّحابية (PaaS)	السحابة الخاصة
المرونة والسرعة	خدمات البنية الأساسيّة (IaaS)	السحابة الهجينة
التوفير السريع		السحابة المجتمعية
الخدمة المقاسة		

الشكل التوضيحي رقم (1) – نموذج الحوسبة السحابية

4.1. خصائص الحوسبة السحابية

الخصائص الأساسية الخمس للحوسبة السحابية التي حددها المعهد الوطني للمعايير والتكنولوجيا (NIST)، تميز الحوسبة السحابية عن تقنية المعلومات التقليدية، وهي مقبولة عالميًا. ويتم تحديدها باختصار كما هو موضح أدناه:

أ. **الخدمة الذاتية عند الطلب**: يمكن للوحدات توفير إمكانات الحوسبة، مثل وقت الخادم وتخزين الشبكة، حسب الحاجة تلقائيًا دون الحاجة إلى تدخل بشري مع مقدم الخدمة.

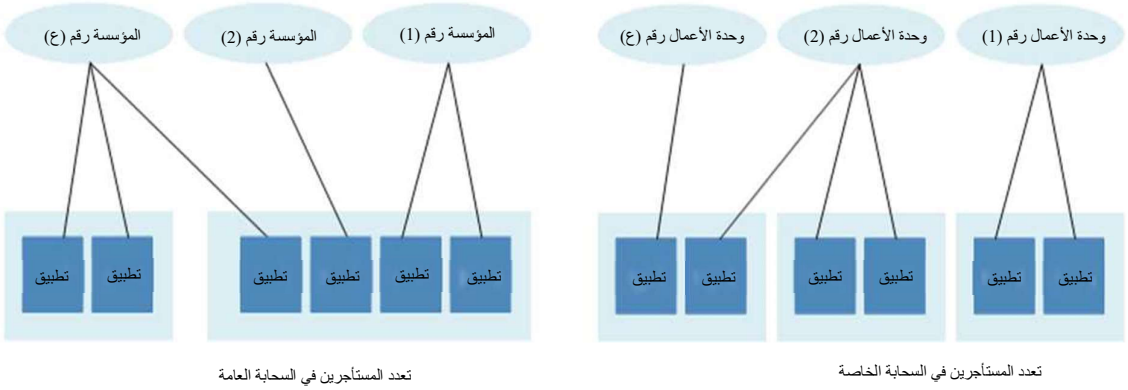
ب. **وصول واسع للشبكة**: أي خدمة (أعمال / دعم / تطبيقات) متاحة عبر الشبكة ويمكن للوحدات الوصول إليها عبر الهواتف المحمولة والأجهزة اللوحية وأجهزة الكمبيوتر المحمولة ومكاتب العمل

ج. **تجميع الموارد**: سيتم تجميع موارد الحوسبة لمقدم الخدمة السحابية لخدمة الوحدات باستخدام نموذج متعدد المستأجرين، مع تخصيص موارد مادية وافتراضية مختلفة وإعادة تخصيصها ديناميكيًا وفقًا لطلب المستخدم.

د. **المرونة والسرعة**: يمكن توفير أي خدمة وإطلاقها بشكل مرن، وفي بعض الحالات تلقائيًا، لتوسيع نطاقها بسرعة نحو الخارج والداخل بما يتناسب مع الطلب. ستبدو الإمكانيات المتاحة للتزويد غير محدودة – بالنسبة للهيئات – ويمكن تخصيصها بأي كمية في أي وقت

ه. **الخدمة المقاسة**: تتحكم الأنظمة السحابية تلقائيًا في استخدام الموارد وتحسّنه من خلال الاستفادة من قدرة القياس عند مستوى معين من التجريد المناسب لنوع الخدمة (على سبيل المثال، التخزين والمعالجة وعرض النطاق الترددي وحسابات المستخدمين النشطة). يمكن مراقبة استخدام الموارد والتحكم فيه والإبلاغ عنه، مما يوفر الشفافية لكل من مقدم الخدمة والوحدات الفردية للخدمة المستخدمة.

تُعد خاصية تعدد المستأجرين خاصية أخرى لم يعترف بها معهد الوطني للمعايير والتكنولوجيا (NIST) على نطاق واسع، ولكنها لا تزال مقبولة عالميًا. وتشير هذه الخاصية إلى إمكانية استخدام وحدات متعددة قد تنتمي إلى وحدات سلطنة عمان أو منظمات مختلفة (عامة وخاصة) لنفس الموارد أو التطبيقات، وهي سمة مهمة جدًا للسحابة العامة.



الشكل التوضيحي رقم (2) – تعدد المستأجرين في السحابة

4.2. نماذج تبني خدمات الحوسبة السحابية

تتمثل أول خطوة لتبني الوحدات لخدمة الحوسبة السحابية المناسبة في اختيار نموذج التسليم الذي سيتم تقديم الخدمات عليه. يمكن الاستفادة من الخدمات على السحابة من خلال تبني أي من النماذج التالية:

أ. السحابة العامة، يقوم من خلالها مقدم الخدمة بتوفير الخدمات، مثل التطبيقات والتخزين، للوحدات عبر الإنترنت بنظام السداد مقابل كل استخدام.

ب. السحابة الخاصة، سيتم استضافتها بمركز بيانات الوحدات، أو كسحابة خاصة يتم استضافتها بمركز خارجي بمعرفة مقدم خدمة خارجي وتُعرف أيضًا باسم السحابة الخاصة الافتراضية. ستتيح السحابة الخاصة للوحدات إمكانية الاحتفاظ بقابلية توحيد وتنفيذ أفضل الممارسات الخاصة بها.

ج. السحابة الهجينة، والتي تجمع بين خصائص السحابة الخاصة والعامة.

د. السحابة المجتمعية، حيث تتشارك العديد من المؤسسات الحكومية من نفس المجال (مثل الحكومات والوحدات التابعة، وما إلى ذلك) في نفس البنية الاساسية السحابية.

يوضح الملحق الوارد أدناه نماذج تبني ونشر خدمات الحوسبة السحابية المختلفة.

نموذج السحابة	الجهة المالكة للبنية الاساسية	الجهة المسؤولة عن إدارة البنية الاساسية	الموقع	المنتفعين من الخدمة (المُستهلكين)
العامة	مقدم خدمة الحوسبة السحابية	مقدم خدمة الحوسبة السحابية	مقدم خدمة الحوسبة السحابية	جهات متعددة
الخاصة	الوحدات	الوحدات	مراكز البيانات المملوكة للوحدات	الوحدات
السحابة الخاصة الافتراضية	مقدم خدمة الحوسبة السحابية	مقدم خدمة الحوسبة السحابية	مقدم خدمة الحوسبة السحابية	الوحدات
الهجينة	كلاهما	كلاهما	كلاهما	الوحدات والكيانات الخاصة
المجتمعية	مقدم خدمة الحوسبة السحابية أو الوحدات	مقدم خدمة الحوسبة السحابية أو الوحدات	مقدم خدمة الحوسبة السحابية أو الوحدات	الوحدات والجهات الخارجية ذات الصلة

الشكل التوضيحي رقم (3) – نماذج تبني خدمات الحوسبة السحابية

4.3. نماذج خدمات الحوسبة السحابية

تتمثل الخطوة الثانية لتبني الوحدات لخدمة الحوسبة السحابية المناسبة في تحديد نوع الخدمة.

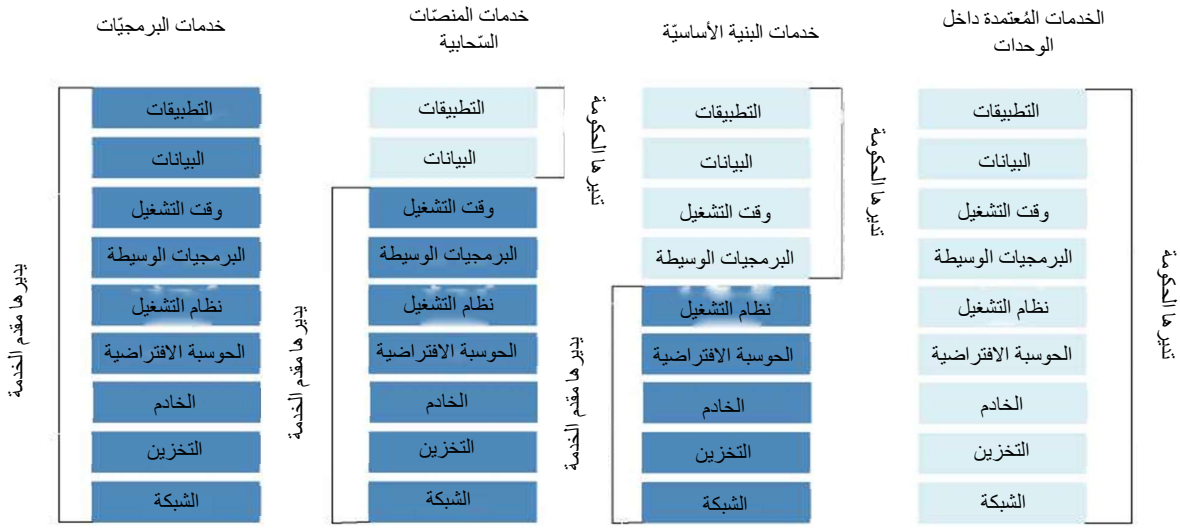
أ. خدمات البرمجيّات (**SaaS**)

ب. خدمات المنصّات السّحابية (**PaaS**)

ج. خدمات البنية الأساسيّة (**IaaS**)

تم تصميم كل نموذج من نماذج خدمات الحوسبة السحابية بحيث يظهر اسم (نوع) الخدمة على مقدمة النموذج الأساسي وتظهر أدناه هيكل ومعايير الخدمات.

يوضح الشكل التوضيحي الوارد أدناه نماذج الخدمة السحابية الثلاثة والطبقات التي تشكل نموذجًا محدداً. ويُظهر الشكل أيضًا الجهة المسؤولة (مقدم الخدمة أو الوحدات) التي ستتولى إدارة النقاط المشمولة في نموذج الخدمة، وفي نفس الوقت يعرض مقارنة بين تلك النماذج ونموذج خدمات تقنية المعلومات التقليدي المُعتمدة داخل الوحدات.



الشكل التوضيحي رقم (4) – نماذج الحوسبة السحابية

أ. تتيح **خدمات البرمجيّات (SaaS)** توافر البنية الاساسية والأنظمة وإدارتها بواسطة مقدم الخدمة. سيهتم مقدم الخدمة بجميع عمليات تطوير البرامج وصيانتها وترقياتها. سيتعين على الوحدات عند اختيار مثل هذه الخدمة أن تدفع فقط مقابل عدد تراخيص البرنامج على أساس الاشتراك. من أمثلة خدمات البرمجيّات (SaaS) برنامج "مايكروسوفت أوفيس 365" (Office 365) وإدارة علاقات العملاء (CRM) وتخطيط موارد المؤسسة وبرنامج المؤتمرات عبر الإنترنت (GoToMeeting) وما إلى ذلك.

ب. تُعد **خدمات المنصّات السّحابية (PaaS)** أعلى من مستوى خدمات البنية الأساسيّة (IaaS) بمستوى واحد وهو مثالي للوحدات لتصميم التطبيقات والخدمات عبر الإنترنت باستخدام مجموعة من الأدوات التي يوفرها مقدم الخدمة. يمكن للوحدات الاختيار من بين الأدوات لتصميم تطبيقات مناسبة وفقاً لمتطلباتهم. وسيوفر مقدم الخدمة الدعم اللازم للوحدات فيما يتعلق بالبنية الاساسية والتطبيقات. ومن الأمثلة على ذلك، منصات المحاكاة الافتراضية وجافا وخدمات "ماي إس كيو إل" (MySQL) وما إلى ذلك.

ج. فيما يتعلق **بخدمات البنية الأساسيّة (IaaS)**، يتم توفير البنية الاساسية لتصميم أو نشر أي خدمات يوفرها مقدمة الخدمة. وتحتاج الوحدات إلى الاهتمام بالبرمجيات الوسيطة وأنظمة التشغيل والتراخيص المرتبطة بها لتصميم تلك الخدمات. ومن الأمثلة على ذلك سحابة أمازون للحوسبة المرنة (AWS EC2) والتخزين المخصص لسحابة "راك سبيس" (Rackspace) (حلول التخزين المباشرة (DAS) والتخزين المتصلة بالشبكة (NAS) وشبكة منطقة التخزين (SAN)).

توجد بعض نماذج الخدمة السحابية المشتقة من بين نماذج الخدمة الرئيسية الثلاثة والتي تعد أيضًا حلولًا تستند إلى نماذج الخدمة الثلاثة المذكورة أعلاه. ويرد أدناه أمثلة على نماذج السحابة سالفة الذكر.

أ. يمكن للوحدات من خلال استخدام **خدمات إجراءات العمل (BPaaS)** تبني التطبيقات المستخدمة لخدمات الأعمال مثل مركز الاتصال الموحد، وإدارة بطاقات الوقت، والتي يمكن تقديمها بناءً على خدمات البرمجيّات (SaaS).

ب. تُعد **خدمات التعافي من الكوارث (DRaaS)** حلاً يمكن بموجبه للوحدات أن تختار النسخ المتماثل واستضافة الخدمات خارج الموقع (بعد تقييم أو تبنيا على أهمية البيانات وتصنيفها) وداخل السحابة لتوفير تجاوز الفشل في حالة كارثة بشرية أو طبيعية.

ج. تُمثل **خدمات الأمن (SECaaS)** حل لتوفير أنظمة وبيانات آمنة على السحابة وكذلك في تثبيت برامج تقنية المعلومات التقليدية عبر الإنترنت. سيوفر مقدم خدمة الحوسبة السحابية خدمات إلى الوحدات مثل برامج مكافحة الفيروسات وإدارة الهوية والوصول (IDAM) كتطبيقات متاحة على السحابة.

د. تعمل **خدمات سطح المكتب (DaaS)** على توفير الواجهة الخلفية لسطح مكتب (جهاز كمبيوتر) افتراضي. سيقوم مقدم الخدمة السحابية بإدارة التخزين والنسخ الاحتياطي والأمان والترقيات. كما سيتعين على الوحدات إدارة صور سطح المكتب والتطبيقات والأمان الخاصة بها بينما يتعامل مقدم الخدمة مع جميع تكاليف البنية الاساسية الخلفية وأعمال الصيانة ذات الصلة.

4.4. عوامل تبني نموذج الحوسبة السحابية

ستحتاج الوحدات إلى تقييم متطلباتها قبل التفكير في تبني نموذج سحابي وذلك لفهم أسباب موائمة نموذج السحابة المحدد لأعمالها.

يتعين على الوحدات التي تقرر اختيار خيار نموذج تقديم خدمات البرمجيّات (SaaS) للسحابة التي ستتبناها أن تأخذ في الاعتبار ما يلي:

أ. يجب على الوحدات اختيار خدمات البرمجيّات (SaaS) عندما يرغبون في تحسين كفاءة العمليات المتعلقة بأعمالها من خلال القدرة على التركيز بشكل أكبر على العمليات المتعلقة بالأعمال بدلاً من العمليات القائمة على تبني برنامج أو تقنية محددة، وتعزيز التعاون بين عدد من الخدمات الإلكترونية المختلفة التي يتم تقديمها.

ب. يتعين على الوحدات أن معرفة متطلباتها من خدمات برامج خدمات البرمجيّات (SaaS) الخاصة بها بدقة والميزات التي ستحتاجها خدمات البرامج. على سبيل المثال، إذا كانت الوحدات ترغب في تحسين التعاون بين الموظفين لتقليل الوقت المستغرق في تنفيذ الخدمة الإلكترونية، فيمكن للوحدات اختيار خدمات برنامج التعاون حيث يكون الموظفون على منصة تعاون واحدة، والتواصل في الوقت الفعلي وحل أي مشكلة بفعالية وكفاءة.

ج. يجب على الوحدات أن تأخذ في الاعتبار اتفاقية مستوى الخدمة التي يجب أن تحدد بوضوح الخدمات التي سيوفرها مقدم خدمات البرمجيّات (SaaS) وأيضًا ما هي العواقب التي ستواجهها إذا فشلت في تقديم هذه الخدمات وفقًا للمعايير المتفق عليها.

د. عند تبني خيار خدمات البرمجيّات (SaaS)، ستدفع الوحدةتكلفة أقل على الأجهزة والبرامج. على سبيل المثال، إذا اختارت الوحدة برنامج "مايكروسوفت أوفيس 365" (Office 365) كحل في السحابة بافتراض أن الوحدة لديها 100 مستخدم فقط. ستدفع الوحدة فقط مقابل عدد (100) ترخيص مستخدم لخدمة "مايكروسوفت أوفيس 365" (Office 365) نشطة في السحابة، وسيتم تقسيم تكلفة صيانة البرنامج المثبت على السحابة بين الوحدات.

ه. سيكون مقدم الخدمة مسؤولاً عن توفير أي ترقيات للبرامج وتصحيحات الأمان ولن تحتاج الوحدات بعد الآن إلى تحمل تكاليف الترقيات وتقليل الاعتماد على الموظفين الفنيين لاختبار الترقيات والتصحيحات والتحقق من سلامتها.

سيكون نموذج خدمات المنصّات السّحابية (PaaS) مفيد للوحدات إذا كانت الوحدات تخطط لتطوير ونشر التطبيقات والخدمات المرتبطة بالتطبيقات السحابية. ويتعين على الوحدات مراعاة ما يلي قبل اختيار خدمات المنصّات السّحابية (PaaS) كنموذج لتقديم خدماتها:

أ. يجب أن يعتمد نموذج اختيار خدمات المنصّات السّحابية (PaaS) الذي تعتمده الوحدات على التطبيقات واستراتيجية الأعمال المُنطبقة لدى تلك الوحدات. فعلى سبيل المثال، يوفر بعض مقدمي خدمات المنصّات السّحابية (PaaS) آليات الاندماج مع الأدوات. ويمكن أن يساعد المستوى العالي من الاندماج في تقليل الوقت اللازم لنشر التطبيقات. كما يجب على الوحدات أيضًا أن تضع في اعتبارها كيفية اندماج تطبيق محدد من خدمات المنصّات السّحابية (PaaS) مع التطبيقات الأخرى وإمكانية مشاركة البيانات.

ب. يجب أن توفر خدمات المنصّـــات السّـــحابية (PaaS) للوحدات خدمات تطوير التطبيقات وقاعدة البيانات والاندماج والدعم وخدمات الأمان. ويجب على الوحدات أن تحدد متطلباتها مقابل كل تطبيق فيما يتعلق بجميع الخدمات المذكورة. فعلى سبيل المثال، إذا احتاج أي منها إلى مساحة تخزين إضافية، فقد تكون الخدمات السحابية الخاصة أفضل خيار متاح للوحدات.

ج. سيتعين على الوحدات أن تحدد نوع خدمات المنصّات السّحابية (PaaS) (المحمولة أو المتكاملة رأسياً) للاختيار من بينها. وتتمثل أفضل الخيارات للهيئات في اختيار منصات خدمات المنصّات السّحابية (PaaS) مفتوحة المصدر. ومن الأمثلة على الأنظمة الأساسية مفتوحة المصدر، (Cloud Foundry) و (OpenShift) و(Stackato) وما إلى ذلك. وتجمع الأنظمة المتكاملة رأسياً بسلاسة بين عروض خدمات البنية الأساسيّة (IaaS) وخدمات المنصّات السّحابية (PaaS) وليست محمولة. يمكن العثور على هذه العروض عادةً على منصات (Azure) وخدمات (AWS).

