الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1750

(2020/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن البيانات – أمن البيانات الضخمة

مبادئ توجيهية بشأن أمن البيانات الضخمة كخدمة من أجل موردي خدمات البيانات الضخمة

التوصية ITU-T X.1750

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن (1)	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
أمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
أمن إنترنت الأشياء (IoT)	X.1369–X.1360
أمن أنظمة النقل الذكية (ITS)	X.1389–X.1370
أمن سجل الحسابات الموزع	X.1429–X.1400
أمن سجل الحسابات الموزع	X.1449–X.1430
البروتوكول الأمني (2)	X.1459–X.1450
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولّد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
أمن البيانات	
أمن البيانات الضخمة	**X.1759–X.1750**
أمن شبكات الجيل الخامس	X.1819–X.1800

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1750

مبادئ توجيهية بشأن أمن البيانات الضخمة كخدمة من أجل موردي خدمات البيانات الضخمة

ملخص

البيانات الضخمة كخدمة (BDaaS) هي فئة خدمة سحابية تتمثل فيها الإمكانات المقدمة لعميل الخدمة السحابية في القدرة على جمع البيانات الضخمة وتخزينها وتحليلها وعرضها وإدارتها، كما هو موصف في التوصية ITU-T Y.3600. ومع النمو الكبير في أحجام البيانات والتطور السريع في الأعمال التجارية للبيانات الضخمة، أصبحت البنية التحتية للبيانات الضخمة مرفقاً محورياً لتوفير خدمات البيانات الضخمة كخدمة. ونتيجةً لذلك، برزت مشكلات أمنية كبيرة فيما يتعلق بالبيانات الضخمة كخدمة. فعلى سبيل المثال، لا تأخذ تصميمات برمجيات البيانات الضخمة مفتوحة المصدر في بعض الأوقات الأمن في الاعتبار منذ البداية. والتكنولوجيات الجديدة التي تطرحها تحليلات البيانات الضخمة يمكن أن تؤدي أيضاً إلى فشل تدابير الحماية الأمنية التقليدية. وتحلل التوصية ITU-T X.1750 التحديات الأمنية التي تواجهها البيانات الضخمة كخدمة، وتحدد الأدوار والمسؤوليات الأمنية من أجل توفير البيانات الضخمة كخدمة، إضافةً إلى إطار أمني لبنية تحتية للبيانات الضخمة. وتوصف التوصية أيضاً تدابير الحماية الأمنية التي ينبغي تنفيذها من أجل الخدمات والمكونات المتعلقة بالبيانات الضخمة كخدمة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1750	2020-09-03	17	11.1002/1000/14266

مصطلحات أساسية

البيانات الضخمة كخدمة، مبادئ توجيهية أمنية، تدابير أمنية.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات (ITU) هو وكالة الأمم المتحدة المتخصصة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1750

مبادئ توجيهية بشأن أمن البيانات الضخمة كخدمة من أجل موردي خدمات البيانات الضخمة

1 مجال التطبيق

تحلل هذه التوصية التحديات الأمنية التي تواجهها البيانات الضخمة كخدمة (BDaaS) وتقدم إلى موردي خدمات البيانات الضخمة (BDSP) مبادئ توجيهية ترمي إلى تأمين البيانات BDaaS. وتحدد التوصية أيضاً الأدوار والمسؤوليات الأمنية لمكونات البيانات BDaaS وإطاراً أمنياً للبنية التحتية للبيانات الضخمة، بما يشمل المنصّات والتطبيقات والتحليلات والسطوح البينية والنظام الإيكولوجي للبيانات BDaaS. كما تحدد هذه التوصية تدابير الحماية الأمنية التي ينبغي اتخاذها في الأنشطة أو المكونات المتصلة بالبيانات BDaaS.

وتشكل هذه التوصية وصفاً رفيع المستوى للمتطلبات الأمنية اللازمة لتنفيذ البيانات BDaaS بالتركيز على هذه البيانات. وتشمل البيانات BDaaS مورّدي البنى التحتية للبيانات الضخمة (BDIP) وموردي تطبيقات البيانات الضخمة (BDAP). ولا يشمل مجال تطبيق هذه التوصية مبادئ توجيهية لموردي البنى التحتية للبيانات الضخمة وموردي تطبيقات البيانات الضخمة، ولا إرشادات مفصَّلة لتنفيذ البيانات BDaaS.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع للمراجعة، يرجى من مستعملي هذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1601] التوصية ITU-T X.1601 (2015)، *إطار أمني للحوسبة السحابية.*

[ITU-T X.1631] التوصية ITU-T X.1631 (2015)، *تكنولوجيا المعلومات – تقنيات الأمن – مدونة قواعد الممارسات المتعلقة بأمن المعلومات استناداً إلى المعيار ISO/IEC 27002 من أجل الخدمات السحابية.*

[ITU-T X.1641] التوصية ITU-T X.1641 (2016)، *مبادئ توجيهية لأمن بيانات عملاء الخدمات السحابية.*

[ITU-T Y.3600] التوصية ITU-T Y.3600 (2015)، *البيانات الضخمة – متطلبات وإمكانات قائمة على الحوسبة السحابية.*

[ISO/IEC 27000] المعيار ISO/IEC 27000:2018، *تكنولوجيا المعلومات – تقنيات الأمن – أنظمة إدارة أمن المعلومات – نظرة عامة ومصطلحات.*

[ISO/IEC 27036-3] المعيار ISO/IEC 27036-3:2013، *تكنولوجيا المعلومات – تقنيات الأمن – أمن المعلومات في العلاقات مع المورّدين – الجزء 3: مبادئ توجيهية بشأن أمن سلسلة توريد تكنولوجيا المعلومات والاتصالات.*

[ISO 28000] المعيار ISO 28000:2007، *توصيف لأنظمة إدارة الأمن في سلسلة التوريد.*

3 التعاريف

1.3 المصطلحات المعرَّفة في مراجع أخرى

تُستخدم في هذه التوصية المصطلحات التالية المعرَّفة في مراجع أخرى:

1.1.3 البيانات الضخمة [ITU-T Y.3600]: هي نموذج لتمكين جمع مجموعات بيانات ضخمة جداً ذات خصائص غير متجانسة وتخزينها وإدارتها وتحليلها وعرضها، مع احتمال تحقيق ذلك في وجود قيود في الوقت الفعلي.