د. فيما يتعلق بأطر عمل التطوير واللغات التي سيتم دعمها في خدمات المنصّات السّحابية (PaaS)، فمن المهم للوحدات فحص وتحديد لغات وأطر عمل التطوير المدعومة في خدمات المنصّات السّحابية (PaaS).

ه. تمثل التكلفة عامل آخر يجب على الوحدات مراعاته كما هو الحال مع خدمات المنصّات السّحابية (PaaS)، وستحتاج الوحدات إلى تحمل تكاليف تطوير التطبيقات وستتحمل الوحدات مسؤولية تنفيذ أعمال الصيانة المرتبطة بها.

ستكون خدمات البنية الأساسيّة (IaaS) للوحدات مثالية في تقديم الخدمات عند الطلب حيث تكون الشبكة والتخزين والخوادم متاحة للاستخدام. ويجب على الوحدات مراعاة ما يلي قبل اختيار خدمات البنية الأساسيّة (IaaS) كنموذج لتقديم خدماتها.

أ. ستكون خدمات البنية الأساسيّة (IaaS) أفضل خيار للوحدات التي تحتاج إلى تنفيذ الأعمال ذات الأعباء الثقيلة وفي نفس الوقت زيادة الموارد أو خفضها بسرعة وبشكل منتظم.

ب. تفي آليات أمان البنية الاساسية والبيانات التي يوفرها مقدم الخدمة بمعايير الوحدات وتفوقها.

ج. يمكن للوحدات باستخدام خدمات البنية الأساسيّة (IaaS) تبني بنية تحتية موحدة للتعافي من الكوارث (DR) مع تخفيض التكاليف مما يؤدي إلى استرداد سريع دون تعرض البيانات للفقد.

د. بالنسبة للوحدات، تكون تكلفة صيانة المعدات أو استبدالها أقل. ولن تضطر الوحدات إلى القلق بشأن وقت التشغيل إذ سيتحمل مقدم الخدمة المسؤولية عن الاهتمام بوقت التشغيل في حالة فترات تنفيذ الترقيات وأعمال الصيانة.

يتعين على الوحدات إجراء تقييم مدى ملائمة الحوسبة السحابية لأعمالها والذي يجب أن يتضمن تقييم نموذج المعلومات مقابل دوافع ومعوقات (قيود) تبني السحابة وتحديد قابلية تنفيذ الخدمة السحابية.

المؤشرات	معوقات (قيود) تبني السحابة				دوافع تبني السحابة			
	3-	2-	1-	0	1	2	3
قابلية التوسع							
المرونة							
القدرة على التكيف							
الاستراتيجية المالية							
المهارات							
الأمان							

المؤشرات	معوقات (قيود) تبني السحابة				دوافع تبني السحابة			
	3-	2-	1-	0	1	2	3
جهود الاندماج							
استراتيجية الخروج							
التنفيذ العاجل							
مدة المشروع							

الشكل التوضيحي رقم (5) – تقييم مدى ملائمة الحوسبة السحابية

يُظهر الشكل التوضيحي الوارد أعلاه مؤشرات القياس من الرقم (-3) إلى الرقم (3) والتي تتدرج من درجات المعوقات (القيود) الشـــديدة إلى الدوافع الشـــديدة. فإذا كان معدل ترجيح المعوقات (القيود) أعلى من معدل ترجيح الدوافع، فيجب على الوحدات أن تفكر في تجنب بعض أنماط تبني السحابة. على سبيل المثال، من الأفضل تخزين واستخدام البيانات الحساسة على سحابة خاصة. وإذا كان العكس صـــحيحًا وكان معدل ترجيح الدوافع أعلى، فيجب أن تســتمر عملية اختيار الســحابة مع نطاق أوســع من أنماط التبني المحتملة.

كما يتعين على الوحدات اســـتخدام مؤشـــر قياس مدى ملائمة الحلول المتاحة لتقييم الخدمات والتطبيقات المختلفة اللازم تبنيها واختيار نموذج السحابة الأنسب للتطبيقات والخدمات.

التقييم	0 = ضعيف	1 = متوسط	2 = جيد	3 = ممتاز
الوفاء بالمتطلبات	لا تفي بها	تفي بها جزئياً	تفي بها بالكامل	تفوق المتطلبات
الاستبدال	يؤدي اختيار هذه الخدمة أو التطبيق إلى حل تنازلات جوهرية	يؤدي اختيار هذه الخدمة أو التطبيق إلى الاستبدال	لا تنطبق عملية استبدال مع اختيار هذه الخدمة أو التطبيق	لا تنطبق عملية استبدال مع اختيار هذه الخدمة أو التطبيق

الشكل التوضيحي رقم (6) – مؤشر قياس مدى ملائمة الحلول المتاحة

5. القيمة المُقدمة والمخاطر

يستعرض هذا القسم بعض المزايا والتحديات والمخاطر المرتبطة بتبني خدمات الحوسبة السحابية. تساعد الحوسبة السحابية على استبعاد الحاجة إلى استثمارات ضخمة في البنية الاساسية وتوفر نماذج تشغيل مرنة. وسيساعد ذلك الوحدات على تعزيز سرعة تنفيذ الأعمال والقدرة على الاستجابة لمتطلبات السوق. كما أنه نظرًا لما توفره السحابة من مزايا معينة، فهناك أيضًا تحديات ومخاطر مرتبطة بها والتي تم توضيحها في الأقسام الواردة أدناه.

5.1. القيمة المُقدمة

ترد أدناه بعض المزايا الجاذبة التي ستساعد على تبني الوحدات العمانية لنموذج خدمات الحوسبة السحابية:

أ. **المرونة**: تُعد الخدمات المستندة إلى السحابة مثالية للوحدات ذات المتطلبات المتغيرة لتقنية المعلومات، حيث تكون هناك حاجة لتوسيع نطاق أي خدمة أو خفضها، فيمكن ضبطها بمرونة وفقًا للمتطلبات. كما يمكن أن يمنح هذا المستوى من السرعة للوحدات التي تستخدم الحوسبة السحابية ميزة حقيقية لتقديم خدمات جديدة في فترة زمنية قصيرة وبسرعة.

ب. **تقليل النفقات الرأسمالية (CapEx)**: تعمل الحوسبة السحابية على تخفيض التكلفة العالية للأجهزة، حيث تدفع الوحدات فقط مقابل الموارد والخدمات المستخدمة مع سهولة ضبط وتوسيع نطاق الخوادم والخدمات في غضون دقائق.

ج. **استخدام الأصول**: ستعمل الحوسبة السحابية على تعزيز كفاءة استخدام أصول تقنية المعلومات للوحدات، إذ سيساعد هذا على تقليل تكرار المعدات وبذل نفس الجهود من جانب الوحدات والإدارات بقدر كبير، ولن تضطر الوحدات إلى استخدام أصول جديدة في أوقات الذروة متى كان يمكنهم مشاركة التطبيقات والتخزين وطاقة الحوسبة.

د. **التعافي من الكوارث (DR)**: نظرًا لأنه يتعين على الوحدات معالجة الكثير من البيانات العامة والتعامل معها والتي قد تتمتع بالخصوصية والسرية، فإن تبني نظام التعافي من الكوارث (DR) يُعد أمراً بالغ الأهمية. وبالنسبة للوحدات الأصغر التي تفتقر إلى التمويل والموارد والخبرة المطلوبة، فإن حل التعافي من الكوارث (DR) المُثبت على السحابة يُعد خياراً مثاليًا أكثر من الحلول الفعلية، إذ أنه سيتم إجراء عمليات التحول بشكل سريع مما سيعمل على تجنب الحاجة إلى الاستثمارات الكبيرة مع توفير مقدم الخدمة الدعم اللازم على مدار الساعة.

ه. **تحسين الأداء**: يمكن للمنصة السحابية عالية الأداء أن تدعم التطبيقات التي تعتمد على الاستخدام الكثيف للموارد وتساعد أيضًا على تنفيذ اتفاقيات مستوى الخدمة (SLAs) للوحدات داخل عُمان.

1. يمكن للوحدات – من خلال المعالجة الأسرع – تشغيل التطبيقات الهامة في السحابة بشكل أكثر فعالية وموثوقية من حيث التكلفة مع توفير النفقات الرأسمالية والنفقات التشغيلية (OpEx) وفي الوقت نفسه تجنب تكرار استخدام الأصول وتحسين معايير استخدام الأصول.
2. يمكن إدارة البيانات الضخمة وإجراء التحليلات والنمذجة والمحاكاة بكفاءة أكبر بسبب الوصول السريع إلى القرص والذاكرة التخزينية والإنتاجية.

أ. **المعالجة الآلية (الأتمتة)**: ستمكّن المعالجة الآلية (الأتمتة) الوحدات من توفير الموارد القائمة بذاتها (وحدة المعالجة المركزية وذاكرة الوصول العشوائي ومساحة القرص التخزينية وما إلى ذلك) على خادم مما يمكن أن يساعد الوحدات في تنفيذ الخدمات بكفاءة مع الأداء المطلوب ودون أي تدخل.

ب. **تعزيز التعاون**: يمكن تخزين جميع المستندات في مكان واحد مركزي وستكون كل هيئة قادرة على العمل وتحديث المستندات بشكل متزامن. كما ستسمح السحابة للموظفين الاجتماع والتعامل مع المعلومات بشكل افتراضي وبسهولة في الوقت الفعلي مما يؤدي إلى تعزيز التعاون.

يوفر هذا المستند إطار عمل لتبني الحوسبة السحابية مع مزاياها وتحدياتها ومخاطرها. ويمكن الحصول على أي معلومات حول خدمات التعاون من خلال الاطلاع على **النموذج المرجعي الفني.**

ج. **ترقيات الخدمات والموارد:** لن تضطر الوحدات للقلق حول تطبيق تصحيحات الأمان أو ترقيات التطبيقات اللازمة لإدارة أعمالها، إذ سيتم اختبار الترقيات والتصحيحات وإتاحتها للوحدات من مقدم الخدمة بعد إجراء الاختبارات اللازمة.

د. **تقنية المعلومات الصديقة للبيئة (الخضراء):** يمكن للوحدات – باستخدام الحوسبة السحابية – تقليل حجم مراكز البيانات الخاصة بها – أو التخلص من بصمة مركز البيانات الخاصة بها تمامًا. ويمكن أن يؤدي تقليل عدد الخوادم وتكلفة البرامج وعدد موظفي الصيانة إلى تقليل تكاليف تقنية المعلومات بشكل كبير دون التأثير على إمكانيات تقنية المعلومات.

يوفر هذا المستند إطار عمل لتبني الحوسبة السحابية مع مزاياها وتحدياتها ومخاطرها. ويمكن الحصول على أي مرجع بشأن المعايير وأفضل الممارسات المتعلقة بتقنية المعلومات الصديقة للبيئة (الخضراء) من خلال الاطلاع على **النموذج المرجعي الفني** التحديات

تدرك الجهات المعنية في مجال الأعمال وتقنية المعلومات أن الوحدات تولي اهتماماً أكبر حول معايير الأمان وصعوبات قياس معدل العائد على الاستثمار (ROI) وتحديد القيمة الاقتصادية الدقيقة للحل متبوعًا بحوكمة الخدمات المستندة إلى السحابة فيما يتعلق بالمعايير الحكومية والعالمية.

ترد أدناه التحديات النموذجية من منظور جهة حكومية بما في ذلك المخاوف بشأن عمليات الأمان وتحديات الاندماج وإدارة المعلومات.

أ. **جودة الخدمة**: إن اتفاقيات مستوى الخدمة (SLAs) لمقدمي الخدمة ليست مشددة ومناسبة لضمان تنفيذ الخدمات بالمستوى المطلوب من التوافر والأداء والموثوقية. كما أن هناك جوانب معينة يتعين على الوحدات وضعها في الاعتبار ويجب أن يكون مقدم خدمة الحوسبة السحابية قادرًا على الإجابة على النقاط المتعلقة بجودة الخدمة مثل:

1. الحد الأدنى من مستويات الخدمة التي تريدها الوحدة.
2. التدابير التصحيحية المتاحة في حالة حدوث الأعطال.
3. إجراءات التعافي من الكوارث واستمرارية الأعمال.
4. قابلية نقل بيانات الوحدة.
5. عملية إدارة التغيير التي يتبعها مقدم الخدمة.
6. معايير البنية الاساسية والأمان التي يعتمدها مقدم الخدمة.
7. الوقت الذي يستغرقه مقدم الخدمة لتحديد المشكلات وحصرها.
8. عملية التصعيد التي يعتمدها مقدم خدمة الحوسبة السحابية.
9. استراتيجية الخروج المنفذة مع مقدم الخدمة بما في ذلك الأدوار والمسؤوليات.
10. عملية إنهاء العقد المنفذة مع مقدم الخدمة.

ب. **التقيد بمورد محدد:** سيقدم مقدمو الخدمات السحابية الضمانات اللازمة للوحدات حول مرونة استخدامها السحابية ويمكن دمجها بسهولة مع مقدمي الخدمات الآخرين أو مع إمكانات الخدمة الداخلية، ومع ذلك لم يتطور التبديل بين مقدمي الخدمات بشكل كامل. قد تجد الوحدات صعوبة في ترحيل الخدمات من مورد إلى آخر بسبب قابلية التشغيل التبادلي ومشكلات الدعم بين مقدمي الخدمة.

ج. **انقطاع الخدمة وإمكانية الوصول:** سيتعين على الوحدات الوصول إلى الخدمات وبياناتها عبر الاتصال بالإنترنت بدلاً من الاتصال المحلي (الداخلي). لذلك عند وجود عطل في الشبكة أو الاتصال بالإنترنت، فهذا يعني أيضًا تعطل الخدمات السحابية. كما يمكن أن يتأثر أداء البنية الاساسية السحابية بمعدل الاستخدام والبيئة وعدد المستخدمين. ويعد ضمان مرونة البنية الاساسية السحابية في مواجهة الانقطاعات أمرًا جوهرياً للوحدات. ومع أنه سيكون من المستحيل تقريبًا التخفيف من جميع حالات الانقطاع، إلا أنه يجب اختيار مقدم خدمة يتبع إجراءات فعالة ومرنة لحماية البيانات الحكومية.

د. **الاعتمادية على الشبكة**: في حال قررت الوحدات اختيار نموذج اندماج سحابة هجينة، فستتطلب الاعتمادية على الشبكة تصميمًا مدروسًا يتضمن المؤشرات التالية:

1. تأثير زمن الاستجابة (المعروف أيضًا باسم التأخير الزمني) بين البنية الاساسية للسحابة الخاصة والسحابة العامة.
2. تحديد التطبيقات التي تحتاج إلى النطاق الترددي والتي تحتاج إلى جهد أكبر للعمل عبر شبكات واسعة النطاق.
3. عرض النطاق الترددي اللازم لنقل مجموعات البيانات الكبيرة.
4. استخدام آليات حجب عناوين بروتوكول الإنترنت (IP) الموجودة في الشبكة (الطوبولوجيا) الهجينة واستخدام الإصدار السادس من بروتوكول الإنترنت (IPv6) إذا لزم الأمر.
5. استخدام الأجهزة والحلول الأمنية المستخدمة على تقنية المعلومات التقليدية أو السحابة الخاصة في عمليات السحابة العامة.

يوفر هذا المستند إطار عمل لتبني الحوسبة السحابية مع مزاياها وتحدياتها ومخاطرها. ويمكن الحصول على أي مرجع حول التبنية على الشبكة من خلال الاطلاع على **نموذج المرجع الفني.**

ه. **التحول إلى خدمات الحوسبة السحابية:** يعد التحول إلى خدمات الحوسبة السحابية عملية معقدة وشاملة، ويجب على الوحدات التأكد من أن الحل المقترح يدعم ويكمل نموذج أعمالها. كما أنه يتعين على الوحدات أن تضع في اعتبارها بعض الجوانب المحددة التي قد يرغب مقدم الخدمة السحابية في معرفتها.

1. أنماط الطلب على الخدمات.
2. أكبر معدل لتدفق البيانات لأي وحدة.
3. زيادة حجم البيانات على أساس سنوي للوحدات.
4. القيود المفروضة على الوحدات فيما يتعلق بمواقع البيانات.
5. ضوابط التحكم في البيانات المطلوبة من الوحدات.
6. توقعات الوحدات فيما يتعلق باتفاقيات مستوى الخدمة (SLAs).

و. **إدارة النظام:** يمكن أن تشكل إدارة دورة حياة الأنظمة السحابية الهجينة تحديًا إذا تم إجراؤها بشكل غير صحيح وتحتاج الوحدات إلى الاستعداد التام لفهم وتحقيق ما يلي:

1. إدارة عمليات ضبط التهيئة الفعالة عندما يتم توفير موارد البنية الاساسية في الخدمة الذاتية عبر البيئات.
2. تحقيق معايير الأمان وتصحيح بيئات متعددة.
3. تتغير طبيعة تخطيط السعة عند التعامل مع مجموعات الموارد المرنة.
4. تنفيذ عمليات مراقبة متكاملة وفعالة في السحابة الهجينة.

يوفر هذا المستند إطار عمل لتبني الحوسبة السحابية مع مزاياها وتحدياتها ومخاطرها. ويمكن الحصول على أي مرجع حول الاعتمادية على الشبكة من خلال الاطلاع على السياسات الواردة في **النموذج المرجعي الفني.**

5.2. المخاطر

مع كل اعتماد للتكنولوجيا هناك بعض المعوقات التي قد تنشأ من عوامل معروفة وغير معروفة. وترد أدناه المخاطر المرتبطة بتبني السحابة.

أ. **الأمان والخصوصية:** عادةً ما تكون معايير أمان البيانات والمعلومات في السحابة عند المستويات المثلى، ويمكن الاعتماد عليه بشكل عام وكفاءة. ويمتثل كل من مقدمي الخدمات السحابية العامة والخاصة إلى معايير مختلفة، ومع ذلك قد تعتمد الوحدات عمليات تحجيم أكثر عند تسليم البيانات المهمة إلى مقدم خدمة خارجي إذ أنهم يتعاملون مع البيانات المقيدة والسرية، ويمكن تخزين البيانات المتاحة على السحابة ونسخها احتياطيًا في أي مكان في جميع أنحاء العالم. ويتعين على الوحدات الأخذ في اعتبارها بعض الجوانب الأمنية ومن أمثلتها:

1. موقع البيانات على السحابة.
2. أمان وتشفير البيانات.
3. سياسات الأمان والحوكمة لمقدم الخدمة السحابية.
4. تحكم الوحدات في بياناتها وبيئتها.
5. الوقت المستغرق لنسخ بيانات الهيئة احتياطيًا على السحابة.
6. إجراءات تدقيق البيانات لمقدم الخدمة.
7. استعادة البيانات في حالة تلفها.
8. إجراءات استخراج البيانات للوحدات إذا كانت الخدمة بحاجة إلى النقل داخليًا أو إلى أي مقدم خدمة سحابية آخر.

بينما يوفر هذا المستند إرشادات نحو تبني الحوسبة السحابية مع المزايا والتحديات والمخاطر المرتبطة بها، إلا أنه يجب الاطلاع على **إدارة أمن المعلومات** لمعرفة السياسات الخاصة بالمعلومات وأمانها.

ب. **التحكم المحدود:** نظرًا لأن البنية الاساسية السحابية، في السحابة العامة، مملوكة ومُدارة ومُراقبة بالكامل من مقدم الخدمة، فيجوز منح الوحدات صلاحية التحكم بأدنى حد. كما يمكن للوحدات فقط التحكم وإدارة التطبيقات والبيانات والخدمات الرئيسية المُنفذة، وليس البنية الاساسية الخلفية نفسها. وسيتعين على الوحدات الموافقة على سياسات الحوكمة والامتثال والإدارة الخاصة بمقدم الخدمة.

بينما يوفر هذا المستند إرشادات نحو تبني الحوسبة السحابية مع المزايا والتحديات والمخاطر المرتبطة بها، إلا أنه يجب الاطلاع على **إدارة أمن المعلومات** لمعرفة السياسات الخاصة بالمعلومات وأمانها.

ج. **موقع تخزين البيانات:** يقوم معظم مقدمي الخدمات بتخزين البيانات أو نسخة من البيانات في موقع جغرافي مختلف، غير الموقع الأساسي وذلك للتعافي من الأحداث الأمنية أو الكوارث. تحتاج الوحدات في عمان إلى مراعاة ما يلي:

1. الشروط المتعلقة بملكية البيانات وإمكانية الوصول إليها والخصوصية والأمان.
2. القرارات الصادرة بشأن تخزين ونقل البيانات إلى نموذج سحابة مختلف.
3. تأثر التطبيق وتصنيف البيانات والخصوصية والأمان الأخرى ذات الصلة.
4. الإطار التنظيمي والقانوني للولاية القضائية ذات الصلة باستضافة البيانات.

بينما يوفر هذا المستند إرشادات نحو تبني الحوسبة السحابية مع المزايا والتحديات والمخاطر المرتبطة بها، إلا أنه يجب الاطلاع على **إدارة أمن المعلومات** لمعرفة السياسات الخاصة بالمعلومات وأمانها.

د. **قابلية التشغيل التبادلي والتوافق:** في حال قررت أي وحدة الاستعانة بمقدم خدمة سحابية مختلف أو ربما نظام داخلي مختلف تابع لها، فقد تكون هناك احتمالات بأن الحلول المختلفة تعتمد على حزمة مختلفة من البنية الاساسية والبرامج. ويشكل هذا خطرًا عند النظر فيما إذا كان سيتم استخدام عمليات إدارة التغيير نفسها عبر السحابة الهجينة، أم أن كل واحدة منها فريدة وسيم تحديد ذلك الأمر اعتمادًا على مقدم الخدمة.

ه. **اللوائح القانونية:** يعد امتثال الوحدات للمعايير التنظيمية والقانونية أمرًا مهمًا للغاية. ويتحمل مقدم الخدمات السحابية والوحدات مسؤولية الالتزام باللوائح القانونية. عندما تتبنى أي وحدة نموذج سحابي وتنشره، فهناك بعض المشكلات التي يجب على الوحدة مراعاتها في جميع مراحل العملية التعاقدية وهي على النحو التالي.

1. العناية الواجبة الأولية.
2. التفاوض حول بنود العقد.
3. التطبيق.
4. إنهاء أو فسخ العقد (بانقضاء المدة المحددة أو الفسخ في الحالات غير الاعتيادية).
5. التحول إلى مورد خدمة آخر.

بينما يوفر هذا المستند إرشادات نحو تبني الحوسبة السحابية مع المزايا والتحديات والمخاطر المرتبطة بها، إلا أنه يجب الاطلاع على **إدارة أمن المعلومات** لمعرفة السياسات الخاصة بالمعلومات وأمانها.

5.3. مقارنة تقنية المعلومات التقليدية مع خدمات الحوسبة السحابية

إن تبني السحابة له مزاياه الخاصة عند مقارنته بنهج مركز البيانات التقليدي. وقد تقوم الوحدات بتقييم مزايا تبني الحوسبة السحابية مقابل النهج التقليدي من خلال إجراء تقييمات الجدوى، وتحليل التكاليف والمزايا، وما إلى ذلك. كما تحتاج الوحدات إلى مراعاة ما يلي:

أ. سيلزم الدخول في استثمارات ضخمة مقدماً للحصول على مركز بيانات وسيتطلب قوى عاملة ماهرة لإدارة وصيانة الخدمات المستضافة.

ب. الحاجة إلى توفير الطاقة اللازمة للحفاظ على أجهزة تقديم الخدمات قيد التشغيل مع توفير نظام نسخ احتياطي عبر مصدر بديل، وذلك بخلاف رفوف وحدات تخزين البيانات ومجموعة الأجهزة المتاحة بمركز البيانات.

ج. توفير نظام تبريد فعال للحفاظ على البنية الاساسية وتشغيلها بدون التعرض لمخاطر سخونة أجهزة حفظ وتشغيل الخدمات وكذلك الوفاء بمتطلبات توافر توصيلات حفظ الكابلات والأسلاك.

د. يلزم دائمًا توفير مساحة تخزين أكبر مع الحاجة المتزايدة والطلب المتزايد على الخدمات.

ه. بالإضافة إلى ذلك، سيتعين على الوحدات شراء مكونات البنية الاساسية اللازمة للشبكة والخادم والتخزين والحفاظ عليها مُحدثة بأحدث الترقيات والتصحيحات، وكذلك تعيين أو الاستعانة بمصادر خارجية لتعيين موظفي الإدارة والصيانة. بالإضافة إلى ذلك، سيتطلب شراء وتصميم الخدمات تكاليف ترخيص اعتمادًا على عدد المستخدمين، وتستمر هذه التكلفة في الزيادة مع زيادة عدد المستخدمين وقدرات الخدمة. وستكون هناك تكاليف مرتبطة بأدوات المراقبة والإدارة مع متطلبات الموظفين المهرة لرصد وإدارة توافر الخدمات وفقًا لاحتياجات الوقت المستهدف لاسترداد البيانات (RTO) ونقطة الاسترجاع المستهدفة (RPO).

و. تُعد تحديثات تقنية المعلومات ممارسة كبرى أخرى يتعين على الوحدات متابعتها على مدار فترة زمنية حيث ستنتهي صلاحية الحلول والخدمات والمنتجات وستتوقف الشركات المصنعة للمعدات الأصلية عن إصدار الترقيات وتصحيحات الأمان المتعلقة بها.

يعرض الشكل التوضيحي الوارد أدناه مقارنة بين تقنية المعلومات التقليدية ونموذج خدمة السحابة.

المؤشرات	الإيضاح	تقنية المعلومات التقليدية	السحابة
جهود مراقبة وإدارة تقنية المعلومات	تشير إلى مستوى المعالجة الآلية (الأتمتة) لمراقبة المعدات	جهد يدوي مرتفع على الرغم من توافر الأدوات	تم تخفيضها بشكل كبير بسبب أدوات الإدارة والمراقبة السحابية. تتيح معدل عائد استثمار أسرع وتخفيض النفقات التشغيلية (OpEx)
النفقات الرأسمالية (CapEx)	التكلفة التي تُسدد لمرة واحدة اللازمة لإعداد مركز البيانات والبنية الاساسية لتقنية المعلومات	البنية الاساسية المخصصة تكاليف أعلى	هناك حاجة إلى النفقات الرأسمالية (CapEx) لإنشاء سحابة مؤسسية. يُظهر رد المبالغ المدفوعة على أساس الاستخدام المراقب لتطبيقات الحوسبة والتخزين والشبكة عائد الاستثمار أسرع واسترداد الاستثمار السحابي عبر رد المبالغ المدفوعة
النفقات التشغيلية (OpEx)	تشير إلى النفقات التشغيلية المطلوبة على مدى فترة زمنية، ربما على مدى من 3 إلى 5 سنوات	أعلى نتيجة عدد معادل الدوام الكامل (FTEs) والطاقة والتبريد وما إلى ذلك.	تم تخفيضها بالمقارنة بتقنية المعلومات التقليدية بسبب المحاكاة الافتراضية والمعالجة الآلية (الأتمتة)، والآلات الافتراضية (VMs) هي "فانيلا" واستعادة الخدمة عن طريق إعادة نشر نظام التشغيل (O/S)، إدارة أسهل للأصول، والنفقات التشغيلية (OpEx) مخفض

المؤشرات	الإيضاح	تقنية المعلومات التقليدية	السحابة
الاستخدام	يشير الاستخدام إلى مقدار موارد تقنية المعلومات التي يتم استهلاكها في أي وقت	عادة تتراوح من 5 إلى 20٪	يتم الاستفادة منها على النحو الأمثل (عادة تتراوح من 60 إلى 70٪). يمكن إعادة توزيع الموارد من أنواع المجموعات الأخرى، مما يقلل من متطلبات البنية الاساسية الإجمالية. وانخفاض النفقات التشغيلية (OpEx)، وتحقيق المقياس المالي لآخر اثني عشر شهرًا (TTM) بشكل أسرع، وسرعة تنفيذ الأعمال بشكل أكبر
الإتاحة	الإتاحة هي وقت التشغيل المطلوب للمعدات والخدمات وفقًا للاتفاقيات	يمكن أن توفر إتاحة مجموعة الخدمات نسبة 99.9٪ ولكن بتكلفة مضاعفة	يتم توسيع نطاق التطبيقات المناسبة أفقيًا باستخدام معاملات قابلة لإعادة التشغيل مما يعني صفر وقت تعطل أسرع، وانخفاض النفقات التشغيلية (OpEx)
المرونة	الدرجة التي يمكن بها زيادة أو تقليل سعة النظام حسب الحاجة	توسيع نطاق العمل أو خفضه هو ممارسة مخطط لها يعتمد على عمليات الشراء	تتم عملية توسيع نطاق العمل أو خفضه تلقائيًا عند الطلب ويتم توفير الخدمات اللازمة لمعدلات الارتفاع اللانهائية من الناحية النظرية عند الطلب بواسطة السحابة (التدفق السحابي)
قابلية التوسع	قدرة النظام على زيادة حجم الأعمال على موارد أجهزته الحالية	حجم الحمل الأقصى في البداية. تغيير الحجم معقدة.	التحجيم التلقائي عند الطلب كأجهزة في مجموعة السحابة المخصصة عند الطلب، وانخفاض النفقات التشغيلية (OpEx)، وتخفض عمليات تخطيط السعة لمتوسط الأحمال من النفقات الرأسمالية (CapEx)

الشكل التوضيحي رقم (7) – مقارنة تقنية المعلومات التقليدية مع خدمات الحوسبة السحابية

5.4. أصحاب المصلحة والأدوار والمسؤوليات

سيلعب أصحاب المصلحة دور من منظور الأعمال أو التكنولوجيا أو الاجراءات في توجيه الوحدات نحو تبني إطار العمل هذا، وذلك لاعتماد تبني الحوسبة السحابية ولتوفير التوجيه المستقبلي داخل الوحدات.

سيكون رئيس إدارة تقنية المعلومات في الوحدات مسؤولاً – على سبيل المثال لا الحصر – عن النقاط التالية:

أ. المراجعة الاستراتيجية للإطار بما يتماشى مع احتياجات أصحاب المصلحة المختلفين داخل الوحدات ومواءمته مع المهام الرئيسية للوحدات.

ب. العمل مع الجهات الراعية لإدارة الميزانية وعمليات التمويل المرتبطة بها، ومراجعتها على فترات مناسبة.

ج. الإشراف على تبني إطار العمل وما يرتبط به من تحديات ومخاطر ومدخلات من أصحاب المصلحة.

سيكون مهندسو تقنية المعلومات في الوحدات مسؤولين عما يلي:

أ. تقييم معدل نضج تقنية المعلومات الحالية بما في ذلك مركز البيانات والتطبيقات والتكنولوجيا.

ب. تحديد نموذج الحوكمة لتبني السحابة ولضمان الامتثال للمعايير واللوائح.

ج. وضع خطة لتبني الحوسبة السحابية.

5.5. التداعيات القانونية لتبني السحابة

يتعين على الوحدات ومقدمي الخدمات السحابية الالتزام بالقوانين واللوائح والصلاحيات لحماية البيانات وأمن المعلومات. كما يتعين على الوحدات التأكد من أن مقدمي الخدمات السحابية قد تبنوا تدابير فنية ومادية وإدارية معقولة من أجل حماية بيانات الوحدات من الضياع أو سوء الاستخدام أو أي تغيير.

ترد أدناه بعض اعتبارات الخصوصية وحماية البيانات الرئيسية في بيئة الحوسبة السحابية وهي:

أ. سيكون للوحدات العمانية سياساتها الخاصة لأمن البيانات وإدارة الوصول. ويجب أن تكون سياسات مقدم الخدمة السحابية متوافقة مع سياسات الوحدات.

ب. بالنسبة للوحدات الحكومية في السلطنة، فإن موقع البيانات له أهمية قصوى. في أي حال، يجب أن تظل البيانات أو أي نسخة أو نسخة احتياطية ضمن الحدود القانونية المنطبقة في سلطنة عُمان.

ج. في حالة تعرض الوحدة إلى هجوم يؤدي إلى فقدان بياناتها، فيجب أن تكون هناك إجراءات موثقة حول كيفية استرداد مقدم الخدمة للبيانات المفقودة.

د. سيتعين على مقدم الخدمات السحابية الالتزام بمعايير الاحتفاظ بالبيانات المختلفة والالتزامات المتعلقة بتسريب البيانات وتلفها – البيانات المتاحة عبر الإنترنت وغير المتصلة بالإنترنت، وذلك بموجب الاختصاص القضائي العماني.

ه. يجب ألا يتم استبدال مقدم الخدمة السحابية ويجب ألا تتغير – في المستقبل – أي متطلبات قانونية وتنظيمية بشأن معايير تشفير البيانات لتعزيز أمان البيانات الموجودة في السحابة.

و. يجب على مقدم الخدمة الامتثال لالتزامات الرقابة المتزايدة إذا تم تغيير القوانين المعمول بها في سلطنة عُمان في أي وقت.

ز. يجب أن يسمح مقدم الخدمة بمشاركة سياساته الأمنية وفي نفس الوقت يجب عليه الخضوع لإجراء عمليات التدقيق الخارجية ومشاركة تقارير التدقيق الداخلي إذا لزم الأمر.

ح. قد تطلب الوحدات من مقدم الخدمة تنفيذ المعايير الوطنية، والتي قد تختلف تفاصيلها بشكل طفيف.

ط. يجب على مقدم الخدمة تحديد ما إذا كانت الوحدات ستفقد السيطرة على بيئة السحابة وإلى أي مدى.

ي. يجب أن يكون مقدم الخدمة على اطلاع دائم بعملية إدارة التغيير للوحدات، وإذا لزم الأمر، يجب تحديث عملية إدارة التغيير ومشاركتها.

ك. يجب – في حالة حدوث مخالفة – أن يكون هناك أحكام منطبقة حول مسؤولية مقدم الخدمة والاستجابة الاستباقية للوحدات وكذلك قيام مقدم الخدمة بدفع التعويضات عن حالات عدم الامتثال.

ل. قد تطلب الوحدات من مقدم الخدمة استيفاء شروط ضمان تعهدات التنفيذ حتى يصبح العقد متاحًا على نموذج ورقي.

م. سوف تطلب الوحدات تنبيهات (عبر البريد الإلكتروني أو الرسائل النصية أو المكالمات الهاتفية) بشأن حالات تعطل الأعمال والانتهاكات، وتقارير حول توافر الخدمة على أساس شهري. كما سيبذل مقدم الخدمة السحابية قصارى جهده لإتاحة الخدمات في أقرب وقت ممكن، وذلك في حالة القوة القاهرة.

ن. ستحتاج الوحدات إلى معرفة ما إذا كان مقدم الخدمة قد تعاقد مع أي جهة خارجية حول أعمال الصيانة المتعلقة بالخدمات وتقديم الدعم.

س. قد ترغب أي وحدة في أي وقت أو في وقت توقيع اتفاقية في معرفة مجموعة مهارات موظفي مقدم الخدمات السحابية وقد ترغب في إجراء عمليات التحقق من السير الذاتية (الخلفية) للموظفين التابعين لمقدمي الخدمات الذين يقدمون الدعم للوحدات.

ع. يجب أن تدرك الوحدات ما إذا كان مقدم الخدمة السحابية لديه القدرة على تغيير شروط العقد والرسوم وهيكل الأسعار دون إشعار مسبق.

ف. يجب أن تطلع الوحدات على الوصف الواضح للخدمة السحابية والذي يجب أن يتضمن نوع الخدمة المقدمة والوظائف وما إذا كان سيتم تطوير الخدمات خلال مدة سريان العقد أم لا. وسيساعد هذا الأمر الوحدات على تحديد اتفاقيات مستوى الخدمة (SLAs).

ص. سترغب الوحدات في تقييد الوصول إلى بياناتها واستخدامها من مقدم الخدمة السحابية والجهات الخارجية التابعة له ما لم وحتى يتم تنفيذ عملية الموافقة المناسبة.

ق. يجب إبلاغ الوحدات مسبقًا قبل انتهاء مدة سريان العقد وكذلك توضيح الشروط التي بموجبها يمكن إنهاء العقد أو تمديده.

ر. تمتلك الوحدة الحق في معرفة ما سيحدث للبيانات، في حالة إنهاء (فسخ) العقد. وكذلك يتم إبلاغ الهيئة عن كيفية استرجاعها للبيانات وبأي صيغة وشكل. ويجب أن يكون مقدم الخدمة داعمًا للوحدة فيما يتعلق بالاحتفاظ بالبيانات لفترة زمنية مطلوبة، وذلك خلال الفترة الانتقالية.

6. إرشادات حول الجاهزية وقابلية تبني خدمات الحوسبة السحابية

يمثل نمط (مفهوم) الحوسبة السحابية عملية التحول في تقديم الخدمات، إذ إنه يتم تقديم الخدمات المستضافة عبر الإنترنت مع التشجيع على الابتكار في مجال الأعمال والتمتع بمزايا التكلفة. وستساعد الحوسبة السحابية الوحدات على تعزيز مرونة تنفيذ أعمالها على الرغم من توافر مستودعات تخزين البيانات الموجودة على الخادم. كما ستكون الوحدات قادرة على توفير الدعم لعملياتها ذات المهام الحرجة من خلال نشر الخدمات السحابية السريعة والابتكارية التي تتيح استخدام التقنيات الاجتماعية والمتنقلة والتحليلية مع الامتثال الصارم وتدابير الأمان لعدم الكشف عن أمن البيانات.

وترد أدناه بعض المجالات الرئيسية التي ستتمكن الوحدات من التركيز عليها من خلال تبني السحابة، وهي:

أ. توحيد خدمات تقنية المعلومات.

ب. الخدمات المشتركة.

ج. الخدمات المُقدمة للمواطنين.

سيشتمل توحيد خدمات تقنية المعلومات على إنشاء وحدة مركزية تجمع بين عدة مراكز بيانات منتشرة عبر الوحدات المختلفة. ويجب تقييم كل مركز بيانات من حيث التكلفة والتطبيقات وقابلية دمج الخادم والمحاكاة الافتراضية للخدمات.

ستمتلك الوحدات خدمات وتطبيقات وقواعد بيانات وبوابات وما إلى ذلك والتي قد تكون مشتركة بين الإدارات. وستقدم الخدمات المشتركة الدعم اللازم للوحدات للتقليل من حالات عدم اليقين المالي، وتوفير النظم الاقتصادية الموفرة للمال وإتاحة فرص لطرح خدمات جديدة تتيح توفير الخدمات إلى المواطنين والشركات بسرعة أكثر.

يمكن تقديم خدمات المواطنين مثل توفير مساحة تخزين المستندات الرقمية وخدمات التصديق عبر الإنترنت وعمليات تسجيل المواليد وما إلى ذلك على السحابة. كما يمكن إعداد خادم جديد يقدم هذه الخدمات في غضون دقائق في السحابة دون أي تدخل يدوي.

يلزم على الوحدات تحديد وتصنيف التطبيقات على النحو التالي حتى يتم ترشيحها لتبني السحابة على النحو الملائم:

أ. المشتركة: التطبيقات المشتركة عبر جميع الوحدات مثل البوابات وإدارة الموارد البشرية ونظم تخزين البيانات وما إلى ذلك.