ملاحظة – من الأمثلة لخصائص مجموعات البيانات كِبَر حجمها وزيادة سرعتها وشدة تنوعها وغيرها من الخصائص.

2.1.3 البيانات الضخمة كخدمة (BDaaS) [ITU-T Y.3600]: هي فئة خدمة سحابية تتمثل فيها الإمكانات المقدمة لعميل الخدمة السحابية في القدرة على جمع البيانات وتخزينها وتحليلها وعرضها وإدارتها باستعمال تكنولوجيا البيانات الضخمة.

3.1.3 مصدر البيانات الضخمة [b-ITU-T Y.3602]: المعلومات التي تسجِّل مسار البيانات التاريخي وفقاً للعمليات المتصلة بدورة حياتها في النظام الإيكولوجي للبيانات الضخمة.

4.1.3 الحوسبة السحابية [b-ITU-T Y.3500]: نموذج للتمكين من النفاذ الشبكي إلى مجموعة قابلة للزيادة ومرنة من الموارد المادية أو الافتراضية التي يمكن تقاسمها والتزود بها وإدارتها على أساس الخدمة الذاتية وعند الحاجة.

5.1.3 خدمة سحابية [b-ITU-T Y.3500]: قدرة أو عدد أكبر من القدرات تُقدم عن طريق الحوسبة السحابية وتُلبى باستخدام سطح بيني معلن.

6.1.3 البيانات الشرحية [b-ITU-T M.3030]: البيانات التي توضح بيانات أخرى.

7.1.3 تحدٍّ أمني [ITU-T X.1601]: "عقبة" أمنية مختلفة عن التهديدات الأمنية المباشرة، تنجم عن طبيعة الخدمات السحابية وبيئتها التشغيلية، بما في ذلك التهديدات "غير المباشرة".

8.1.3 تهديد [ISO/IEC 27000]: سبب محتمل لحادث غير مرغوب قد يُلحق ضرراً بالنظام أو المنظمة.

9.1.3 نقطة ضعف [b-NIST-SP-800-30]: مكمن ضعف في نظام المعلومات أو إجراءات أمن النظام أو أدوات الرقابة الداخلية أو التنفيذ يمكن استغلاله من جانب مصدر التهديد.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرِّف هذه التوصية المصطلحات التالية:

1.2.3 أصول البيانات: موارد البيانات المسجَّلة إلكترونياً التي تمتلكها أو تتحكم فيها أي منظمة.

4 المختصرات والتسميات المختصرة

تستخدم هذه التوصية المختصرات والتسميات المختصرة التالية:

API السطح البيني لبرمجة التطبيقات *(Application Programming Interface)*

ABAC التحكّم في النفاذ القائم على النعوت *(Attribute-Based Access Control)*

BDaaS البيانات الضخمة كخدمة *(Big Data as a Service)*

BDAP مُورِّد تطبيقات البيانات الضخمة *(Big Data Application Provider)*

BDIP مُورِّد البنية التحتية للبيانات الضخمة *(Big Data Infrastructure Provider)*

BDSN الشركاء في خدمات البيانات الضخمة *(Big Data Service Partners)*

BDSP مُورِّد خدمات البيانات الضخمة *(Big Data Service Provider)*

BDSU مُستعمِل خدمات البيانات الضخمة *(Big Data Service User)*

CSC عميل الخدمة السحابية *(Cloud Service Customer)*

DP مُورِّد البيانات *(Data Provider)*

IT تكنولوجيا المعلومات *(Information Technology)*

PII المعلومات المحدِّدة لهوية الأشخاص *(Personally Identifiable Information)*

PKI البنية التحتية للمفاتيح العمومية *(Public Key Infrastructure)*

SAML لغة وسم التأكيدات الأمنية *(Security Assertion Markup Language)*

SDK مجموعة أدوات تطوير البرمجيات *(Software Development Kit)*

SSL طبقة مقابس مأمونة *(Secure Sockets Layer)*

TLS أمن طبقة النقل *(Transport Layer Security)*

USB ناقل عام بالتسلسل *(Universal Serial Bus)*

5 الاصطلاحات

يتعين فهم العبارات التالية في هذه التوصية على النحو التالي:

"**يجب**" تدل على متطلَّب إلزامي يجب التقيّد به بصرامة، ولا يُسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

"**يوصى**" تدل على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا يتعين تقدم هذا المتطلب لزعم الامتثال.

"**يحظر**" تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم الامتثال لهذه التوصية.

"**من الجائز**" تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا يرمي هذا المصطلح إلى إلزام تنفيذ البائع بتقديم هذا الخيار الذي يمكن أن يقدمه مشغل الشبكة أو مورد الخدمة اختيارياً. وبالأحرى، فإن البائع يمكنه إدراج هذه الخاصية اختيارياً ويدعى إلى الامتثال لهذه المواصفة في نفس الوقت.

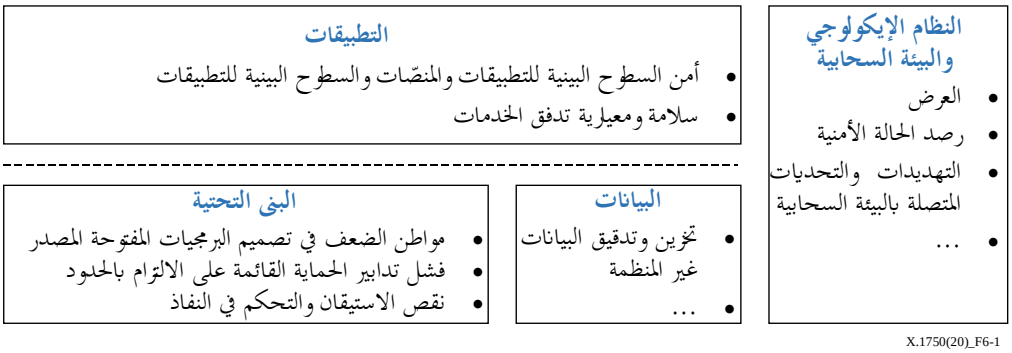
6 التهديدات والتحديات الأمنية التي قد تتعرض لها البيانات الضخمة كخدمة