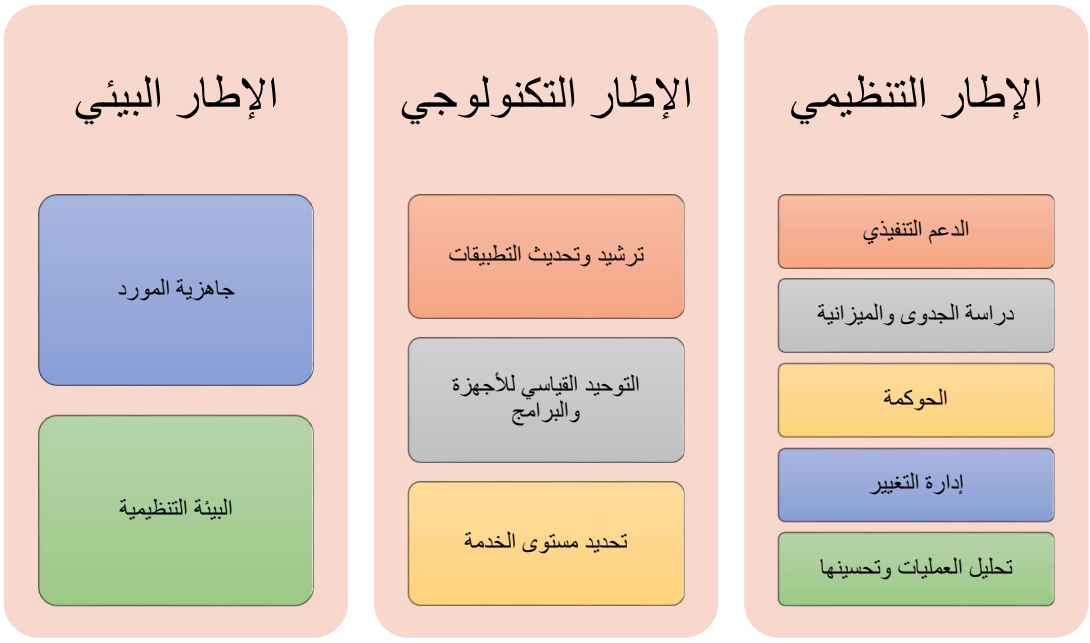
ب. المجموعة: يمكن أن تكون التطبيقات مثل التعليم وإدارة المعلومات الصحية وإدارة متطلبات تقنية المعلومات ترشيحات مناسبة ليتم استخدامها كتطبيقات على مستوى المجموعات وقابلة للتنفيذ على السحابة.

ج. الإدارة: يمكن تعميم التطبيقات التي قد تكون شائعة عبر عدد قليل من الإدارات وتكون مناسبة وقابلة للتنفيذ على السحابة مثل قطاعات الشرطة والنيابة العامة والبلديات، وما إلى ذلك.

تستند المبادئ التوجيهية لتبني الخدمات السحابية على إطار عمل المجالات التكنولوجية والتنظيمية والبيئية (TOE) الذي يصف العوامل التي تؤثر على تبني الخدمات التكنولوجية واحتمالية حدوثها.

6.1. إرشادات حول الجاهزية

يعد تبني السحابة تحولًا جذريًا عن طريقة استخدام التكنولوجيا وسيتطلب دعمًا واستعدادًا من أعلى مستوى من أصحاب المصلحة الذين يتم إبلاغهم وإعداد دراسة الجدوى والعثور على راع. ويرد أدناه العناصر الرئيسية للجاهزية في مختلف مراحل تبني الخدمات السحابية.



الشكل التوضيحي رقم (8) – عناصر الجاهزية لتبني الخدمات السحابية

6.1.1. الإطار التنظيمي

تركز الوحدات – من المنظور المؤسسي – على مفهوم الانفتاح على الابتكار والعمليات التي تلائم إجراءات التغيير باعتبارها عوامل أساسية لتبني الخدمات السحابية.

أ. **الدعم التنفيذي**: ستحتاج الوحدات إلى مشاركة عميقة في مهام الأعمال وفحص دقيق للوضع التكنولوجي الحالي من أجل التبني الناجح للحوسبة السحابية. وقد يتطلب ذلك دعمًا تنفيذيًا على مستويات مختلفة داخل الوحدات وفيما بينها لإنشاء أهداف البرنامج، ومواكبة خطة التبني، وتوفير الإشراف على مستوى مستدام.

ب. **دراسة الجدوى والميزانية**: سوف يرتبط تبني الخدمات السحابية بالعديد من البرامج والخطوات الأخرى التي تتطلب إعداد دراسة جدوى. ويجب تحديد أهداف العمل لجميع الوحدات بوضوح مع الاستثمارات المستقبلية المطلوبة والضرورية.

ج. **الحوكمة**: ستكون حوكمة تبني السحابة بالكامل والبرامج والخطوات المرتبطة بها مهمة من منظور الوحدات لتجنب تجاوز الوقت والتكلفة. كما سيحتاج برنامج السحابة إلى مزيج من إدارة الأعمال وتقنية المعلومات لتبنيه على نحو فعال وناجح. وقد تحتاج الوحدات إلى إعادة تنظيم منظومة الحوكمة الخاصة بها لتبني الخدمات السحابية أو تشكيل فريق حوكمة مستقل.

د. **إدارة التغيير**: سيتعين على الوحدات إجراء تغيير داخل منظومة تقنية المعلومات الخاصة بهم وذلك مع تبني الخدمات السحابية. ويمكن أن تكون هذه التغييرات شاملة بطبيعتها تتطلب تدخلًا متكررًا ومتعدد الأوجه ومستدامًا اعتمادًا على طبيعة عمليات تبني الخدمات السحابية. ويتعين على الوحدات أن تكون مستعدة لخوض هذا التحول الثقافي.

ه. **تحليل العمليات وتحسينها**: ستستفيد منظومة تقنية المعلومات التابعة للهيئات من الانتقال إلى الخدمات السحابية. وستكون أكبر استفادة من اختيار خدمات البرمجيّات (SaaS) حيث سيؤدي تحليل العمليات والتحسينات إلى مواءمة العمليات التجارية مع التغييرات التي تطرأ على تطبيقات البرامج والخدمات، وبالتالي تمكن العمليات التجارية من الاستفادة المثلى من القدرات التي توفرها التطبيقات.

6.1.2. الإطار التكنولوجي

ستحتاج الوحدات إلى التركيز على التقنيات الداخلية والتقنيات السحابية والحلول المتاحة في السوق. ستعتمد عملية تبني السحابة – داخليًا – على موظفين أكفاء يمكنهم إدارة بنية تحتية تقنية مناسبة ولديهم الدراية الكافية بالأعمال التجارية الإلكترونية. بينما يعُد توافر تقنيات الأعمال التجارية الإلكترونية أمرًا ضروريًا على الصعيد الخارجي.

أ. **ترشيد وتحديث التطبيقات**: من شأن الانتقال إلى السحابة – بالنسبة للوحدات – أن يسمح لهم بتقييم وضع تطبيقاتهم، وفهم مزايا التطبيقات وإجراء عملية تنظيف. ويعد تحديث مجموعة التطبيقات جانبًا مهمًا للانتقال إلى السحابة حيث سيساعد في ترشيد استخدام مجموعة التطبيقات وتجنب وجود نظامين – السحابة والبيئة القديمة. وسيكون الحفاظ على هذين النظامين أمراً مكلفًا. كما يجب بالنشبة لأي هيئة أن يكون التحديث والانتقال إلى السحابة وفقًا لمعاييرها المتوقعة.

ب. **التوحيد القياسي للأجهزة والبرامج**: عندما ترغب أي وحدة في تبني خدمات الحوسبة السحابية، فإن أول خطوة يلزم عليها اتباعها هي تعزيز بنيتها الاساسية وأنظمتها وبرامجها. وستحتاج كل وحدة بعد ذلك إلى تطوير معاييرها. كما ستحتاج كل وحدة – لتبني السحابة – إلى تطبيق معايير من شأنها أن تكون مدفوعة بمجموعة من المبادرات الهندسية والتي ستخضع بدورها لعملية تحول خلال عمليات تبني الخدمات السحابية. وستتمكن كل هيئة من تحقيق المرونة وسرعة تنفيذ الأعمال إلى أن تصل إلى المرحلة التي لا يتم خلالها تجاوز الحد المسموح به لتنفيذ عمليات التوحيد القياسي. وسيكون التوحيد القياسي للأجهزة والبرامج دافعاً مهمًا لمعظم مزايا الخدمات السحابية وستحتاج كل هيئة لتحقيق التوازن بين أولوياتها الحالية والتطلعات المستقبلية.

يوفر هذا المستند إطار عمل لتبني الحوسبة السحابية مع مزاياها وتحدياتها ومخاطرها. ويمكن الحصول على أي مرجع حول معايير الأجهزة والبرامج من خلال الاطلاع على **النموذج المرجعي الفني.**

ج. **تحديد مستوى الخدمة**: سيتم تقديم المتطلبات التقنية للوحدات بناءً على خدمات الحوسبة السحابة المناسبة. وستحدد مستويات الخدمة متطلبات الوحدة فيما يتعلق بالخدمة. وبالنسبة لمنظومة تقنية المعلومات التابعة للوحدات، فستكون بمثابة مقياس لمؤشرات الأداء الرئيسية (KPIs).

6.1.3. الإطار البيئي

يشتمل الإطار البيئي على جاهزية المورد لتقديم الخدمات السحابية، والمنافسين في مجال الخدمات السحابية في السوق، والإطار الاقتصاد الكلي (الشامل)، والبيئة التنظيمية.

أ. **جاهزية المورد**: يتعين على أي وحدة ترغب في تبني نموذج سحابي أن تأخذ في الاعتبار مدى جاهزية الموردين الذين قد يكونون أو لا يكونون جزءًا من اعتباراتهم في المعاملات السابقة. كما ستحتاج الوحدة أيضًا إلى النظر في الحلول التي تعتبر معايير مفتوحة المصدر. وستؤثر جاهزية المورد على تبني السحابة إلى حد كبير وعند التبديل بين مقدمي الخدمات السحابية.

ب. **البيئة التنظيمية**: يمكن للبيئة التنظيمية أن تعزز أو تبطئ من عملية تبني الخدمات السحابية وتحويلها. كما يمكن للوائح الحكومية والعالمية أن تفرض آليات لتخصيص الموارد لتحقيق معايير الامتثال المرجوة.

6.2. إرشادات تبني الخدمات السحابية

تخضع عملية تبني الخدمات السحابية المناسبة، بالنسبة للوحدات التي تتطلع إلى تبني الخدمات السحابية أو في طور تبني الخدمات السحابية، إلى معالم رئيسية محددة. ويجب أن تخضع أي وحدة تعتمد الخدمات السحابية لإحدى مراحل هذه المعالم الرئيسية. ويتم تنفيذ هذه المعالم الرئيسية بطريقة تقدمية (تدريجية) بطبيعتها، إذ تؤدي إحداها إلى أخرى وتشير المرحلة النهائية إلى الحل المناسب لتبني الخدمة السحابية المستضافة. وتختلف هذه المعالم الرئيسية بالتأكيد باختلاف الطريقة التي ستحدد بها الوحدات برامجها السحابية.

6.2.1. الإطار التنظيمي

أ. **عمليات طلب تقديم العروض والمناقصات**: اعتمادًا على حجم الوحدة – عادة ما تخضع الوحدات الكبيرة إلى عملية طلب تقديم العروض لتوضيح أهداف الوحدة ومتطلباتها للشركاء الخارجيين وتحديد المنظمات لتقديم الاستشارات بشأن الخدمات السحابية وتنفيذ الأعمال وتقديم خدمات الدعم ذات الصلة بالخدمات السحابية. وتكون عملية طلب تقديم العروض فرصة تعريفية لكل من الشركاء الخارجيين والوحدة وستساعد في تحديد النقاط التي تحدد مستوى الخدمة والتوقعات العامة من برنامج تبني الخدمات السحابية.

6.2.2. الإطار التكنولوجي

أ. **إثبات المفهوم (POC)**: سيساعد إثبات المفهوم في معرفة الخدمات السحابية التي سيتم تبنيها ونشرها، كما سيساعد على الاندماج بين طبقات الخدمات السحابية المختلفة وسيوفر مدخلات لاختيار التقنيات المناسبة. ويعد إثبات المفهوم جانبًا مهمًا يجب على أي وحدة مراعاته إذ أن العديد من الأدوات المستخدمة في الخدمات السحابية تعتمد على المصدر المفتوح وقد تستخدم منظومة تقنية المعلومات التابعة للهيئة هذه الأداة لأول مرة.

ب. **اختيار الموردين**: ستساعد المدخلات المتحصل عليها من مرحلتي "طلب تقديم العروض" (RFP) و"إثبات المفهوم" (PoC) الوحدات في تحديد الشركاء الملائمين لتنفيذ الخدمات السحابية. ويمكن لهؤلاء الشركاء تقديم الاستشارات السحابية وخدمات ترشيد التطبيقات وصيانة البنية الاساسية وأدوات وتقنيات السحابة وإدارة التغيير. ويتعين على الوحدات – في هذه المرحلة – أن تشدد على خياراتها الخاصة بتقنيات السحابة التي سيتم نشرها والشريك الذي سينفذ استراتيجية النشر.

ج. **نموذج الخدمة السحابية**: سيتم تقديم نماذج خدمة سحابية متنوعة للوحدات خلال هذه المرحلة من العملية. ويجوز للوحدات أن تقرر اختيار أي من نماذج الخدمات السحابية مباشرة من خدمات البنية الأساسيّة (IaaS) وخدمات المنصّات السّحابية (PaaS) وخدمات البرمجيّات (SaaS) وأي من النماذج السحابية المدمجة تبنيا على مدى النضج والحاجة إلى الحوكمة والتحكم.

1. قد تختار وحدة أكبر أو أكثر نضجًا خدمات البنية الأساسيّة (IaaS) كخدمة للتحكم في معايير البرامج الخاصة بها وتعيينها ونشرها وفقًا للطلب والمتطلبات المستقبلية.
2. بينما قد تكون خدمات سطح المكتب (DaaS) نموذجًا مناسبًا للهيئات الأخرى، إذ أنه يوفر تطبيقًا مركزيًا للسياسات ويجلب أيضًا التركيز على التغيير الفردي. كما يمكن للموظف أو المستخدم إحضار أجهزته الخاصة والعمل عليها مع الامتثال الكامل لخصوصية البيانات وأمانها من خلال اتباع سياسة استخدام الأجهزة الشخصية في العمل (BYOD). وقد تكون خدمات سطح المكتب (DaaS) حلاً جيدًا كبيئة سطح مكتب موازية للموظفين الذين يعملون عن بُعد أو يسافرون.
3. وبالمثل، فيجوز للوحدات التي ترغب في تصميم مجموعة الخدمات أو التطبيقات الخاصة بها أن تختار خدمات المنصّات السّحابية (PaaS) لبيئات التطوير والاختبار مع توافر منصات التطوير.

د. **المنصة السحابية المتكاملة**: تقوم الوحدات خلال هذه المرحلة بالتحول بنجاح إلى مرحلة يمكنها خلالها قياس جميع خدمات البنية الاساسية والنظام الأساسي والبرمجيات وتقديم فواتير عنها وسدادها على أساس الدفع مقابل الخدمات التي يتم الحصول عليها مع قابلية التوسع في نطاق الخدمات غير المحدودة.

6.2.3. الإطار البيئي

أ. **العروض التنافسية**: تمثل المسائل الأمنية والقانونية العوامل البيئية الرئيسية التي يجب على كل وحدة العمل مع مقدم الخدمات السحابية لتصنيف اختصاصاتهم حول البيانات وسرية البيانات والمخاطر الأمنية. وبهذا ستكون الوحدات قادرة على اعتماد وتقديم خدمات أفضل لموظفيها والمواطنين وشركات الأعمال. كما ستكون الوحدات قادرة على الاستفادة من عروض خدمات البرمجيّات (SaaS) مع أو بدون إجراء تعديلات حسب الطلب وتركيز المزيد من موظفيها على العمل.

6.3. تحديد نموذج الخدمات السحابية المناسب

ستختلف كل وحدة عن مثيلاتها باختلاف مجموعة البنية الاساسية وحجم الأعمال. وبالتالي ستتغير الطلبات أيضًا، لذا ستؤثر خيارات البنية الاساسية التي ستتخذها الوحدات على قدرتها على تقديم إمكانيات جديدة. لهذا السبب يتعين على الوحدات البحث عن حل الخدمة السحابية الذي يلبي متطلبات أعمالهم بالطريقة الأكثر فعالية. ولمساعدة الوحدات على القيام بذلك، فهناك خمس خطوات تساعد على اختيار حل الخدمة السحابية المناسب.

أ. يجب أن تدرك الوحدات حجم أعمالها.

ب. يجب على الوحدات التعاون معاً.

ج. تحليل مستويات البنية الاساسية من الأعلى إلى الأسفل.

د. الأخذ في الاعتبار متطلبات العملية.

ه. مطابقة وتبني حل الخدمة السحابية المناسب.

ترد أدناه فئات التطبيقات التي قد تكون مناسبة بشكل جيد للانتقال إلى السحابة العامة:

أ. **التطبيقات المخصصة للتطوير أو الاختبار**: يمثل حجم الأعمال التطويرية أو الاختبارية النصيب الأكبر من مواضيع الحوسبة السحابية التي يقوم بها مقدمي الخدمات السحابية الرئيسيين (مثل Amazon Web Services). وتميل عملية البناء والاختبار إلى إجراء عمليات حوسبة سحابية كثيفة، وبالتالي فهي مناسبة للحوسبة السحابية العامة.

ستواجه الوحدات أيضًا مخاطر أقل لاختبار التطبيقات وتطويرها، إن وجدت، إذ أنه يمكن إجراء الاختبارات باستخدام بيانات وهمية.

ب. **تطبيقات الإنتاجية الشخصية**: تميل برامج معالجة الكلمات، وإعداد وتصميم جداول البيانات والعروض التقديمية، والبريد الإلكتروني إلى أن تكون مناسبة بشكل جيد، إذ تعتمد هذه التطبيقات على بيانات غير منظمة ولا تتطلب عمومًا زمن انتقال منخفض.

في حال كانت البيانات ونسخ البيانات الخاصة بالوحدات مخزنة في أماكن خاضعة للاختصاص القضائي في سلطنة عُمان بمعايير عالية من أمان البيانات، فيمكن للوحدات أن تبحث عن اختيار السحابة العامة لمثل هذه التطبيقات.

ج. **التطبيقات التعاونية**: تعد تطبيقات الشبكات الاجتماعية وعقد المؤتمرات عبر الويب والتطبيقات التعاونية الأخرى مفيدة للسحابة، خاصة وأن العديد من هذه الحلول تمت إعدادها خصيصاً للخدمات السحابية في المقام الأول. وبالنسبة للوحدات، فستعمل هذه المنصات الاجتماعية كطريقة للوصول إلى المواطنين والشركات في عمان والتواصل معهم. ويمكن أيضًا تشغيل التطبيقات ذات الإصدارات السابقة (القديمة) مثل (SharePoint) في السحابة العامة.

د. **تطبيقات الحوسبة عالية الأداء (HPC)**: إذا كان لدى الوحدات تطبيقات تميل إلى استهلاك قدر كبير جدًا من الموارد (مثل وحدة المعالجة المركزية وذاكرة الوصول العشوائي ومساحة القرص وما إلى ذلك)، فعادة ما تكون هذه التطبيقات مناسبة لمحطات (حقول) الحوسبة السحابية العامة، طالما يمكن إدارة احتياجات البيانات الخاصة بهم.