يبين هذا القسم من التوصية التهديدات والتحديات الأمنية التي قد تتعرض لها البيانات الضخمة كخدمة (BDaaS). وتوصَّف في التوصية [ITU-T Y.3600] البيانات BDaaS القائمة على الحوسبة السحابية. وفيما يتعلق بالبيانات BDaaS، ينبغي أن تؤخذ في الاعتبار التحديات الأمنية المتصلة ببيئات الحوسبة السحابية، المبيّنة في القسم 8 من التوصية [ITU-T X.1601]. ثم تأتي هذه التوصية لتبيّن التهديدات والتحديات الأمنية التي قد تتعرض لها قدرتان وخدمتان محددتان من قدرات وخدمات البيانات BDaaS، ألا وهما منصّات البيانات الضخمة كخدمة والبرمجيات المتعلقة بالبيانات الضخمة كخدمة (إدراكاً لاشتمال النظام الإيكولوجي للبيانات BDaas على موردي البيانات (DP) وموردي تطبيقات البيانات الضخمة (BDAP) وموّردي البنى التحتية للبيانات الضخمة (BDIP))، وتشمل هذه التهديدات والتحديات الأمنية ما يلي:

- مواطن الضعف في البنى التحتية للبيانات الضخمة وفشل التدابير الأمنية؛
- مشاكل التخزين والتدقيق في البيانات غير المنظمة؛

- أمن وتنظيم السطوح البينية للتطبيقات والمنصّات وتدفق الخدمات؛
- شواغل أمنية أخرى مثل مسائل الثقة والاستيقان والعرض.

ويبين الشكل 6-1 معماريةً للتحديات الأمنية التي قد تتعرض لها البيانات BDaaS.



الشكل 6-1 – التحديات الأمنية التي قد تتعرض لها البيانات الضخمة كخدمة

1.6 التحديات الأمنية التي قد تتعرض لها البنى التحتية للبيانات الضخمة

يمكن أن تتألف البنى التحتية للبيانات الضخمة من مكوّنات مختلفة، إما تجارية المصدر أو مفتوحة المصدر. وقد لا يراعي تصميم بعض هذه المكونات منذ البداية مسألة الأمن، الأمر الذي قد يُعرِّضها لمخاطر أمنية من بينها ما يلي:

- انعدام أمن شفرة المصدر وانعدام الآليات الأمنية في المكونات المفتوحة المصدر؛
- اتسام المنصّات المفتوحة والمنصّات بين الميادين بخصائص تطْمِس الحدود الأمنية التقليدية، وهو ما يؤدي إلى فشل تدابير الحماية القائمة على الالتزام بالحدود؛
- احتمال أن يؤدي نقص آليات الاستيقان والتحكم في النفاذ المناسبة للأدوار المختلفة إلى وقوع انتهاكات.

2.6 التحديات الأمنية التي قد تتعرض لها تطبيقات البيانات الضخمة

تضم البنية التحتية للبيانات الضخمة مجموعةً متنوعة من التطبيقات ذات المركزية العالية ونماذج خدمات معقّدة. ومن التحديات الأمنية التي قد تتعرض لها تطبيقات البيانات الضخمة ما يلي:

- احتمال افتقار السطوح البينية لبرمجة التطبيقات (API) ومجموعات أدوات تطوير البرمجيات (SDK) والسطوح البينية للتطبيقات إلى قدرتَيْ التحقق الأمني والتحكم في الإرسال؛
- ضرورة تتبّع تنفيذ تطبيقات المستعمِلين وتدقيقها وتحديد مواقعها لكفالة أمن منطق عملها.

3.6 التحديات الأمنية التي قد تتعرض لها البيانات

تتعامل البنى التحتية للبيانات الضخمة وتطبيقاتها مع كميات ضخمة من البيانات. وفي نظام إيكولوجي للبيانات الضخمة، تشتمل أنماط البيانات على البيانات المنظمة والبيانات شبه المنظمة والبيانات غير المنظمة. وغالباً ما تُخزَّن البيانات المنظمة في قواعد بيانات قد تكون منظمة وفقاً لنماذج مختلفة من قبيل النموذج العلائقي والنموذج الوثائقي والنموذج القائم على قيمة المفتاح ونموذج الرسوم البيانية. أما البيانات شبه المنظمة، فهي لا تتفق مع البنية الرسمية لنماذج البيانات لكنّها تتضمن شارات أو علامات لتحديد البيانات. أما البيانات غير المنظمة، فهي غير خاضعة لنموذج بيانات محدد سلفاً وغير منظمة بأي كيفية محددة. ويمكن أن توجد أنساق مختلفة، كالنصوص وجداول البيانات والمنتجات الفيديوية والمسموعة والصور والخرائط، في جميع أنماط البيانات (انظر [ITU-T Y.3600]). وتُستخدم هذه البيانات في مراحل التخزين والتحليل والحساب وغيرها من مراحل خدمات البيانات. ومن التحديات الأمنية التي قد تتعرض لها البيانات ما يلي:

- لزوم وجود تدابير أمنية (من بينها أنظمة التحكم في النفاذ) تضمن سرية البيانات وتدعم، في الوقت ذاته، كفاءة تشغيلها؛

- تدقيق البيانات غير المنظمة؛
- خطر تسرّب المعلومات المتعلقة بالخصوصية الشخصية إذا كانت البيانات مفتوحة أو مشتركة؛
- ضرورة تطبيق التدابير الأمنية التقليدية المبيّنة في التوصية [ITU-T X.1601] على البيانات الشرحية نظراً لاتسامها بنفس خصائص البيانات المنشورة على الويب.

من التحديات الأمنية المحتمل رصدها عند التعامل مع مصدر البيانات: تلوّث السجلات أو التلاعب الخبيث بها في جميع مراحل سلسلة معالجة المصدر، ووجود كيانات غير مصرّح لها بذلك في عملية معالجة أو تبادل بيانات المصدر، ووجود شفرات غير أصلية لمعالجة مصدر البيانات، فضلاً عن تعرّض بيانات المصدر ذاتها لتحديات أمنية.

4.6 التحديات الأمنية التي قد يتعرض لها النظام الإيكولوجي للبيانات الضخمة كخدمة

وفقاً للتوصية [ITU-T Y.3600]، يتألف النظام الإيكولوجي للبيانات الضخمة كخدمة (BDaaS)، من أدوار وأدوار فرعية تؤديها مختلف الأطراف أو المكوّنات المقدِّمة لخدمات البيانات الضخمة والمستهلكة لها. ويلزم أن يقوم النظام الإيكولوجي للبيانات BDaaS بوضع خطط التدابير الأمنية، وتصميمها، وتنفيذها، في مراحل البناء والعمل والتدقيق وغيرها من مراحل مصدر الخدمات. وتشمل التحديات الأمنية التي قد تتعرض لها خدمات البيانات الضخمة ما يلي:

- ضرورة استمرار رصد أفعال المستعمِلين وأحوال الشبكات وحالة الموارد وما إلى ذلك للتأقلم مع تغيّر التهديدات؛
- نشوء نواقل جديدة للتهديدات وانعدام آليات الحماية الممكنة؛
- عدم القدرة على إرساء الثقة بين مختلف الأطراف الفاعلة بمن فيهم مالكو البيانات والأجهزة (لجمع البيانات)؛
- أمن عملية إنشاء الأمثلة الافتراضية، مثل التشكيل الأمني وسلامة الصور الافتراضية؛
- إمكانية وجود سلسلة إمداد معقدة في النظام الإيكولوجي للبيانات الضخمة – حتى الطرف المتعاقِد الذي لم تتعاقد معه المنظمة المعنية مباشرةً قد يؤثر على استمرارية أعمالها.
- ينبغي تحليل المخاطر المتصلة بسلسلة الإمداد واتخاذ التدابير اللازمة، ومنها التدابير الأمنية المحددة في [ISO/IEC 27000] [ISO 28000].

7 مفاهيم رفيعة المستوى بشأن البيانات الضخمة كخدمة – الاعتبارات الأمنية للبيانات الضخمة كخدمة ودور موردي خدمات البيانات الضخمة

توصف التوصية [ITU-T Y.3600] معماريةً عامة ومتعددة المستويات لتكنولوجيا البيانات الضخمة تتألف من مكوّنات وظيفية منطقية. وبناءً على هذه المعمارية، تشمل القدرات الأمنية لخدمات البيانات الضخمة أمن الأنظمة وأمن البيانات كليهما.

ومن منظور الأنظمة، تشمل المتطلبات الأمنية لأنظمة البيانات الضخمة كخدمة (BDaaS) قدرات كل من الوحدات الوظيفية المتصلة بها وهي: 1) البنية التحتية للبيانات الضخمة؛ 2) إدارة تطبيقات البيانات الضخمة؛ 3) أمن السطوح البينية؛ 4) تشغيل منصّات البيانات الضخمة والحفاظ على أمنها (النظام الإيكولوجي للبيانات BDaaS).

وتبيّن التوصية [ITU-T Y.3600]، على وجه الخصوص، أن البيانات BDaaS تشتمل على عنصرين أساسيين، هما:

- مورّدو البنية التحتية للبيانات الضخمة (BDIP): يمكنهم استعمال الخدمات السحابية من أنماط قدرات البنى التحتية السحابية، مثل الحوسبة كخدمة وتخزين البيانات كخدمة والبنى التحتية كخدمة والشبكات كخدمة، لتقديم خدمات البيانات الضخمة كجمع البيانات ومعالجتها وإدارتها.
- مورّدو تطبيقات البيانات الضخمة (BDAP): يقدمون تطبيقات تحليل البيانات وعرضها وتطبيقات أخرى للبيانات الضخمة.

ومن منظور البيانات، تشمل المتطلبات الأمنية كل نشاط في عملية تطوير أعمال خدمات البيانات. فضلاً عن ذلك، تضم قدرات خدمات البيانات الضخمة أيضاً المتطلبات الأمنية للبيانات الشرحية وسلسلة الإمداد بالبيانات.

ومن وجهة النظر النظامية للبيانات BDaaS، تحدد التوصية [ITU-T Y.3600] سياق أنظمة هذه البيانات، بما في ذلك الأدوار والأنشطة وتدفق البيانات وتدفق الخدمات.

وفيما يتعلق بالأدوار [ITU-T Y.3600]، يُعنى موردو خدمات البيانات الضخمة (BDSP) بتقديم خدمات البيانات BDaaS، وبالتالي فهم المسؤولون عن ضمان أمن هذا البيانات والحد من المخاطر التي قد تتعرض لها. ويوصى بأن يأخذ موردو خدمات البيانات الضخمة (مورّدو البنى التحتية للبيانات الضخمة وموردو تطبيقات البيانات الضخمة) أمن الأنظمة وأمن البيانات كليهما في اعتبارهم عند الاضطلاع بالأنشطة المتعلقة بالبيانات BDaaS.

8 التدابير الأمنية المتعلقة بالبيانات الضخمة كخدمة

1.8 التدابير الأمنية اللازمة للبنى التحتية للبيانات الضخمة

1.1.8 أمن أصول الأنظمة

1.1.1.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- وضع استراتيجيات لإدارة أمن أصول الأنظمة، وتوضيح الأهداف والمبادئ المتعلقة بأمن هذه الأصول؛
- وضع سياسات وإجراءات لإدارة إنشاء أصول الأنظمة وتشغيلها، تشمل عمليات تخطيطها وتصميمها وشرائها وتطويرها وتشغيلها وصيانتها وتخريدها؛
- إنشاء آلية لتسجيل أصول الأنظمة، وإعداد قائمة بهذه الأصول، وتحديد مسألة المسؤولية عن أمن أصول الأنظمة والأطراف المعنية بها، وتحديث المعلومات المتعلقة بهذه الأصول بانتظام؛
- وضع وتنفيذ إجراءات لتصنيف أصول الأنظمة وتوسيمها؛
- الانتظام في عمليات تدقيق وتحديث أصول تكنولوجيا المعلومات (IT) وسياسات إدارة أمنها.