التطبيقات المناسبة للانتقال إلى السحابة الخاصة:

أ. **التطبيقات ذات المهام الحرجة**: إن التطبيقات ذات المهام الحرجة مثل تخطيط موارد المؤسسات (ERP) قائمة على المعاملات الكثيفة مع معدل عالي من الإنتاجية ومتطلبات زمن انتقال منخفض. وبالنسبة للوحدات التي تدير أنظمة تخطيط موارد المؤسسات (ERP)، فإنها تمتلك بيانات حساسة ومجموعات بيانات كبيرة في كثير من الأحيان، والتي يكون لها متطلبات توافر عالية. وقد يكون لبعض هذه التطبيقات أيضًا احتياجات الامتثال التنظيمي التي قد يكون من الصعب تلبيتها في السحابة العامة.

ب. **التطبيقات القائمة على الشبكة بشكل كبير**: تتطلب مثل هذه التطبيقات موارد شبكة سريعة وعالية الجودة تعمل باستمرار على إرسال واستقبال كميات كبيرة من البيانات. وقد تتطلب هذه التطبيقات غالبًا الوصول إلى التطبيقات الأخرى أو الاندماج معها لمشاركة البيانات.

سيلزم إجراء تقييم تقني لفهم التطبيقات الأكثر ملاءمة للسحابة من الناحية التصميمية والاستراتيجية. وسيتعين على الوحدات تحديد التطبيقات التي سيتم نقلها إلى السحابة أولاً، والتطبيقات التي سيتم نقلها لاحقًا وما إذا كان يجب أن تظل أي تطبيقات داخلية.

يجب على الوحدات – خلال مرحلة التقييم الفني – إيجاد حل لما يلي:

أ. ما هي تطبيقات الأعمال التي ستنتقل إلى السحابة أولاً؟

ب. يجب أن توفر السحابة جميع اللبنات الأساسية المطلوبة للبنية الاساسية.

ج. هل تستطيع الوحدات إعادة استخدام أدوات إدارة الموارد الحالية وضبط التهيئة – إن وجدت؟

د. هل يمكن للهيئات إنهاء عقود تقديم خدمات الدعم للأجهزة والبرمجيات والشبكات؟

يُظهر الشكل التوضيحي الوارد أدناه مؤشرات اختيار السحابة العامة التي يمكن للوحدات استخدامها لاختيار وتحديد أفضل المرشحين المناسبين للسحابة.

المؤشرات	السحابة العامة	السحابة الخاصة	السحابة الهجينة
مستوى التجريد	مرتفع	منخفض	متوسط
الإيجار	إما بيئة تشغيل فردية (مخصصة) أو متعددة المستأجرين (مشتركة)	بيئة تشغيل لمستأجر واحد (مخصص)	مجموعة من عروض السحابة العامة والخاصة التي تسمح بتبادل المعلومات المتعدّد
مستوى الأمان	منخفض. لا يمكن الوصول إلى البيانات المتاحة في منشآت مقدم الخدمة	مرتفع. يمكن الوصول الكامل إلى البيانات	مرتفع. يمكن الوصول الكامل إلى البيانات
التقيد بمورد محدد	تعتمد على التكنولوجيا المستخدمة	مرتفع. تعتمد على التكنولوجيا المستخدمة	تعتمد على التكنولوجيا المستخدمة
النفقات الرأسمالية (CapEx)	منخفضة. نظرًا لأن معظم البنية الاساسية يتم صيانتها بمعرفة مقدم الخدمة	مرتفعة. يجب أن تكون البنية الاساسية الداخلية معدة للنشر	مرتفعة. هي عبارة عن مزيج من خصائص السحابة العامة والخاصة
النفقات التشغيلية (OpEx)	مرتفعة. الدفع المستمر مقابل رسوم الاستخدام	متوسطة. رسوم مرتفعة تُسدد لمرة واحدة فقط مقابل التثبيت	متوسط
تُدار بمعرفة	الجهات الخارجية	الوحدات أو الجهات الخارجية	كلا من الوحدات والجهات الخارجية
مستوى المحاكاة الافتراضية	تعتمد على التكنولوجيا المستخدمة	توفر الذكاء الاصطناعي عبر المحاكاة الافتراضية	مستوى المحاكاة الافتراضية أقل من مستوى السحابة الخاصة
ضمان اتفاقية مستوى الخدمة	من الصعب الحصول عليها	أسهل في الحصول عليها ومراقبتها	أسهل في الحصول عليها ومراقبتها
مناسبة لـ	الشركات الصغيرة والمتوسطة (SMB)	المؤسسات	كلاهما
خصوصية البيانات	منخفضة	مرتفعة	متوسطة
المسائل القانونية ومسائل الامتثال	مرتفعة إذ قد يتعين تخزين البيانات على أرض أجنبية	منخفضة إذ أنه يتم تخزين البيانات في مركز البيانات الخاص بالوحدات	منخفضة إذ أنه يتم تخزين البيانات في مركز البيانات الخاص بالوحدات
أنواع التطبيقات المناسبة	تطبيقات أقل أهمية للمهمة ولها مستوى اندماج أقل	تطبيقات تتعامل مع بيانات سرية للغاية	تطبيقات تتعامل مع بيانات سرية للغاية
الجهة المالكة للبنية الاساسية	الجهات الخارجية	المنظمات أو الجهات الخارجية	كلا من المنظمات والجهات الخارجية

الشكل التوضيحي رقم (9) – مؤشرات تحديد نموذج نشر الخدمات السحابية

6.4. تقييم الجاهزية السحابية

ستشمل مرحلة التقييم إجراء تقييم للوضع الراهن وتحديد المتطلبات وتطوير رؤية لتبني الحوسبة السحابية. كما سيوفر تقييم الوضع الراهن تقرير لانتقال أو عدم الانتقالويجب أن يستند إلى ما يلي:

تقييم الوضع الراهن	تحديد المتطلبات	تحديد الرؤية
أ. فهم الأنظمة القديمة – البيئية والفنية والتشغيلية ب. تقييم ملاءمة العرض المتعلق بالمنتجات ج. تقييم مدى امتثال بيانات الوحدات واحتياجات الأمان د. تقييم البنية الاساسية لتقنية المعلومات للهيئات من أجل الاستمرارية والاعتماد المتبادل للتطبيقات ه. تقييم قدرة الوحدات على تحمل المخاطر وقيود الموارد	أ. مقابلة أصحاب المصلحة الرئيسيين ب. ورشة عمل لتحديد المتطلبات ج. التحقق من مستند المتطلبات د. تحديد متطلبات التوافق والأمان لحل السحابة الجديد	أ. تحديد أهداف الوحدات ب. تحديد الرؤية قصيرة المدى وطويلة المدى ج. تحديد مستوى الترحيل إلى حل السحابة الجديد

الشكل التوضيحي رقم (10) – تقييم الجاهزية السحابية

تشتمل مخرجات تقييم الوضع الراهن للهيئات على مستندات الوضع الراهن ومستند المتطلبات وبيان نطاق الأعمال والرؤية.

الشكل التوضيحي رقم (11) – نهج التقييم

أ. يتعين على الوحدات الوفاء بمعايير التقييم خلال كل خطوة قبل انتقالها إلى الخطوة التالية. كما يتعين عليها تخصـــيص مؤشر لكل معيار (أحمر أو أصفر أو أخضر).

ب. يشير الإخفاق في تلبية معايير التقييم الأساسية – حتى بكل نطاق – إلى أن الملاءمة لم تعد قابلة للتطبيق وأن التطبيقات ليست مناسبة للسحابة في هذا الوقت.

ج. يجب أن تعرض طلبات الوحدات السمات التالية وسيتم تقييمها وفقًا لذلك.

1. الأهمية المنخفضة أو المتوسطة للتطبيقات.
2. الحد الأدنى من أوجه التبني المتبادل لبعض التطبيقات والبيانات الأخرى.
3. استخدام الأجهزة السلعية.
4. متطلبات النطاق الترددي.
5. بيئات العمل أو حزم البرامج المستقلة.
6. لا تعتمد على الأجهزة المتخصصة.
7. المتطلبات المنخفضة أو المتوسطة لاتفاقيات مستوى الخدمة.
8. لا توجد بيانات سرية أو يمكن إخفاء البيانات بسهولة.

المرحلة	المعايير	التوضيح
تقييم الوضع الراهن	مدى أهمية النظام القديم	تحددها هيئات حسب بيئات الإنتاج،
	مدى تعقيد النظام القديم	مدى تعقيد التصميم، ومدى الاعتماد على التطبيقات الأخرى، وقواعد البيانات، والبرمجيات الوسيطة
	المحاكاة الافتراضية المُقترحة	هل يمكن جعل حجم الأعمال افتراضـيًا؟ يعتمد هذا على نظام تشغيل النظام الأساسي ومنصة المحاكاة الافتراضية
	البنية الاساسية للخدمات السلعية	يُنفذ حجم الأعمال على البنية الاساسية للخدمات السلعية
تحديد مدى ملاءمة السحابة	دراسة الجدوى الفنية	
	النطاق الترددي للشبكة	متطلبات النطاق الترددي لشبكة الاتصال المحلية (LAN) أو شـــبكة الاتصـــال واســـعة النطاق (WAN) عند تنفيذ حجم الأعمال في السحابة
	متطلبات البنية الاساسية	مقياس متطلبات الحوســـبة والتخزين والشـــبكة لدعم حجم الأعمال
	البيئات المشتركة	الأنواع التي يمكن أن تدعمها البيئة المشتركة
	البرمجيات المشتركة	مشـاركة البرامج (مثل قواعد البيانات والبرمجيات الوسيطة) مع برامج أخرى
	البنية الاساسية المتخصصة	مدى التبني على الملكيات والمعدات والتراخيص والأجهزة ذات الأغراض الخاصة وما إلى ذلك.

المرحلة	المعايير	التوضيح
	دراسة جدوى الأعمال التجارية	
	الواجهات الداخلية والخارجية	هل يوفر النظام خدمة واجهة العملاء أو مهام المكتب الخلفي (مثل الموارد البشرية)؟
	مدى التأثير على المستخدمين	التأثير على مجتمع المستخدمين بسبب نقل حجم الأعمال إلى السحابة (على سبيل المثال، عدم الوصول إلى مجموعة فرعية من المستخدمين)
	متطلبات مستوى الخدمة	التوافر ووقت الاستجابة وقابلية الاسترداد والتعافي من الكوارث وما إلى ذلك.
	العملاء والبيانات السرية	هل يفي موقع مقدم الخدمة أو الخصائص الأخرى للخدمة السحابية بمتطلبات الأمان الخاصة بكيفية تخزين البيانات وموقع تخزينها؟
دراسة الجدوى والتحليل التشغيلي	تحليل دراسة الجدوى	تحليل التكلفة والمزايا، بما في ذلك التكاليف المبدئية وتكاليف الترحيل والتكاليف الجارية والإطار الزمني للعائد على الاستثمار
	التحليل الفني المفصل	ما هي التغييرات المطلوبة للتطبيقات؟ وكيف ستبدو بنية التطبيقات المستقبلية؟
	تحليل العمليات	ما هو التأثير التشغيلي الناتج عن نقل حجم الأعمال إلى السحابة؟ وما هو نموذج الدعم بعد نقل حجم الأعمال إلى السحابة؟ وما هي مسؤولية مقدم الخدمة إزاء العميل وعمليات التسليم؟
	اعتبارات الإدارة	كيف تتم إدارة حجم الأعمال في السحابة؟ على سبيل المثال، استخدام الأدوات والعمليات والموظفين الداخليين أو الذين يوفرهم المورد، وقرار "الانتقال أو عدم الانتقال" استنادًا إلى بطاقة أداء التقييم

الشكل التوضيحي رقم (12) – معايير التقييم

تستطيع الوحدات اتخاذ قرار بشأن تبني السحابة أم لا بناءً على التقييم ومع مراعاة النقاط المذكورة أعلاه.

	أحمر	أصفر	أخضر	قرار "الانتقال أو عدم الانتقال"
تقييم الوضع الراهن				
دراسة الجدوى الفنية				
دراسة جدوى الأعمال التجارية				
قرار "الانتقال أو عدم الانتقال"				

الشكل التوضيحي رقم (13) – مصفوفة اتخاذ القرار

أ. في حال كان عدد تقييمات المؤشر "الأحمر" هو (1) على الأكثر، فقد تقرر الهيئة "الانتقال" إلى حل السحابة، ويجوز عدا ذلك التوصل إلى قرار "عدم الانتقال".

ب. في حال كان عدد تقييمات المؤشر "الأصفر" هو (2) على الأكثر، فقد تقرر الهيئة "الانتقال" إلى حل السحابة، ويجوز عدا ذلك التوصل إلى قرار "عدم الانتقال".

ج. يجب أن يكون عدد تقييمات المؤشر "الأخضر" هو (2) على الأكثر حتى تتمكن الهيئة من التوصل إلى قرار "الانتقال" إلى حل السحابة، ويجوز عدا ذلك التوصل إلى قرار "عدم الانتقال".

يوفر هذا القسم من الملحق معلومات حول مجالات المخاطر المختلفة التي يتعين على الوحدات أن تكون على دراية بها وأن توفر استبيان حول تقييم المخاطر للسحابة.

يوفر القسم الوارد أدناه خارطة الطريق المفصلة التي يتعين على الوحدات النظر فيها نحو تبني الخدمات السحابية.

6.5. خارطة الطريق لتبني الخدمات السحابية

سيتعين على الوحدات اجتياز خمس مراحل وواحد وعشرين مستوى وفقاً للشكل التوضيحي المبين في الصفحة اللاحقة وذلك حتى يمكنهم تبني الخدمات السحابية المناسبة.

أ. ستشتمل المرحلة الأولى على فهم الخدمات السحابية من المنظور التجاري للهيئات وتأثير تبني الخدمات السحابية على تقنية المعلومات الحالية.

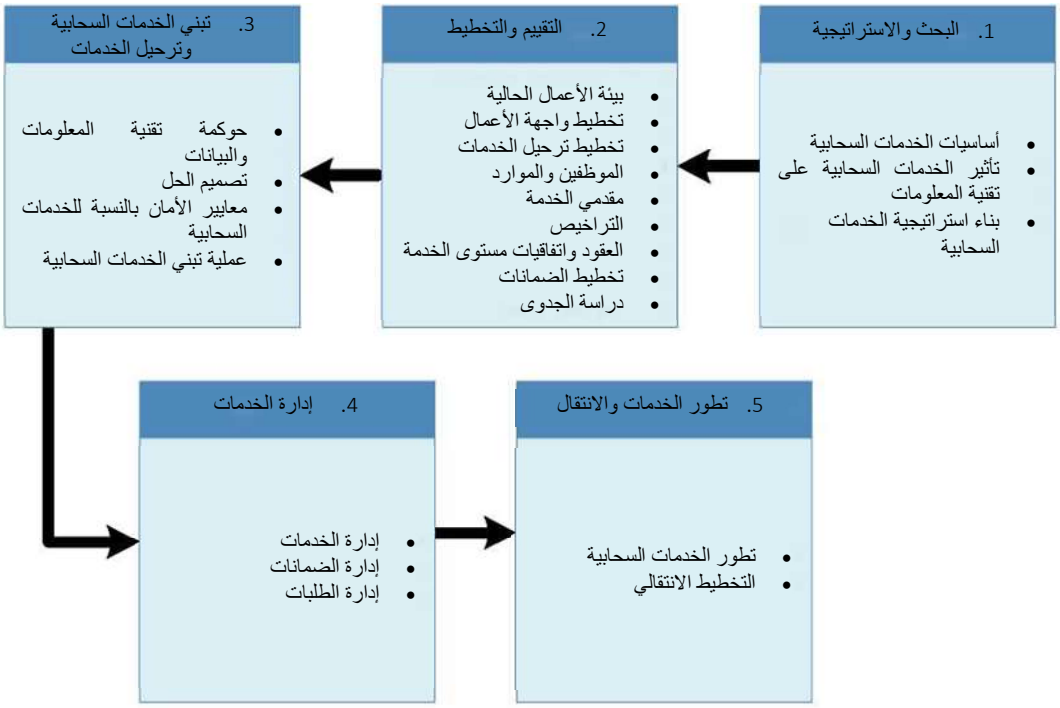
ب. تتمثل المرحلة الثانية التي تنفذها الوحدات في تقييم بيئة تقنية المعلومات الحالية مع فهم العمليات التجارية، وطبيعة التطبيقات الحالية والتخطيط للوجهة مع فهم سيناريوهات الترحيل، والموظفين والموارد المطلوبة، والدعم الذي يوفره مقدمي الخدمات وما إلى ذلك، لإعداد دراسة جدوى لتبني الخدمات السحابية.

ج. كما ستشتمل مرحلة تبني الخدمات السحابية والترحيل على تحديد تصاميم تقنية المعلومات وحوكمة البيانات والسياسات مع تصاميم الحلول وتحديد وفهم معايير الأمان في السحابة.

د. بينما تكون المرحلة التالية هي إدارة الخدمات، إذ يجب على الوحدات العمل مع مقدم الخدمات لإدارة اتفاقيات مستوى الخدمة المضمونة للوحدات. وقد تحتاج الوحدات في أي وقت إلى موارد إضافية وخاصة في حال كانت الخدمات

السـحابية قائمة على توفير الموارد عند الطلب. أما في حالة الكشـف عن البيانات أو الإخفاق في تقديم الخدمة، يجب أن يكون مقدم الخدمة قد وضع آليات لإبلاغ الوحدات وموافاتها بآخر المستجدات حول طبيعة الإخفاق وأثره.

ه. لقد تطورت الخدمات السـحابية على مر السـنين ويجب على الوحدات العمل مع مقدم الخدمة لفهم كيفية تطوير الخدمات السـحابية لمقدم الخدمة للتوافق مع العمليات والتقنيات وفقًا لمتطلبات الوحدات والامتثال الحالية والمسـتقبلية. وبمجرد أن يتم توثيق ذلك بوضوح، فيتعين على الوحدات ومقدمي الخدمات العمل على ترحيل الخدمات.



الشكل التوضيحي رقم (14) – خارطة الطريق لتبني الخدمات السحابية

6.6. اتفاقيات مستوى الخدمات السحابية (SLAs)

ستساعد اتفاقيات مستوى الخدمة السحابية (SLAs) أصحاب المصلحة المعنيين بمجال تقنية المعلومات والأعمال التجارية على تحليل اتفاقيات الخدمة السـحابية عند التفكير في الاسـتعانة بمجموعة مختلفة من مقدمي الخدمات لتبني الخدمات السـحابية. كما ستساعد اتفاقيات مستوى الخدمة الوحدات على الحصول على توقعات واضحة بشن الخدمة من مقدم الخدمة السحابية وأيضًا بين الوحدات ومقدم الخدمة. ويرد أدناه أهم عشر خطوات لازمة فيما يتعلق باتفاقيات مستوى الخدمات السحابية.

أ. يجب توضـيح أدوار ومسـؤوليات الوحدات (المسـتهلكين) ومقدمي الخدمات وغيرهم من الأطراف المعنية الأخرى مثل شركات النقل، وما إلى ذلك، وتحديدها بشكل واضح في اتفاقيات مستوى الخدمة.

ب. يجب مراعاة اسـتراتيجيات وسـياسـات الوحدات أثناء صـياغة اتفاقيات مسـتوى الخدمة نظرًا لوجود روابط متبادلة بين الخدمات السحابية وجوانب الأعمال.