2.1.1.8 المتطلبات التعزيزية

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- تحديد الضوابط المتاحة لإدارة الأصول، كتلك الموصفة في التوصية [ITU-T X.1631]، بهدف إجراء عمليات جرد مكوّنات أصول الأنظمة وتسجيلها وتدقيقها ورصدها؛
- وضع إجراءات لتقييم المخاطر التي قد تتعرض لها أصول أنظمة البيانات الضخمة، مثل تنفيذ عملية تحديد لمكونات المنتجات أو الخدمات، الحاسمة في الحفاظ على الأداء الوظيفي لهذه الأصول، والتي تستلزم بالتالي المزيد من الاهتمام والتدقيق؛
- وضع إجراءات لتقييم أمن سلاسل الإمداد، كتلك المحددة في المعيار [ISO/IEC 27036-3]. ويشمل ذلك تقييم المخاطر المتصلة بالمكونات التي لم تَعُد متاحة، وتنفيذ عمليات استجابة منهجية ومتكررة لمواطن الضعف.

2.1.8 أمن أصول البيانات

1.2.1.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- وضع استراتيجيات لإدارة أمن أصول البيانات، وتوضيح الأهداف والمبادئ المتعلقة بإدارة أمن هذه الأصول؛
- وضع آليات وإجراءات لإدارة أمن أصول البيانات تغطي دورة حياتها؛
- وضع أساليب وإرشادات عمل لتصنيف أصول البيانات وتدريجها وفقاً لقيمتها ودلالتها؛
- إنشاء آليات للموافقة على تغيير الاستراتيجيات والإجراءات والأساليب وإرشادات العمل المتعلقة بتصنيف البيانات وتدريجها؛

- وضع مواصفات أمنية وآليات وإجراءات إدارة للأمن تتعلق بسرية أصول البيانات وسلامتها وتيسرها (مثل استراتيجيات كلمات السر، وإدارة المفاتيح)؛
- إنشاء قائمة لأصول البيانات، وتحديد مسألة المسؤولية عن أمن البيانات والأطراف المعنية بها؛
- الانتظام في عمليات تدقيق وتحديث استراتيجيات إدارة أمن أصول البيانات والإجراءات المتصلة بهذه الاستراتيجيات.

2.2.1.8 المتطلبات التعزيزية

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- وضع مبادئ لإدارة الأمن وسياسات لتكامل البيانات لجميع أنواع موارد البيانات الداخلية والخارجية؛
- وضع ما يلزم من استراتيجيات التوسيم، والتحكم في النفاذ المتعدد المستويات، وتجفير البيانات وفك تجفيرها، ولامركزية البيانات، وغيرها من الاستراتيجيات الأمنية وفقاً لمدى حساسية أصول البيانات.

3.1.8 أمن عمليات سلسلة الإمداد بالبيانات

1.3.1.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- توضيح أهداف إدارة أمن سلسلة الإمداد بالبيانات، ومبادئها، ونطاقها؛
- استحداث سياسات وإجراءات لإدارة أمن سلسلة الإمداد بالبيانات، بما في ذلك معايير لإدارة أمنها تستهدف المشاركين فيها؛
- تحديد أغراض البيانات وأنماط الإمداد في سلسلة الإمداد بالبيانات والمسؤوليات الأمنية للمشاركين فيها، وذلك بموجب اتفاقات تعاون؛
- تسجيل معدات وتطبيقات الحصول على البيانات ونشرها، وتسجيل وتدقيق سلوكيات الحصول عليها ونشرها؛
- تدقيق سلوكيات المشاركين في سلسلة الإمداد بالبيانات فيما يتعلق باستهلاكهم البيانات؛
- إنشاء آلية لتطبيع مصادر البيانات، ومواصفات للسطوح البينية، في سلسلة الإمداد بالبيانات وتسجيل العمليات المهمة وتدقيقها؛
- إنشاء الهيكل التنظيمي لعمل سلسلة الإمداد وإدارتها، ونموذج بيانات أساسي لها، وآلية لمعالجة جودة البيانات، وآلية تتبّع للبيانات؛
- توضيح المسؤوليات الأمنية في سلسلة الإمداد بالبيانات، وضمان أصالة خدمات البيانات المتصلة بها وتيسرها؛
- ضمان تنفيذ تدابير أمنية في عمليات الإمداد بالبيانات، مثل عمليات تبادل البيانات واستخدامها؛
- إنشاء فهارس لسلاسل الإمداد بالبيانات وقواميس لمصادر البيانات، وتحديد الطرف المسؤول عن أمن عمليات الإمداد بالبيانات؛
- ضمان موثوقية السجلات في جميع مراحل سلسلة معالجة المصدر؛
- توضيح الكيانات المسؤولة عن معالجة مصدر البيانات؛
- تنفيذ آليات استيقان لضمان أصالة الكيانات الموجودة في سلسلة معالجة وتبادل بيانات المصدر؛
- ضمان أصالة شفرات مصادر البيانات، والحفاظ على أصالتها بتحديثها؛
- ضمان سرية بيانات المصدر وسلامتها وتيسرها، وتبيّن التوصية [ITU-T X.1601] هذه المتطلبات الأمنية.

2.3.1.8 المتطلبات التعزيزية

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- تحديد متطلبات مختلف المشاركين في سلسلة الإمداد بالبيانات من قدرات خدمات البيانات، وفقاً لدور كل منهم في النظام الإيكولوجي لسلسلة أعمال البيانات؛
- الانتظام في فحص قدرة المشاركين في سلسلة الإمداد بالبيانات على إدارة أمن البيانات؛ وتقييم المخاطر الأمنية التي يتعرضون لها؛
- الانتظام في تقييم المخاطر الأمنية المتصلة بكامل دورة حياة سلسلة الإمداد بالبيانات.

4.1.8 أمن البيانات الشرحية

ينبغي أن تؤخذ في الاعتبار المتطلبات الأمنية لبيانات عميل الخدمة السحابية (CSC)، المتصلة بهذا القسم والموصفة في التوصية [ITU-T X.1641].

1.4.1.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- إنشاء قواميس للبيانات والممارسات الإدارية المتصلة بها وفقاً لمعمارية المؤسسة المعنية وخدمات البيانات فيها، بحيث تشمل مجال البيانات ونمط الحقل وهياكل الجداول، فضلاً عن أسلوب التخزين المنطقي والمادي؛
- إنشاء بيانات شرحية أمنية والممارسات الإدارية المتصلة بها وفقاً لمعمارية أمن البيانات الضخمة، بما في ذلك سياسات كلمات السر وقائمة الإسناد ومواصفات التصاريح؛
- وضع استراتيجية للتحكم في النفاذ إلى البيانات الشرحية، وتحديد أدوار هذه البيانات وآليات التحكم في تصاريح النفاذ إليها؛
- وضع إجراءات لتدقيق عمليات البيانات الشرحية.

2.4.1.8 المتطلبات التعزيزية

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- إنشاء أنظمة لإدارة البيانات الشرحية توحِّد إدارة البيانات الشرحية لخدمات البيانات الضخمة؛
- إنشاء آلية تدريج تلقائي للنعوت الأمنية للبيانات الشرحية وفقاً لتصنيف الأصول واستراتيجية تدريجها؛
- وضع استراتيجية للتوسيم، تشمل ربط البيانات بمالكها، وفقاً للمتطلبات الأمنية للبيانات الشرحية.

2.8 التدابير الأمنية اللازمة لتطبيقات البيانات الضخمة

1.2.8 الحصول على موارد المنصّات

1.1.2.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- ضمان وعي مستعملي خدمات البيانات الضخمة (BDSU) وإبلاغهم بأصول الأنظمة التي سينفُّذ إليها تطبيق ما، كالتوصيل الشبكي، وخدمة تحديد الموقع، وقائمة موارد العتاد مثل الناقل العام بالتسلسل (USB) وتكنولوجيا Bluetooth؛
- ضمان وعي مستعملي خدمات البيانات الضخمة وإبلاغهم بأصول البيانات الحساسة في النظام التي سينفُّذ إليها تطبيق ما، كدفتر العناوين، وسجلات وقائع النظام، وغيرها من مصادر المعلومات الحساسة؛
- ضمان وجاهة سبب الزيارة فيما يتعلق بالتطبيقات التي تطلب النفاذ إلى الموارد، كأن تكون هذه التطبيقات محددة في الوثائق المقدمة من مُطوِّر التطبيقات.

2.1.2.8 المتطلَّب التعزيزي

ينبغي لمقدمي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- ضمان أن يفرض التطبيق المستخدَم قيوداً على الاتصالات الشبكية الداخلية والخارجية غير الضرورية، أو يُقيِّد الاتصالات الشبكية التي يُبادر المستعمِلون إلى إجرائها بما يتفق مع متطلبات العمل.

2.2.8 التحكم في التصاريح وفي النفاذ

1.2.2.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- إنشاء آليات لقياس حجم تفاصيل تصاريح النفاذ المادي والمنطقي إلى تطبيقات البيانات الضخمة ولتحديد مواصفات هذه التصاريح والتحكم فيها، وذلك لضمان أن تكون عمليات النفاذ إلى أصول البيانات والأنظمة المتصلة بخدمات البيانات الضخمة مصرَّحاً بها على النحو السليم؛
- وضع تدابير للتحكم في التصاريح وفي النفاذ استناداً إلى استراتيجيات إدارة الأصول، ووسوم الأصول، والنعوت الأمنية، لضمان قدرة تطبيقات البيانات الضخمة على إدارة التحكم في النفاذ بالتصاريح الدقيقة التفاصيل؛
- استحداث استراتيجية للتحكم في تدفق المعلومات تهدف إلى التحكم في عمليات استيراد البيانات وتصديرها وتقاسمها الجارية في البنية التحتية للبيانات الضخمة فيما بين تطبيقات مختلفة للبيانات الضخمة، أو بين تطبيق البيانات الضخمة ونظام خارجي لتكنولوجيا المعلومات؛
- تنفيذ تصاريح موافَق عليها على النحو السليم لنفاذ الأفراد والمجموعات والأدوار والأجهزة والتطبيقات إلى أصول البيانات والأنظمة المتصلة بخدمات البيانات الضخمة؛
- منح قدرة 'التحديد الذاتي من قبل المستعمِل لاستراتيجية النفاذ بتصريح' بناءً على متطلبات الخدمة، وتدقيق طبيعة السلطة التي يمنحها كل مستعمِل بناءً على متطلبات الخدمة، وذلك لضمان أن يقتصر النفاذ إلى الخدمة على الحد الأدنى من الكيانات المستوفية لمتطلبات سيناريو الخدمة.

2.2.2.8 المتطلَّبان التعزيزيان

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- رصد دورات النفاذ عن بُعد والتحكم فيها، تلقائياً، للكشف عن أي هجمات قد تستهدف الشبكة، وضمان إعمال سياسة النفاذ عن بُعد؛
- توفير محرِّكات تتحكّم في النفاذ القائم على النعوت (ABAC) ووظيفتي إدارة التصاريح والتحكم في النفاذ الموجّهتين نحو كيانات البيانات، فضلاً عن وظائف مثل نقطة إدارة السياسات، ونقطة اتخاذ القرارات السياساتية، ونقطة إنفاذ السياسات، ونقطة النفاذ إلى السياسات.

3.2.8 مراقبة سلوكيات التطبيقات

1.3.2.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- وضع استراتيجيات وإجراءات لمراقبة سلوكيات تطبيقات البيانات الضخمة تغطي كامل دورة حياة البيانات؛
- مساعدة المستعمِلين في استخدام قواعد للمراقبة مكيَّفة بحسب احتياجاتهم الشخصية يمكنها دعم عمليتي رصد أي عمليات شاذة قد تتصل بالبيانات الحرِجة والإبلاغ بها؛
- امتلاك القدرة على تسجيل المعلومات المتعلقة بالسلوكيات الشاذة لأي تطبيقات، وتوسيمها، وتحليلها.