ج. يجب فهم مستويات الموارد والخدمات السحابية بناءً على نموذج الخدمة السحابية (مثل خدمات البنية الأساسيّة (IaaS) وخدمات المنصّـــات السّـــحابية (PaaS) وخدمات البرمجيّات (SaaS)). وســـيكون لكل نموذج خدمة الاعتبارات الخاصة به المتعلقة باتفاقية مستوى الخدمة والتي يجب أن تفهمها الوحدات بوضوح.

د. عادةً ما يتضمن هدف أداء الحوسبة السحابية التوافر ومعدل المعاملات ووقت الاستجابة وسرعة المعالجة. ويجب أن تكون تلك الأهداف قابلة للتدقيق والقياس عند النظر في مدى توفير مستويات التيسير المتعلقة بالخدمات السحابية.

ه. بالمقارنة مع تقنية المعلومات التقليدية، تعتبر المخاطر المتعلقة بأمن البيانات والخصوصية أعلى وبالتالي يتعين على مقدم الخدمة والوحدات إدارتها بحذر. كما يجب أن تحدد اتفاقيات مستوى الخدمة مخطط تصنيف مستوى الأمان استنادًا إلى مدى أهمية البيانات ودرجة حساسيتها بجانب التفاصيل وملكية البيانات، ومستويات الأمان المحددة وضوابط الحماية، وسياسات الاحتفاظ بالبيانات وإتلافها.

و. تعتبر الأنظمة التي تتمتع بالشفافية والقابلة للتوسيع المخصصة لمراقبة الخدمات السحابية ضرورية لتلبية الأداء المتوقع. وسيتعين على الوحدات التحقق من صحة الإجراءات والسياسات المتعلقة بالتقارير والقياس والتوفير السريع والتحديث والتدقيق مع مقدم الخدمة.

ز. يتعين على الوحدات أن تطلب الحصول على توثيق واضح بشأن قابلية تنفيذ الخدمات وتوقعات الأداء لاستعادة أو تجنب تعطل الخدمات. ويجب على كل من مقدم الخدمة والوحدات إعداد إجراءات وقائية وتصحيحية فيما يتعلق بالتصورات في حالة عدم تنفيذ عمليات تقديم الخدمة على النحو المتوقع.

ح. يتعين على مقدم الخدمة تقديم خطة عمل مستمرة (BCP) إلى الوحدات مع التركيز على العمليات التكنولوجية لمكونات تقنية المعلومات. كما يجب تبرير مستوى تفاصيل خطة التعافي من الكوارث (DR) مقابل أهداف الأعمال وأهمية الخدمات السحابية للهيئات.

ط. يجب على الوحدات ومقدمي الخدمات اتخاذ قرار بشأن وضع خطة إدارة فعالة يمكن تنفيذها من خلال الاجتماعات الروتينية، والتنسيق، وآليات التصعيد لضمان التعامل مع المشكلات المحددة بشكل صحيح.

ي. يتعين على كل من الوحدات ومقدم الخدمة الرجوع إلى اتفاقيات مستوى الخدمة التي يجب أن تشتمل على إجراءات الخروج، وذلك في حال عدم تحقيق توقعات الوحدات أو لا يمكن الاستمرار في تقديم الخدمة بسبب عوامل أخرى. كما يجب أن تضمن إجراءات الخروج عدم تعطيل استمرارية العمل، مثل الحفاظ على بيانات الوحدات ونقلها إلى مقدمي الخدمات الآخرين أو إلى مركز البيانات المملوك للوحدات.

6.7. عوامل تكلفة الخدمات السحابية

تمثل خدمات الحوسبة السحابية التي تقدمها خدماتنا السحابية أداة مساعدة لنا. إذ ستسمح الخدمات السحابية للوحدات بالتخلص من بعض البنية الاساسية لتقنية المعلومات باهظة الثمن وتحويل تكاليف الحوسبة إلى نفقات تشغيلية يمكن التحكم فيها. وستستفيد الوحدات أيضًا من الأعباء التكنولوجية التي ينطوي عليها دعم أنظمة تقنية المعلومات وصيانتها. ومع ذلك، فإن للحوسبة السحابية بعض التكاليف الاستثمارية والمتكررة التي يجب على الوحدات وضعها في الاعتبار وهي على النحو المذكور أدناه.

أ. التكاليف الأولية التي ستشتمل على الاستثمار الأولي المطلوب لإعداد الخدمات السحابية.

1. تكاليف **الجاهزية الفنية** تشير إلى التكاليف اللازمة لتتناسب مع تثبيت الشبكة أو ترقية بعض المكونات المطلوبة للاتصال بالسحابة.
2. **التنفيذ والاندماج**: تشير إلى الخدمات المهنية اللازمة لإدارة الانتقال إلى السحابة ودمجها مع الوحدات الداخلية أو الخدمات السحابية الأخرى (السحابة الهجينة).
3. **ضبط التهيئة والتخصيص حسب الطلب**: تشير إلى تكاليف ضبط تهيئة تطبيقات خدمات البرمجيّات (SaaS) التابعة إلى أي هيئة.

4. **التدريب**: تشير إلى الموارد المطلوبة لإدارة مقدمي الخدمات والخدمات.
5. **التغيير التنظيمي**: تشير إلى العمليات المطلوبة لتلبية احتياجات السحابة المحددة مثل التدقيق الداخلي وإدارة التغيير والمراقبة وما إلى ذلك.

ب. التكاليف المتكررة المتعلقة بالرسوم وعمليات الدعم الروتينية للحفاظ على استخدام الخدمات السحابية.

1. **رسوم الاشتراك**: يتم الاتفاق على الرسوم الدورية للاشتراك في الخدمات السحابية (الدفع حسب الاستخدام).
2. **إدارة التغيير**: تشير إلى التكاليف المتكبدة عند طلب تغييرات في النظام.
3. **إدارة الموردين**: تشير إلى التكاليف المتعلقة بالمراقبة الروتينية لأنشطة مقدم الخدمة السحابية، واتفاقية مستوى الخدمة، والتقييمات الأخرى.
4. **التنسيق بشأن الخدمات السحابية**: تشير إلى تكاليف إدارة التنسيق بشأن الخدمات السحابية (في حالة وجود أكثر من مقدم خدمة سحابية).
5. **تقديم الدعم إلى المستخدم النهائي وإدارة عملياته**: تشير إلى التكاليف التي لا تزال تحتجزها الوحدات.
6. **تخفيف المخاطر**: تشير إلى الجهود المطلوبة لتقليل المخاطر إلى مستويات مقبولة.
7. **تخفيض أو زيادة حجم الأعمال**: تشير إلى التكاليف المتعلقة بزيادة حجم أعمال موارد الحوسبة السحابية أو تخفيضها (المرونة).

7. الروابط والاعتمادات المتبادلة

سيكون لإطار عمل تبني الخدمات السحابية تبعيات تؤثر على السياسات وأطر العمل التالية.

أ. سياسة الموقع الإلكتروني والاستضافة للوحدات الحكومية في سلطنة عمان.

ب. سياسات أمن المعلومات لحماية البيانات والمعلومات والتي تعد من أهم الأصول بالنسبة للوحدات العمانية. وستساعد إرشادات إدارة أمن المعلومات في حماية البيانات من أي وصول وتعديل غير مصرح به وضمان توافر المعلومات في الوقت المناسب للأشخاص المعنيين.

ج. إطار المعايير التقنية للحكومة الإلكترونية (OeGAF) – النموذج المرجعي الفني (TRM) المخصص لتوفير الإرشادات التوجيهية لتبني المعايير الفنية وأفضل الممارسات لإدارة الاندماج والتشغيل البيني لأنظمة تقنية المعلومات عبر جميع الوحدات العمانية.

8. الملحق (أ) – متطلبات الاستضافة السحابية أو الحوسبة السحابية

(الالتزامات التعاقدية)

يتعين على الوحدات الحكومية ضمان توافر المتطلبات التالية في العقود المبرمة مع مقدم الخدمة السحابية (CSP) الخارجي.

1. متطلبات الأمان – يتعين على مقدم الخدمة السحابية (CSP) الذي يقدم خدمات الحوسبة السحابية للوحدات الحكومية تطبيق مجموعة الضوابط المناسبة لضمان الامتثال لمعايير الأمان بما في ذلك على سبيل المثال لا الحصر:
   - معيار أيزو/أي إي سي 27001،
   - معيار أيزو/أي إي سي 27017،
   - معيار أيزو/أي إي سي 27018،
   - مصفوفة ضوابط التحكم الصادرة عن "منظمة تحالف أمن الحوسبة السحابية" (CSA).
   - التوافق مع معيار أمان بيانات صناعة بطاقات الدفع (PCI DSS) – لاستضافة حلول الدفع عبر الإنترنت.
2. متطلبات الخصوصية – يتحمل مقدم الخدمة السحابية (CSP) المسؤولية عن إجراءات حماية الخصوصية والأمان التالية:

أ. يتعين على مقدم الخدمة السحابية (CSP) منح الحكومة إمكانية الاطلاع والحصول على مرافقه ومنشآته وقدراته الفنية وعملياته ومستنداته وسجلاته وقواعد بياناته، وذلك إلى الحد المطلوب للحماية من التهديدات والمخاطر المتعلقة بأمن وسلامة وسرية أي بيانات حكومية غير عامة يحصل عليها ويجمعها ويخزنها مقدم الخدمة السحابية (CSP).

ب. في حال اكتشاف الحكومة أو مقدم الخدمة السحابية (CSP) لتهديدات أو مخاطر جديدة أو غير متوقعة، أو إذا توقفت الضمانات الحالية عن العمل، فيجب على الجهة التي اكتشفت هذا الأمر أن تلفت انتباه الطرف الآخر إلى الموقف على الفور.

ج. يتعين على مقدم الخدمة السحابية (CSP) الالتزام أيضًا بمتطلبات الخصوصية الإضافية التي قد تطلبها الحكومة.

3. يحق للحكومة إجراء عمليات تدقيق يدوية أو آلية أو عمليات مسح أو مراجعات أو عمليات تفتيش أخرى لبيئة تقنية المعلومات الخاصة بمقدم الخدمة السحابية (CSP) المستخدمة لتوفير أو تيسير الخدمات للحكومة. كما يتحمل مقدم الخدمة السحابية (CSP) المسؤولية عن ضمانات الخصوصية والأمان التالية:

أ. يجب ألا ينشر مقدم الخدمة السحابية (CSP) أو يفصح بأي شكل من الأشكال – دون الحصول على موافقة خطية من مسؤول التعاقد – عن تفاصيل أي إجراءات وقائية سواء أصممها أو طورها مقدم الخدمة السحابية (CSP) بموجب هذا العقد أو التي تقدمها الحكومة بطريقة أخرى. باستثناء؟

ب. يتعين على مقدم الخدمة السحابية (CSP) منح الحكومة إمكانية الاطلاع والحصول على مرافقه ومنشآته وقدراته الفنية وعملياته ومستنداته وسجلاته وقواعد بياناته في غضون 72 ساعة وذلك إلى الحد المطلوب لتنفيذ برنامج التفتيش للحماية من التهديدات والمخاطر التي تهدد أمن وسلامة وسرية البيانات الحكومية. كما يجب أن يشمل برنامج التفتيش – على سبيل المثال لا الحصر – ما يلي:

1. عمليات فحص الثغرات الأمنية على نظام التشغيل أو على الشبكة المصادق عليها وغير المصادق عليها

2. عمليات فحص الثغرات الأمنية على تطبيقات الويب المصدق عليها وغير المصدق عليها
3. عمليات فحص الثغرات الأمنية على تطبيقات قاعدة البيانات المصدق عليها وغير المصدق عليها
4. يمكن إجراء عمليات الفحص الآلي بمعرفة الموظفين الحكوميين، أو الوكلاء الذين يعملون نيابة عن الحكومة، باستخدام المعدات التي تديرها الحكومة، والأدوات التي تحددها الحكومة.

في حال اختار مقدم الخدمة السحابية (CSP) تنفيذ عمليات الفحص أو التدقيق الآلي الخاصة به، فقد يتم قبول نتائج عمليات الفحص هذه، وفقًا لتقدير الحكومة، بدلاً من عمليات فحص الثغرات الأمنية التي تنفذها الحكومة. وفي هذه الحالات، يجب أن توافق الحكومة على أدوات الفحص وضبط تهيئتها. بالإضافة إلى ذلك، يجب تقديم نتائج عمليات الفحص التي أجراها المورد بالكامل إلى الحكومة.

4. تخزين المعلومات الحساسة ومعالجتها – يجب استضافة البيانات أو المعلومات الحكومية فقط أو التعامل معها أو معالجتها داخل الحدود الجغرافية لسلطنة عمان. ويتضمن ذلك ترتيبات التخزين الأساسي بالإضافة إلى ترتيبات النسخ الاحتياطي أو عمليات التعافي من الكوارث.

لن يتم الإفصاح عن المعلومات أو البيانات أو المعدات الحساسة إلا للموظفين المصرح لهم على أساس الحاجة إلى المعرفة. كما يتعين على مقدم الخدمة السحابية (CSP) التأكد من تبني الضمانات الإدارية والفنية والمادية المناسبة لضمان حماية أمن وسرية هذه المعلومات أو البيانات أو المعدات بشكل صحيح. وسيتم إعادة هذه المعلومات أو البيانات أو المعدات – متى لم تعد مطلوبة – إلى حيازة الحكومة أو يتم إتلافها أو الاحتفاظ بها إلى أن تصدر تعليمات أخرى بشأنها بخلاف ذلك. كما يتم تدمير المواد باتباع أساليب تطهير البيانات المتفق عليها.

يتعين على مقدم الخدمة السحابية (CSP) تطوير وتنفيذ خطة للتخارج ونقل الخدمات – وذلك في حال قررت الهيئة الاستعانة بمقدم خدمة سحابية (CSP) جديد أو إعادة تقديم الخدمات داخلياً.

الاتفاق بشأن استعادة أو إعادة جميع البيانات (بما في ذلك ترتيبات التخزين الأساسي وكذلك ترتيبات النسخ الاحتياطي أو التعافي من الكوارث)، في حالة التخارج باستخدام التنسيقات المعتمدة من الهيئة.

5. حماية المعلومات –

أ. يتحمل مقدم الخدمة السحابية (CSP) المسؤولية عن توفير الحماية المناسبة لجميع المعلومات المستخدمة أو المُتحصل عليها أو المطورة كنتيجة للأعمال المُنفذة بموجب هذا العقد. كما يجب على مقدم الخدمة السحابية (CSP) أيضًا حماية جميع البيانات والمعدات الحكومية وما إلى ذلك من خلال التعامل مع المعلومات على أنها حساسة. ومن المتوقع أن يتم جمع هذه المعلومات وإنشائها وتخزينها داخل موقع العمل الأساسي. وفي حال تعين على موظفي مقدم الخدمة السحابية (CSP) إزالة أي معلومات من موقع العمل الأساسي، فيجب عليهم حمايتها بنفس القدر الذي يحمون به بياناتهم الخاصة أو الأسرار التجارية للشركة.

ب. ستحتفظ الحكومة بحقوق غير مقيدة فيما يتعلق بالبيانات الحكومية. كما تحتفظ الوحدة مقدمة الطلب بملكية أي بيانات أو تطبيقات تم إنشاؤها أو تحميلها بمعرفة المستخدم، والتي تمت استضافتها على البنية الاساسية للمورد، بالإضافة إلى الاحتفاظ بالحق في طلب نسخ كاملة من هذه البيانات في أي وقت.

ج. تحتوي البيانات التي تتم معالجتها وتخزينها من خلال التطبيقات المختلفة داخل البنية الاساسية للشبكة على بيانات مالية بالإضافة إلى معلومات التعريف الشخصية (PII). ويجب حماية هذه البيانات ومعلومات التعريف الشخصية (PII) ضد الوصول أو الإفصاح أو التعديل غير المصرح به أو السرقة أو الإتلاف. كما يجب أن يضمن مقدم الخدمة السحابية (CSP) أن المرافق التي تضم البنية الاساسية للشبكة آمنة ماديًا.

د. يجب أن تكون البيانات متاحة للحكومة عند الطلب خلال يوم عمل واحد أو خلال الإطار الزمني المحدد بخلاف ذلك، ولا يجوز استخدامها لأي غرض آخر بخلاف ما هو مذكور في هذا المستند. ويلتزم مقدم الخدمة السحابية (CSP) تقديم البيانات المطلوبة دون تحميل أي تكاليف إضافية على الحكومة.

ه. لا يجوز لمقدم الخدمة السحابية (CSP) الإفصاح عن أي بيانات دون الحصول على موافقة خطية من الحكومة. ويجب تقديم جميع طلبات الإفصاح خطياً إلى ممثل الهيئة.

6. السرية وعدم الإفصاح –

أ. تعتبر المخرجات الأولية والنهائية وجميع أوراق العمل ذات الصلة والمواد الأخرى التي تعتبرها الهيئة ذات صلة والتي تم إنشاؤها بمعرفة مقدم الخدمة السحابية (CSP) في تنفيذ الأعمال المنصوص عليها بموجب هذا العقد، ملكًا لحكومة عمان ويجب تقديمها إلى الهيئة المتعاقدة بعد انقضاء العقد.

ب. تمتلك حكومة عمان حقوق بيانات غير محدودة لجميع المخرجات وكذلك جميع أوراق العمل والمواد المرتبطة بها.

ج. تخضع جميع المستندات التي تم إعدادها بموجب هذا المشروع لملكية الحكومة العُمانية ولا يجوز لمقدم الخدمة السحابية (CSP) نسخها أو الاحتفاظ بها. وسيتم تقديم جميع مستندات المشروع المناسبة للهيئة أثناء هذا العقد وبعد انقضائه.

د. لا يجوز لمقدم الخدمة السحابية (CSP) الإفصاح عن أي معلومات دون الحصول على موافقة خطية من مسؤول التعاقد.

ه. قد يُطلب من الموظفين الذين يعملون في أي من المهام المُحددة – بناءً على طلب الحكومة – التوقيع على اتفاقيات رسمية بعدم الإفصاح أو تعارض المصالح لضمان حماية وسلامة المعلومات والمستندات الحكومية.

و. بالإضـــافة إلى ذلك، فإنه يجب اســـتخدام أي معلومات توفرها الحكومة لمقدم الخدمة الســـحابية (CSP) فقط لغرض تنفيذ أحكام هذا العقد ولن يتم الإفصـاح أو الكشـف عنها بأي شـكل من الأشـكال لأي شـخص ما لم يكن هذا الأمر ضـروريًا في تنفيذ الأعمال المنصـوص عليها بموجب العقد. ويتحمل مقدم الخدمة السحابية (CSP) المسؤولية عن حماية سرية السجلات الحكومية أثناء تنفيذ هذا العقد، ويجب أن يضمن أن جميع الأعمال التي يقوم بها مقاول الباطن التابع له خاضـعة لإشـرافه أو لإشـراف موظفيه المعنيين. كما يجب إخطار كل مسـؤول أو موظف تابع لمقدم الخدمة الســـحابية (CSP) أو أي من مقاولي الباطن التابعين له الذين قد يوفر لهم مقدم الخدمة الســـحابية (CSP) أي ســـجل حكومي أو يفصـــح لهم عنه خطياً بأنه ينبغي اســـتخدام هذا المعلومات المُفصح عنها لهذا المسؤول أو الموظف فقط للغرض المخصص له وإلى الحد المسموح به بموجب العقد. وقد تُعرض عمليات الإفصـاح الأخرى غير المصـرح بها عن أي من هذه المعلومات مرتكبها للوقوع في عقوبات جنائية مفروضة بموجب [يرجى توضيح مواد القانون المعمول بها / ذات الصلة].

9. الملحق (ب) – تقييم المخاطر

عندما يتم النظر في برنامج لتطوير ونشر حل أعمال جديد، فستظهر مخاطر مرتبطة به، والتي ستؤثر على قدرة الحل على تحقيق أهدافه.