2.3.2.8 المتطلبات التعزيزية

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- إنشاء آليات لإدارة مراقبة سلوكيات التطبيقات تستهدف الهيئات التنظيمية والمستعمِلين من ذوي المتطلبات المحددة، وتوفير واجهة للمراقبة على شبكة الإنترنت بعد منح تصريح النفاذ؛
- إنشاء منصّة لتسجيل وتحليل سلوكيات تطبيقات البيانات الضخمة، ومنح القدرة على التحليل الأمني المحدِّد لسلوكيات المستعمِلين والمستخرِج للمكونات أو السطوح البينية في بروتوكولات الاتصالات المتعلقة بخدمات البيانات الضخمة؛
- توفير أنظمة مواصفات لإجراءات مراقبة السلوكيات ومبادئ توجيهية بشأن عمل هذه الإجراءات.

4.2.8 الاستراتيجيات والإجراءات المتعلقة بأمن التطبيقات

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- وضع سياسة لإدارة إصدار تطبيقات خدمات البيانات الضخمة في شكل إجراء خطي لمَنح التصاريح وتحديد المسؤوليات المُسندة إلى الأدوار المتصلة به – ينبغي أن يُذكر في وثيقة التصريح اسم التطبيق ونسخته ومصدره ومُطوِّره ووظيفته ومكان نشره ونتيجة التقييم الأمني الذي أُجري له والمتطلبات الأمنية المحددة بشأنه؛
- تحديد الحماية اللازمة لإرسال البيانات بين التطبيقات والبنى التحتية للبيانات الضخمة، فضلاً عن منتجات تكنولوجيا المعلومات الأصلية الأخرى، كتطبيق أنظمة أمنية مثل طبقة المقابس المأمونة (SSL) وأمن طبقة النقل (TLS) لتجفير البيانات الحساسة أثناء إرسالها؛
- التحقق من التوقيعات الإلكترونية لرُزَم تثبيت التطبيقات ورُزَم تحديثها؛
- ضمان قدرة التطبيقات على الاستفسار عن النسخة الحالية للبرمجية المشغِّلة، إما على نحو مستقل أو باستخدام الوظائف المتصلة بذلك في البنية التحتية للبيانات الضخمة؛
- ضمان قدرة التطبيقات على التعامل مع عمليات الخطأ التي يمكن التنبؤ بها، دون التأثير على سير العمل الطبيعي للأنظمة الإيكولوجية للبيانات الضخمة؛
- وضع سياسة لإدارة تحديث تطبيقات البيانات الضخمة وتصحيحها، وضمان قدرة التطبيقات على البحث عن التحديثات وتثبيت تصحيحات المكوّنات؛
- اتّباع المواصفات الأمنية لتصميم تطبيقات البيانات الضخمة، وتجنّب المداخل التي قد تنتهك القواعد الأمنية أو تتجاوزها والمداخل غير المحددة؛
- تصميم آليات لمنع استغلال مواطن الضعف في تطبيقات البيانات الضخمة، مثل تجنّب تخصيص مساحات من الذاكرة تخضع لإذنَيْ كتابة وتنفيذ معاً، وعدم القيام بذلك إلا في وظائف التجميع في الوقت المناسب.

5.2.8 تخزين إثباتات الهوية

1.5.2.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- تحديد أسلوب للتخزين الدائم لإثباتات هويات التطبيقات، بما في ذلك استخدام وظيفة المنصّة، عوضاً عن وظيفة التخزين، من أجل تخزين جميع إثباتات الهوية تخزيناً مأموناً، أو استخدام تطبيقات تؤدي هي بنفسها وظيفة التخزين المأمون لإثباتات الهوية؛
- توضيح المعلومات المتصلة بإثبات هوية التطبيق، مثل المفتاح أو البنية التحتية للمفاتيح العمومية (PKI) أو المفتاح الخاص أو كلمة السر؛
- توضيح أساليب حماية الأمن وتدابير التحكم المستخدمة في جمع المعلومات المحدِّدة لهوية الأشخاص (PII) وتخزينها واستخدامها؛

- إنشاء عملية تقييم لأسلوب تخزين إثبات هوية التطبيق لضمان وفائها بمتطلبات الاستراتيجيات والإجراءات الأمنية المتعلقة بأنظمة خدمات البيانات الضخمة.

2.5.2.8 المتطلَّب التعزيزي

ينبغي لمورد خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- التأكد من أن وثائق المواصفات الأمنية تسرد أغراض وأساليب التخزين الدائم لإثباتات الهوية.

6.2.8 الهوية والاستيقان

1.6.2.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- منح القدرة على إدارة هوية المستعمِل، والتحديد التلقائي للمعلومات المتعلقة بهويته في تطبيقات البيانات الضخمة لضمان تحقُّق علاقات التقابل بين تعرّف هوية المستعمِل والمعلومات المتصلة بتصريح النفاذ إلى طبقة التطبيق ذي الصلة؛
- الاستيقان من هوية المستعمِل باستخدام أكثر من تقنية استيقان واحدة فيما يتعلق بتشغيل البيانات أو الوحدات المهمة؛
- عرض ما قد يكون مفيداً من المعلومات المتعلقة باستعمال خدمات أنظمة البيانات الضخمة المتاحة للجمهور، مثل عرض تاريخ آخر تسجيل للدخول وتوقيته أو آخر مكان سُجِّل منه الدخول.

2.6.2.8 المتطلّبان التعزيزيان

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- الاستيقان من هوية المستعمِل باستخدام أكثر من تقنية استيقان واحدة في جميع تطبيقات المستعمِلين الذين يشغلون مواقع رئيسية، على أن تكون تقنية واحدة منها على الأقل قائمة على أسلوب الشهادة البيومترية أو الرقمية؛
- استخدام لغة اتحادية لوسم التأكيدات الأمنية (SAML) من أجل تحديد الهويات والأدوار، وإضافة متطلبات أمنية ومتطلبات تتعلق بالخصوصية، وبالتالي دعم إمكانية نفاذ هويات متعددة إلى خدمات البيانات الضخمة.