يتضمن تقييم مخاطر تبني الحوسبة السحابية النظر في عدد من العوامل المعقدة والمترابطة. وسيشتمل تقييم مخاطر تبني السحابة على إجراء مقابلات مع مقدمي الخدمات، وجمع الاستبيانات والمستندات والمراجعات، ومناقشات جماعية مع مقدمي الخدمات.

تكمن التحديات التي تواجه تبني الحوسبة السحابية في عدة نقاط مثل موقع البيانات والخروج من الخدمات السحابية أو إنهاء التعاقد مع مقدم الخدمة، وعدد الأطراف المشاركة في الخدمات السحابية وعمليات المراقبة التي تنفذها الوحدات.

سيختلف مستوى المخاطر بشكل كبير بناءً على نوع بنية السحابة التي يتم النظر فيها. ويمكن تصنيف المخاطر المحددة على النحو التالي:

أ. مخاطر الامتثال.

ب. المخاطر الاستراتيجية.

ج. المخاطر التشغيلية.

د. مخاطر السوق والتمويل.

تمثل الأشكال التوضيحية الواردة أدناه صيغ نموذجية قياسية ويمكن للهيئة المعنية تخصيصها حسب الاقتضاء. إذ يغطي الشكل التوضيحي الأول مجالات المخاطر المختلفة مع احتمالية وتأثير المخاطر المرتبطة بها، بينما يوضح الشكل التوضيحي الثاني استبيان لتقييم المخاطر فيما يتعلق بالخصوصية والأمان والامتثال والحوكمة وما إلى ذلك.

نموذج إطار عمل إدارة المخاطر				
مجال المخاطر	نطاق التحكم في المخاطر	الوصف	احتمالية المخاطر	تأثير المخاطر
مخاطر الامتثال	الحوكمة وإدارة المخاطر المؤسسية	عدم توافر نظام حوكمة داخلي فعال لأمن المعلومات، وإدارة المخاطر والامتثال، وعدم التوافق مع نظام الحوكمة الأمني الخاص بمقدم الخدمة	محتمل	متوسط
	المسائل القانونية: العقود والاكتشاف الإلكتروني	تخزين البيانات الشخصية ومعالجتها والإفصاح عنها لجهات خارجية ونقلها إلى جهات قانونية أخرى مع التعرض لمخاطر	متوقع	جسيم

نموذج إطار عمل إدارة المخاطر				
مجال المخاطر	نطاق التحكم في المخاطر	الوصف	احتمالية المخاطر	تأثير المخاطر
		عدم قدرة مقدم الخدمة على إنشـــاء (إعداد) بيانات تجارية في حالة الاستدعاء.		
	الاستجابة للحوادث	إخفاق مقدم الخدمة في الكشـــف عن الحوادث والتعامل معها والإبلاغ عنها إلى الوحدات من خلال توفير البيانات القابلة للتحليل بســـهولة لتلبية المتطلبات القانونية في حالة تحقيقات التحليل الجنائي	محتمل	خطير
	تخزين البيانات لدى جهات متعددة وانعدام الشفافية	نسخ البيانات للتسليم والتخزين المتكرر دون الحاجة مع عدم توفير معلومات فعلية حول مكان تخزين البيانات. قد تخالف الوحدات اللوائح دون علمها وخاصـــة إذا لم يتم توفير معلومات واضحة حول جهات التخزين	متوقع	خطير
	إدارة الامتثال والتدقيق	خطر عدم الامتثال للوائح والمعايير الحكومية والخاصـــة بالمجال، وعدم الحصـــول على معلومات التدقيق من مقدم الخدمة	محتمل	خطير
	مخاطر حماية البيانات	خطر عدم توافر المعايير المناســـبة للحفاظ على حماية البيانات بالتوافق مع مســـتوى الامتثال المطلوب	محتمل	خطير
	تطهير البيانات الحساسة	لا يمكن تدمير البيانات ماديًا، أو لا يمكن تحديدها بشـــكل صـــحيح أو لا ينطبق إجراء مناسب	مرجح جدا	خطير

نموذج إطار عمل إدارة المخاطر				
مجال المخاطر	نطاق التحكم في المخاطر	الوصف	احتمالية المخاطر	تأثير المخاطر
	عدم توافر عمليات التدقيق أو التبني	لا يمكن إجراء عمليات التدقيق على النظام أو تبنيه على النحو المطلوب	محتمل	خطير
	تدني معايير الامتثال	الفشل في تحقيق الامتثال أو الحفاظ عليه (على نطاق اللوائح والحوكمة والمعايير)	محتمل	خطير
	تدني معايير الحوكمة	قد تتنازل الوحدات لمقدم الخدمة عن سيطرتها على عدد من المسائل التي قد تؤثر على الحوكمة الشاملة	مرجح جدا	خطير
المخاطر الاستراتيجية	إدارة المعلومات وأمن البيانات	التحديد الضعيف للبيانات الحساسة أو حماية البيانات العابرة أو المخزنة على السحابة، ومنع تسرب البيانات	محتمل	خطير
	قابلية التشغيل التبادلي وقابلية النقل	عدم القدرة على توفير قابلية التشغيل التبادلي لتطبيقات الأعمال بين مقدمي الخدمات والافتقار إلى المعايير لتقليل مخاطر التقيد بمورد محدد	محتمل	خطير
	اختيار مقدم خدمة غير كفء	اختيار التقنيات أو الخدمات ذات المعيار دون المستوى الأمثل، مما يؤدي إلى تدني كفاءة تشغيل النظام	غير مرجح	خطير
	الجاهزية التنظيمية	عدم القدرة على تحقيق التوافق الاستراتيجي، والجاهزية الثقافية والتوظيفية، والدعم، ومشاركة أصحاب المصلحة	غير مرجح	خطير

نموذج إطار عمل إدارة المخاطر				
مجال المخاطر	نطاق التحكم في المخاطر	الوصف	احتمالية المخاطر	تأثير المخاطر
	عدم وجود فائض في عدد الموردين	عدم القدرة على تحديد أو التعاقد مع مورد بديل	مرجح جدا	خطير
	التقيد بمورد محدد	المخاطر المرتبطة بالانتقال من بيئة تقنية المعلومات الداخلية إلى مقدم خدمة خارجي، ومن مقدم خدمة إلى آخر	محتمل	خطير
	تصنيف البيانات من طرف الوحدات	التصنيف غير المناسب للبيانات وتعريف ضوابط التخفيف مما يؤدي إلى عدم القدرة على تحديد المتطلبات إزاء مقدم الخدمة	مرجح جدا	خطير
	ترحيل البيانات من المرافق الداخلية إلى السحابة (بغض النظر عما إذا كانت عامة أو خاصة أو هجينة)	صعوبة نقل البيانات القديمة إلى بيئة قائمة على السحابة	محتمل	خطير
المخاطر التشغيلية	عمليات مركز البيانات	عدم إمتثال مقدم الخدمة لمعايير الإدارة وأفضل الممارسات وتنفيذ الضوابط الأمنية وفقًا لمدى حساسية خدمات الأعمال	محتمل	خطير
	فشل تسجيل البيانات وتعقبها	فقدان السجلات التشغيلية أو تعرضها للخطر (بما في ذلك سجلات الأمان)	غير مرجح	خطير
	فشل النسخ الاحتياطي	التضليل أو سرقة معلومات النسخ الاحتياطي	محتمل	خطير

نموذج إطار عمل إدارة المخاطر				
مجال المخاطر	نطاق التحكم في المخاطر	الوصف	احتمالية المخاطر	تأثير المخاطر
	إدارة المعلومات وأمن البيانات	التحديد الضعيف للبيانات الحساسة أو حماية البيانات العابرة أو المخزنة على السحابة، ومنع تسرب البيانات	محتمل	خطير
	مدى التأثير على الإجراءات التشغيلية الداخلية الحالية	مراجعة الإجراءات التشغيلية القائمة فيما يتعلق بإدارة التغيير، وإدارة الحوادث أو المشاكل، وإدارة استمرارية الأعمال	محتمل	خطير
	النمذجة غير الدقيقة لاستخدام الموارد أو استنفاد الموارد	الفشل المؤقت في توفير كفاءات إضافية أو الامتثال إلى اتفاقية مستوى الخدمة.	غير مرجح	خطير
	الاندماج في حلول الأعمال الحالية	صعوبة الاندماج في البيئة القديمة أو الحالية (الواجهات)	محتمل	خطير
	أنشطة خبيثة من أحد المسؤولين الداخليين	المستخدمين المميزين (مثل المسؤول) الذين يقومون بأنشطة غير مصرح بها على النظام (مثل سرقة البيانات، التلاعب بالبيانات...)	محتمل	خطير
	تسرب المعلومات الحساسة	نشاط عرضي أو خبيث يؤدي إلى الكشف عن المعلومات الحساسة لمجموعة غير مصرح لها	محتمل	خطير
	إدارة العمليات	ينفذ مقدم الخدمة العمليات بطريقة لا تفي بمتطلبات الامتثال (مثل إدارة التغيير وإدارة التصحيح)	محتمل	خطير
	الاستدعاء والاكتشاف الإلكتروني	مصادرة النظام الحرج نتيجة لاستدعاء من هيئات إنفاذ القانون أو بموجب الدعاوى المدنية	محتمل	خطير

نموذج إطار عمل إدارة المخاطر				
مجال المخاطر	نطاق التحكم في المخاطر	الوصف	احتمالية المخاطر	تأثير المخاطر
	الدخول غير المصرح به إلى المنشآت	يشتمل الدخول غير المصرح به إلى المبنشآت على الوصـــول المادي إلى الأجهزة والمرافق الأخرى	محتمل	خطير
	سرقة أجهزة الحاسب الآلي	سرقة الأنظمة أو البيانات	محتمل	خطير
	أمـان نقطـة النهـايـة (على سـبيـل المثـال، الكمبيوتر المـحـمـول، الـكـمـبـيـوتـر الشـخصـي، الهاتف الذكي، الجهاز اللوحي) المُسـتخدمة في الـدخول على الخـدمـات السحابية.	عدم القدرة على توفير السياسات أو الضوابط المناسبة لحماية نقطة النهاية	غير مرجح	خطير
	القيود في الموارد البشرية	عدم القدرة على العثور على الموارد المناسبة والاحتفاظ بها لضـــمان تنفيذ الخدمات وتقديم الدعم	طفيفة	خطير
	الكوارث الطبيعية	التعامل مع حالات الكوارث الطبيعية (إدارة استمرارية الأعمال)	محتمل	خطير
	مخاطر التراخيص	عدم القدرة على التعامل مع حالات الكوارث الطبيعية (إدارة استمرارية الأعمال)	غير مرجح	خطير
	الأمن التقليدي واســتمرارية الأعمـال والـتـعـافـي من الكوارث	إخفـاق مقـدم الخـدمـة في تنفيـذ خطط أمـان مراكز البيانات واستمرارية الأعمال والتعافي من الكوارث	محتمل	خطير

نموذج إطار عمل إدارة المخاطر				
مجال المخاطر	نطاق التحكم في المخاطر	الوصف	احتمالية المخاطر	تأثير المخاطر
مخاطر السوق والتمويل	الإضرار بالسمعة التجارية	النظام الداخلي: المخاطر المتعلقة ببعض الحوادث الهامة والعامة/ على السحابة: المخاطر المتعلقة بمقدم الخدمة السحابية أو أنشطة المستأجرين الشركاء في السحابة	مرجح جدا	خطير
	إنهاء الخدمات أو تعطلها	لم يعد من الممكن تقديم الخدمة على النحو المتوقع	محتمل	خطير
	فشل العزل	رفض الوصول إلى الخدمة مؤقتًا، مما قد يؤدي إلى مشاكل تتعلق بالسمعة أو الحرجة أو المالية	محتمل	خطير
	إدارة القدرات	عدم توفير الموارد والاستثمار في البنية الاساسية على النحو المناسب	محتمل	خطير
	مرونة البيئية أو وقت التسويق	زمن الاستجابة أو الصعوبة الشاملة في القدرة على ضبط خصائص الأنظمة (الأداء، التصميم، التقسيم) لمعالجة البيئة الديناميكية	طفيفة	خطير
	الاستجابة للحوادث	عدم قدرة مقدم الخدمة على الكشف عن الحوادث والتعامل معها والإبلاغ عنها إلى الوحدات من خلال توفير البيانات القابلة للتحليل بسهولة لتلبية المتطلبات القانونية في حالة تحقيقات التحليل الجنائي	محتمل	خطيرة

الشكل التوضيحي رقم (15) – مجالات المخاطر

استبيان تقييم المخاطر	
رقم السؤال	السؤال
	قيمة المعلومات ومدى أهميتها وحساسيتها

استبيان تقييم المخاطر	
رقم السؤال	السؤال
1	من الجهة المالكة للمعلومات؟
2	ما هي العمليات التجارية للهيئات المدعومة بالمعلومات؟
3	ما هو التصنيف الأمني للمعلومات بناءً على إرشادات الوحدات لحماية المعلومات الرسمية؟
4	هل هناك أي مخاوف محددة تتعلق بسرية المعلومات التي سيتم تخزينها أو معالجتها من خلال الخدمة السحابية؟
5	هل تحتوي البيانات على أي معلومات شخصية؟
6	من هم مستخدمو المعلومات؟
7	ما هي التصاريح التي يطلبها المستخدمون للمعلومات؟ (أي القراءة أو الكتابة أو التعديل أو الحذف)
8	ما هو القانون المنطبق على المعلومات؟
9	ما هي الالتزامات التعاقدية المنطبقة على المعلومات؟ (على سبيل المثال، الامتثال إلى مجموعة من المعايير، وما إلى ذلك.)
10	ما مدى التأثير على الهيئة في حال تم الإفصاح عن المعلومات بطريقة غير مصرح بها؟
11	ما مدى التأثير على الهيئة في حال تم المساس بسلامة المعلومات؟
12	هل تمتلك الهيئة خطط للاستجابة للحوادث وإدارتها لتقليل التأثير الناتج عن الإفصاح غير المصرح به؟
13	ما مدى التأثير على الهيئة في حال كانت المعلومات غير متوفرة؟
13.أ	ما هو أقصى حد مسموح به لفقدان البيانات الذي يمكن تحمله بعد حدوث عطل؟
13.ب	ما هي الفترة الزمنية القصوى التي يجب قبلها استعادة الحد الأدنى من مستويات الخدمات بعد حدوث عطل؟
13.ج	ما هي الفترة الزمنية القصوى التي يجب قبلها استعادة الخدمات بالكامل لتجنب تعرض أهداف العمل للخطر الدائم؟
	سيادة البيانات
14	أين يقع المقر الرئيسي لمقدم الخدمة السحابية؟
15	ما هي البلدان التي يتم تقديم الخدمات السحابية منها؟
16	في أي اختصاص قانوني سيتم تخزين بيانات الهيئة ومعالجتها؟
17	هل سيسمح مقدم الخدمة السحابية للهيئات بتحديد المواقع التي يمكن فيها تخزين بياناتهم ومعالجتها؟

استبيان تقييم المخاطر	
رقم السؤال	السؤال
18	هل تعتمد الخدمة على أي جهات خارجية (مثل المتعهدين الخارجيين أو مقاولي الباطن أو أي مقدمة خدمة سحابية آخر) مما يؤدي إلى مخاطر اختصاصية إضافية؟ إذا كانت الإجابة بنعم، فهل يمكن لمقدم الخدمة السحابية تقديم التفاصيل التالية المتعلقة بكل الجهات الخارجية المشاركة في تقديم الخدمة؟
18.أ	المقر الرئيسي للجهات الخارجية.
18.ب	البلد أو البلدان التي يتم تقديم خدماتهم منها.
18.ج	نوع الوصول إلى بيانات الهيئة التي يتم تخزينها ومعالجتها ونقلها باستخدام الخدمة السحابية
19	هل تم الإطلاع على قوانين البلد أو البلدان التي سيتم فيها تخزين البيانات ومعالجتها لتقييم كيف يمكن أن تؤثر تلك القوانين على أمن أو خصوصية المعلومات؟
20	هل تنطبق القوانين فعليًا على مقدم الخدمة السحابية أو معلومات عملائه؟ (على سبيل المثال، تستثني بعض قوانين الخصوصية أنواعًا محددة من الأعمال التجارية أو لا تنطبق على المعلومات الشخصية للأجانب.)
21	هل توفر قوانين الخصوصية المعمول بها مستوى حماية مماثل أو أعلى؟
21.أ	إذا كانت الإجابة لا، فهل ستكون الوحدات قادرة على التفاوض مع مقدم الخدمات السحابية لضمان تحديد حماية الخصوصية المماثلة في العقد؟
22	كيف يتعامل مقدم الخدمات السحابية مع طلبات الوحدات التنظيمية للوصول إلى معلومات الهيئة؟
22.أ	هل سيفصح مقدم الخدمة عن المعلومات فقط استجابة لحكم محكمة ساري؟
22.ب	هل سيخطر مقدم الخدمة الهيئة إذا كان عليها الإفصاح عن المعلومات استجابة لمثل هذا الطلب؟
22.ج	هل يُحظر على مقدم الخدمة إخطار عملائه بما في ذلك الوحدات بأنه تلقى حكم محكمة يطلب الوصول إلى معلوماتهم؟
	الخصوصية
23	هل يمكن للوحدات إجراء تقييم تأثير الخصوصية (PIA) لمقدم الخدمة لتحديد مخاطر الخصوصية المرتبطة باستخدام الخدمة السحابية جنبًا إلى جنب مع الضوابط المطلوبة لإدارتها بفعالية؟ أو هل سيمتثل مقدم الخدمة لمتطلبات الوحدات بشأن الخصوصية؟
24	هل تشتمل سياسة الخصوصية الخاصة بمقدم الخدمات السحابية على نقاط واضحة حول استخدامه للمعلومات الشخصية؟
24.أ	هل تتوافق سياسة الخصوصية لمقدم الخدمة السحابية مع متطلبات أعمال الوحدة؟
25	هل سيخطر مقدم الخدمة السحابية الوحدات في حال تم الوصول إلى بياناتهم من طرف غير مصرح له أو الإفصاح عنها له؟

استبيان تقييم المخاطر	
رقم السؤال	السؤال
26	إلى من يمكن للوحدة أو موظفيها أو عملائها تقديم شكوى إذا كان هناك انتهاك للخصوصية؟
	الحوكمة
	شروط الخدمة
27	هل سيتفاوض مقدم الخدمة السحابية مع الوحدات بشأن بنود العقود أم يكون مُلزم بقبول شروط الخدمة الموحدة؟
28	هل ستحدد شروط خدمات مقدم الخدمة السحابية واتفاقية مستوى الخدمة بوضوح كيف تحمي الخدمة سرية وسلامة وتوافر جميع معلومات الوحدة الموكلة إليها، خاصة المعلومات الرسمية، وخصوصية جميع المعلومات المحددة للهوية الشخصية؟
29	هل ستحدد شروط خدمات مقدم الخدمة السحابية ما إذا كانت الوحدة ستحتفظ بملكية بياناتها؟
30	هل سيستخدم مقدم الخدمة السحابية البيانات لأي غرض آخر بخلاف الأغراض المتعلقة بتقديم الخدمة؟
31	هل تعتمد خدمة مقدمة الخدمة السحابية على أي خدمات مقدمة من جهات خارجية؟
	الامتثال
32	هل ستسمح شروط خدمات مقدم الخدمة السحابية للهيئات بإجراء التدقيق المباشر على عمليات تنفيذ وإدارة التدابير الأمنية المعمول بها لحماية الخدمة والبيانات المتاحة بموجبها؟
32.أ	إذا كانت الإجابة بنعم، فهل يشمل ذلك إجراء عمليات فحص التحقق من الثغرات الأمنية واختبار اختراق الخدمة والبنية الاساسية الداعمة؟
32.ب	إذا كانت الإجابة لا، فهل يخضع مقدم الخدمة السحابية لتقييم منتظم رسمي مقابل معيار أو إطار أمن معلومات معترف به دوليًا تقدمه جهة خارجية مستقلة؟ (على سبيل المثال، هل هي معتمدة على أنها متوافقة مع معيار أيزو/أي إي سي 27001؟ هل خضعوا لتقييم المعيار الدولي بشأن عمليات التأكيد (ISAE) رقم 3402 المتعلق بضوابط المؤسسات الخدمية 2 النوع الثاني؟
33	هل سيسمح مقدم الخدمة السحابية للهيئة بمراجعة تقارير التدقيق الأخيرة بدقة قبل التسجيل في الخدمة؟ (على سبيل المثال، هل سيقدم مقدم الخدمات السحابية بيان الانطباق مع نسخة من تقارير التدقيق الكاملة من المدقق الخارجي ونتائج أي عمليات تدقيق داخلية حديثة؟)
34	هل سيمكن مقدم الخدمة السحابية العملاء المحتملين من إجراء فحوصات مرجعية من خلال توفير تفاصيل الاتصال لاثنين أو أكثر من عملائه الحاليين؟
35	هل قام مقدم الخدمة السحابية بنشر مدونة ممارسات الحوسبة السحابية المكتملة؟
	السرية

استبيان تقييم المخاطر	
رقم السؤال	السؤال
	المصادقة وتصاريح الدخول
36	هل ستدعم الخدمة السحابية استراتيجية إدارة الهوية الخاصة بالهيئة؟
37	هل لدى مقدم الخدمة السحابية عملية داخلية فعالة تضمن إدارة الهويات وحمايتها طوال مدة سريان الخدمات؟
38	هل لدى مقدم الخدمة عملية تدقيق فعالة يتم تنفيذها على فترات منتظمة لضمان إدارة حسابات المستخدمين وحمايتها بالشكل المناسب؟
39	هل تم تحديد الضوابط المطلوبة لإدارة المخاطر المرتبطة بالوصول الشامل الذي توفره السحابة؟
39.أ	هل تلبي الخدمة السحابية متطلبات التحكم هذه؟
40	هل يتم تشفير جميع كلمات المرور، وخاصة حسابات المسؤولين بالنسبة للنظام أو الخدمة، وفقًا لمتطلبات التعقيد؟
	تعدد المستأجرين
41	هل سيسمح مقدم الخدمة السحابية للوحدة بمراجعة تقرير تدقيق حديث من جهات خارجية (على سبيل المثال معيار الأيزو 27001 أو المعيار الدولي بشأن عمليات التأكيد (ISAE) رقم 3402 المتعلق بضوابط المؤسسات الخدمية 2 النوع الثاني) يتضمن تقييمًا للضوابط والممارسات الأمنية المتعلقة بنشر بيانات العميل على نظام المحاكاة الافتراضي وفصلها؟
42	هل سيسمح مقدم الخدمة السحابية للهيئات بإجراء اختبارات أمنية (بما في ذلك اختبارات الاختراق) لتقييم فعالية ضوابط الوصول المستخدمة لفرض فصل بيانات العميل؟
	بيئات التشغيل الموحدة
43	هل هناك معايير تصميم وتقوية مناسبة محددة وموثقة لمكونات الخدمة التي تكون الوحدة مسؤولة عن إدارتها؟
44	هل يمكن للوحدة نشر أنظمة التشغيل والتطبيقات وفقًا لمعايير التصميم أو التقوية الداخلية؟
44.أ	إذا كانت الإجابة لا، فهل لدى مقدم الخدمات السحابية معايير بناء وتقوية مناسبة تلبي متطلبات أمن أي هيئة؟
44.ب	هل تتضمن الصورة الافتراضية جدار حماية يستند إلى المضيف تم ضبط تهيئته للسماح فقط بحركة الاستقبال والإرسال (الواردة والصادرة) اللازمة لدعم الخدمة؟
44.ج	هل يسمح مقدم الخدمة السحابية بتثبيت وكلاء خدمة كشف ومنع التسلل (IDS/IDP) المستندة إلى المضيف داخل الأجهزة الافتراضية؟
45	هل يقوم مقدم الخدمة السحابية بإجراء اختبارات منتظمة لعملياته وضوابطه الأمنية؟
45.أ	هل ستزود الوحدات بنسخة من التقارير المرتبطة بها؟
46	هل يمكن إجراء اختبار اختراق للخدمة لضمان نشرها بشكل آمن؟

استبيان تقييم المخاطر	
رقم السؤال	السؤال
	إدارة التصحيحات والثغرات الأمنية
47	هل مقدم الخدمة السحابية مسؤول عن تصحيح جميع المكونات الداخلة في تكوين الخدمة السحابية؟
47.أ	في حال لم يكن مقدم الخدمة السحابية مسؤولاً عن تصحيح جميع المكونات التي تشكل الخدمة السحابية، فهل سيشارك تفاصيل التصحيح مع تحمل المسؤولية؟
48	هل تتضمن بنود خدمة مقدم الخدمة السحابية أو اتفاقية مستوى الخدمة مستويات الخدمة لإدارة التصحيحات والثغرات الأمنية التي تتضمن نافذة الحد الأقصى للتعرض المحدد؟
49	هل سيسمح مقدم الخدمة السحابية للوحدة بإجراء تقييمات منتظمة للثغرات الأمنية؟
50	هل ستتضمن شروط الخدمة أو اتفاقية مستوى الخدمة بندًا للتعويض عن الانتهاكات الناجمة عن الثغرات الأمنية في الخدمة؟
50.أ	إذا كانت شروط الخدمة أو اتفاقية مستوى الخدمة تتضمن بندًا للتعويض عن الانتهاكات الناجمة عن الثغرات الأمنية في الخدمة، فهل توفر مستوى مناسبًا من التعويض في حالة حدوث خرق؟
	التشفير
51	هل تستخدم الخدمة السحابية فقط بروتوكولات التشفير والخوارزميات المعتمدة؟
52	من سيكون مسؤولا عن إدارة العملية؟
53	هل لدى مقدم الخدمة خطة إدارة رئيسية تلبي متطلبات الوحدات؟
	التهديد الداخلي لمقدم الخدمة السحابية
54	هل سيقوم مقدم الخدمات السحابية بإجراء فحص مناسب قبل توظيف جميع الموظفين الذين لديهم حق الوصول إلى بيانات الهيئة؟
54.أ	هل يقوم مقدم الخدمات السحابية بإجراء فحوصات مستمرة خلال فترة التوظيف؟
55	إذا كان مقدم الخدمة السحابية يعتمد على جهة خارجية لتقديم أي جزء من خدمته، فهل ستقوم الجهة الخارجية بإجراء فحص مناسب قبل التوظيف لجميع الموظفين الذين لديهم حق الوصول إلى بيانات العملاء؟
56	هل سيحصل مقدم الخدمة السحابية على خدمة إدارة المعلومات الأمنية والأحداث (SIEM) التي تسجل وتراقب جميع حالات الوصول المنطقي إلى بيانات العميل؟
57	هل يقوم مقدم الخدمة السحابية بفرض الفصل بين الواجبات لضمان حماية سجلات التدقيق من التعديل والحذف غير المصرح به؟
58	هل تتطلب شروط الخدمة أو اتفاقية مستوى الخدمة من مقدم الخدمة السحابية الإبلاغ عن الوصول غير المصرح به إلى بيانات العملاء من قبل موظفيه؟

استبيان تقييم المخاطر	
رقم السؤال	السؤال
58.أ	إذا كانت الإجابة بنعم، فهل يُطلب من مقدم الخدمة السحابية تقديم تفاصيل حول الحادث إلى الوحدات المتضررة لتمكينها من تقييم وإدارة التأثير ذي الصلة؟
	ثبات البيانات
59	هل لدى مقدم الخدمة السحابية عملية قابلة للتدقيق للتعقيم الآمن لوسائط التخزين قبل إتاحتها لعميل آخر؟
60	هل لدى مقدم الخدمة السحابية عملية قابلة للتدقيق للتخلص الآمن أو تدمير معدات تكنولوجيا المعلومات والاتصالات ووسائط التخزين (مثل محركات الأقراص الصلبة والأشرطة الاحتياطية وما إلى ذلك) التي تحتوي على بيانات العملاء؟
	الأمن المادي
61	هل يمكن مراجعة ضوابط الأمن المادي لمقدم الخدمة السحابية أو تقييمها مباشرة من قبل الوحدة، إذا كان يمكن تنفيذ هذا الأمر من الناحية العملية؟
61.1	إذا كانت الإجابة لا، فهل سيسمح مقدم الخدمة السحابية للوحدة بمراجعة تقرير تدقيق حديث صادر عن جهة خارجية (على سبيل المثال معيار الأيزو 27001 أو المعيار الدولي بشأن عمليات التأكيد (ISAE) رقم 3402 المتعلق بضوابط المؤسسات الخدمية 2 النوع الثاني) يتضمن تقييمًا لضوابط الأمن المادي الخاصة بهم؟
62	هل تلبي ضوابط الأمن المادي لمقدم الخدمة السحابية الحد الأدنى من المتطلبات على النحو المحدد في إرشادات أمان الوحدات لحماية المعلومات المخزنة في الخدمة السحابية؟
	سلامة البيانات
63	هل سيوفر مقدم الخدمات السحابية خدمات النسخ الاحتياطي للبيانات أو الأرشفة كجزء من الخدمة الموحدة التي يقدمها للحماية من فقدان البيانات أو تلفها؟ إذا لم يكن الأمر كذلك، فهل يقدم خدمات النسخ الاحتياطي أو الأرشفة كخدمة إضافية للحماية من فقدان البيانات وتلفها؟
64	كيف يتم توفير خدمات النسخ الاحتياطي والأرشفة للبيانات؟
65	هل تحدد اتفاقية مستوى الخدمة جدول النسخ الاحتياطي للبيانات؟
66	هل تضمن خدمة النسخ الاحتياطي أو الأرشفة تلبية متطلبات العمل المتعلقة بالحماية من فقدان البيانات؟ (أي هل تدعم الخدمة هدف نقطة استعادة الأعمال؟)
67	ما هو مستوى التفصيل الذي يقدمه مقدم الخدمة السحابية لاستعادة البيانات؟
68	ما هي إجراءات مقدم الخدمة السحابية لبدء عملية الاستعادة؟
69	هل يقوم مقدم الخدمة السحابية بإجراء عمليات استعادة الاختبار بانتظام لضمان إمكانية استرداد البيانات من الوسائط الاحتياطية؟
70	هل تحتاج الوحدة إلى تنفيذ استراتيجية نسخ احتياطي للبيانات للتأكد من أنها يمكن أن تتعافى من حادث يؤدي إلى فقدان البيانات أو الفساد؟

استبيان تقييم المخاطر	
رقم السؤال	السؤال
71	هل تدعم استراتيجية النسخ الاحتياطي والأرشفة المقترحة الوحدة في الوفاء بالتزاماتها؟
	الإتاحة
	اتفاقية مستوى الخدمات
72	هل تتضمن اتفاقية مستوى الخدمة نسبة متوقعة ودنيا لأداء التوافر على مدى فترة محددة بوضوح؟
72.أ	إذا تضمنت اتفاقية مستوى الخدمة نسبة متوقعة ودنيا لأداء التوافر على مدى فترة محددة بوضوح، فهل يتم استيفاء متطلبات أعمال الوحدات للتوافر؟ على سبيل المثال، هل تدعم الخدمة هدف وقت الاسترداد ونافذة المقاطعة المقبولة الخاصة بالعمل؟
73	هل تتضمن اتفاقية مستوى الخدمة نوافذ انقطاع محددة ومجدولة؟
73.أ	إذا تضمنت اتفاقية مستوى الخدمة نوافذ انقطاع الخدمة محددة ومجدولة، فهل تؤثر نوافذ الانقطاع المحددة على العمليات التجارية؟
73.ب	إذا لم تتضمن اتفاقية مستوى الخدمة نوافذ انقطاع الخدمة محددة ومجدولة، فهل قام مقدم الخدمة السحابية بتطبيق التقنيات التي تمكنه من أداء أعمال الصيانة دون الحاجة إلى تنفيذ عمليات الانقطاع؟
74	هل تتضمن اتفاقية مستوى الخدمة بند للتعويض عن مخالفة نسب التوافر المضمونة؟
74.أ	إذا تضمنت اتفاقية مستوى الخدمة بند للتعويض عن مخالفة نسب التوافر المضمونة، فهل يوفر ذلك مستوى مناسبًا من التعويض في حالة مخالفة مقدم الخدمة السحابية لاتفاقية مستوى الخدمة؟
	هجمات الحرمان من الخدمة
75	هل يستخدم مقدم الخدمة السحابية البروتوكولات والتقنيات التي يمكن أن تحمي من هجمات الحرمان من الخدمات (DDoS)؟
75.أ	إذا كانت الإجابة بنعم، فهل يؤثر تمكين خدمات الحماية من هجمات الحرمان من الخدمات (DDoS) لمقدم الخدمة السحابية على الإجابة على الأسئلة رقم 15 و16 و17؟
76	هل يمكن للهيئة تحديد أو ضبط تهيئة حدود استخدام الموارد للحماية من هجمات الحرمان الاقتصادي للاستدامة (EDoS) أو التعرض لهجمات غير المتوقعة (bill shock)؟
	توافر الشبكة وأدائها
77	هل توفر خدمات الشبكة التي تديرها الهيئة بصفة مباشرة أو تشارك في إدارتها، مستوى مناسبًا من التوافر؟
78	هل توفر خدمات الشبكة التي تديرها الهيئة بصفة مباشرة أو تشارك في إدارتها مستوى كافياً من التكرار أو تحمل الأخطاء؟
79	هل توفر خدمات الشبكة التي تديرها الهيئة بصفة مباشرة أو تشارك في إدارتها، مستوى مناسبًا من عرض النطاق الترددي (إنتاجية الشبكة)؟

استبيان تقييم المخاطر	
رقم السؤال	السؤال
80	هل يعتبر زمن الاستجابة بين شبكات الوحدة وخدمة مقدم الخدمات السحابية عند مستويات مقبولة لتحقيق تجربة المستخدم المطلوبة؟
80.أ	إذا كانت الإجابة لا، فهل تدير الوحدة عمليات وقت الاستجابة على خدمات الشبكة بصفة مباشرة أم تشترك في إدارتها؟
80.ب	هل يمكن حل المشكلة سواء عن طريق مقدم الشبكة السحابية أو الوحدة؟
81	هل مستويات فقدان البيانات بين شبكات الوحدة وخدمة مقدم الخدمة السحابية في الحد المسموح به لتحقيق تجربة المستخدم المطلوبة؟
81.أ	إذا كانت الإجابة لا، فهل تحدث خسارة البيانات على خدمات الشبكة التي تديرها الوحدة بصفة مباشرة أو تشارك في إدارتها؟
81.ب	هل يمكن حل المشكلة سواء عن طريق مقدم الشبكة السحابية أو الوحدة؟
	استمرارية الأعمال والتعافي من الكوارث
82	هل يمتلك مقدم الخدمة السحابية خطط لاستمرارية الأعمال والتعافي من الكوارث؟
83	هل سيسمح مقدم الخدمة السحابية للهيئة بمراجعة خطط استمرارية أعمالها والتعافي من الكوارث؟
84	هل تغطي خطط مقدم الخدمات السحابية استعادة بيانات الوحدة أم فقط استعادة الخدمة؟
85	إذا كانت خطط مقدم الخدمة السحابية تغطي استعادة بيانات الوحدة، فهل يتم إعطاء الأولوية لاسترداد بيانات العملاء؟
85.أ	إن كان سيتم تنفيذ هذا الأمر، فيرجى توضيح كيفية التنفيذ؟ وهل سيتم إعطاء الأولوية للهيئات بناءً على الحجم وقيمة العقد؟
86	هل يختبر مقدم الخدمة السحابية خطط استمرارية الأعمال والتعافي من الكوارث بشكل منتظم؟
86.أ	إذا كانت الإجابة بنعم، ما مدى انتظام إجراء مثل هذه الاختبارات؟
86.ب	هل سيزود مقدم الخدمة الوحدات بنسخة من التقارير ذات الصلة؟
	الاستجابة للحوادث وإدارتها
87	هل لدى مقدم الخدمة السحابية عملية رسمية للاستجابة للحوادث وإدارتها وخطط تحدد بوضوح كيفية اكتشافه لحوادث أمن المعلومات والاستجابة لها؟
87.أ	إذا كانت الإجابة بنعم، فهل سيزود الوحدة بنسخة من عمليته وخططه لتمكينها من تحديد ما إذا كانت مناسبة وملائمة؟
88	هل يقوم مقدم الخدمة السحابية باختبار عملية الاستجابة للحوادث وإدارتها وخططها على أساس منتظم؟
89	هل سيشرك مقدم الخدمة السحابية الوحدات عند اختبار عمليات وخطط الاستجابة للحوادث وإدارتها؟

استبيان تقييم المخاطر	
رقم السؤال	السؤال
90	هل يزود مقدم الخدمة السحابية موظفيه بالتدريب المناسب على الاستجابة للحوادث وعمليات الإدارة والخطط لضمان استجابتهم للحوادث بكفاءة وفعالية؟
91	هل تحدد بنود خدمة مقدم الخدمات السحابية أو اتفاقية مستوى الخدمة بوضوح عمليات الدعم التي سيقدمها إلى الوحدة في حالة وقوع حادث يتعلق بأمن المعلومات؟
91.أ	هل سيقوم مقدم الخدمة السحابية بإخطار الوحدات عند اكتشاف أو الإبلاغ عن حادث قد يؤثر على أمن معلوماتهم أو الأنظمة ذات الصلة؟
91.ب	تحديد مسؤول الاتصال وقناة الاتصال الذين تستعين بهم الوحدات للإبلاغ عن حوادث أمن المعلومات المشتبه في وقوعها؟
91.ج	تحديد أدوار ومسؤوليات كل طرف أثناء حادث أمن المعلومات؟
91.د	تزويد الوحدات بإمكانية الوصول إلى الأدلة (مثل سجلات التدقيق المختومة أو لقطات التحليل الجنائي للآلات الافتراضية وما إلى ذلك) لتمكينها من إجراء تحقيقاتها الخاصة في الحادث؟
91.ه	تقديم معلومات كافية لتمكين الهيئة من التعاون الفعال مع التحقيقات التي تجريها الجهاتالتنظيمية؟
91.و	تحديد الطرف المسؤول عن استعادة البيانات والخدمات بعد وقوع حادث أمن المعلومات؟
91.ز	مشاركة تقارير ما بعد الحادث مع الوحدات المتضررة لتمكينها من فهم سبب الحادث واتخاذ قرار مستنير حول ما إذا كان يجب الاستمرار في استخدام الخدمة السحابية؟
91.ح	تحديد نطاق (حدود) وأحكام العقد المتعلقة بالتأمين والالتزامات والتعويضات في حالات حوادث أمن المعلومات؟
92	هل يخطط مقدمو الخدمات السحابية للاستجابة للحوادث وإجراءات الإدارة (أو يمتثلون إلى) السياسة والإجراءات الداخلية للوحدة، هذا لا يعوق أو يؤخر قدرة الهيئة على إدارة الحوادث في الوقت المناسب وبطريقة فعالة؟

الشكل التوضيحي رقم (16) – استبيان تقييم المخاطر