7.2.8 أمن التشكيل المحدَّد افتراضياً

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- في حال استخدام إثباتات الهوية المحدَّدة افتراضياً أو إثباتات هوية غير مُشكَّلة، ضمان أن تقتصر قدرة التطبيق المستخدَم على أداء الوظائف الأساسية المتصلة بتشكيل هوية جديدة حصراً؛ فعلى سبيل المثال، إذا كان المستعمِل يستخدم كلمة سر محددة افتراضياً لتسجيل دخوله، فلا يجوز له إلا إدخال واجهة تعديل كلمة السر وينبغي ألا يؤدي التطبيق، في هذه الحالة، أي وظائف أخرى إلى حين تغيّر كلمة السر المحددة افتراضياً؛
- فيما يتعلق بالتطبيقات، توفير وحدات وظيفية أكثر مأمونيةً وتفعيل التشكيلات الأمنية ذات المستوى الأمني المرتفع في أسلوب التثبيت الافتراضي؛ فعلى سبيل المثال، إذا كان التطبيق قادراً على توفير وحدة تسجيل الدخول بكلمة السر ووحدة الشهادة الرقمية في آنٍ واحد، وفي حال أسلوب التثبيت الافتراضي، يختار التطبيق تثبيت وحدة الشهادة الرقمية؛
- تقييد مَنح أذون النفاذ الافتراضي لمستعمِل افتراضي للتطبيق، كمنع مستعمِل حائز على حد أدنى من الأذون غير الأصلية من بدء تشغيل برنامج افتراضياً؛
- ضمان أن تُفعِّل التطبيقات افتراضياً وظيفة تشكيل أمن حساب المستعمِل، بما يشمل طول كلمة السر ومدى تعقيدها وعمر الخدمة الافتراضي واستراتيجية إغلاق الحساب؛
- ضمان بدء تفعيل وظائف تدقيق تسجيل الدخول اللازمة في حال تثبيت التطبيق بالتشكيل المحدَّد افتراضياً، مثل تحديث المكوّنات المثبَّتة أو تعديل المعلمات.

8.2.8 استيراد البيانات وتصديرها

1.8.2.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- صوْغ استراتيجيات ووضع إجراءات لاستيراد البيانات وتصديرها تراعي عوامل من قبيل سعة التخزين، وسرعة نمو حجم البيانات، ومتطلبات العمل، ووسط التخزين، والأداء، بهدف منع فقدان البيانات المهمة والحد من أضرار فقدان البيانات؛
- وضع استراتيجيات وآليات لإدارة تصدير البيانات، وإنشاء آليات لتقييم أمن استيراد البيانات وتصديرها وعملية موافقة على منح التصاريح؛
- وضع مواصفات لمحدِّدات هوية وسط تخزين البيانات المصدَّرة، وينبغي أن تتفق محدِّدات الهوية هذه مع قواعد التسمية الموحَّدة، وتشير إلى رقم الوسط، ووقت التصدير، ومدة الصلاحية، وغيرها من المعلومات المهمة؛
- إتاحة أساليب متنوعة وشاملة لتفاصيل متعددة لاستيراد البيانات وتصديرها، مثل تفاصيل قاعدة البيانات والنموذج المستخدَم والكيان المحدد من قبل المستعمِل؛
- إجراء عملية تحقق من نتائج البيانات المستوردة والمصدَّرة، وضمان سلامة البيانات وصلاحيتها؛
- تسجيل المعلومات المتعلقة بعمليات استيراد البيانات وتصديرها مثل المعلومات المتصلة بالعمليات، ودورة حياة العملية، ورقم الوسط وحجمه، وحالة النقل والتخزين، وتحديث سجلات التغييرات ذات الصلة؛
- اعتماد آليات تجفير وتدابير للتحكم في النفاذ وغيرها من التدابير التقنية الرامية إلى ضمان سرية البيانات المصدَّرة وسلامتها وتوفرها؛
- التحقق بانتظام من سلامة البيانات المصدَّرة وتوفرها.

2.8.2.8 المتطلبات التعزيزية

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- تحديد أساس حساب مَعلمة الفهرس في نظام الإدارة التلقائية للنسخ الاحتياطية للبيانات، بما في ذلك حساب متوسط زمن العطل ومتوسط زمن الاستعادة ومتوسط الزمن بين الأعطال، وتشكيل ما يلزم من برمجيات استيراد البيانات وتصديرها تلقائياً؛
- امتلاك القدرة على استيراد البيانات وتصديرها عن بُعد على شبكة الإنترنت؛ وتخزين البيانات عن بُعد بانتظام وبكيفية شبه تلقائية؛
- دعم إمكانية إعادة تجميع النسخ الاحتياطية للبيانات وضغطها تلقائياً وفقاً لمدى الطلب عليها وغير ذلك من العوامل، وضمان توفر كم هائل من البيانات؛
- امتلاك القدرة على أداء وظيفة التخزين التلقائي بالضغط فيما يتعلق بالنسخ الاحتياطية لبيانات المستعملين، وذلك وفقاً لوتيرة إعداد النسخ الاحتياطية من البيانات واستعادتها.

3.8 التدابير الأمنية اللازمة للسطوح البينية

1.3.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- توفير سطح بيني لكل من مدير النظام ومدير الأمن ومُدقق الحالة الأمنية وغير ذلك من السطوح البينية الخاصة بأدوار المستعمِلين، وتوفير سطوح بينية خاصة بالأدوار التنظيمية؛
- تحديد المتطلبات الأمنية وتدابير المراقبة الأمنية اللازمة لكل من السطوح البينية الخاصة بالأدوار مثل الاستيقان من الهوية، ومنح التصاريح، والتوقيع، وخاتم التوقيت، وبروتوكول الأمن؛
- فرض قيود أمنية على استخدام كل نوع من أنواع السطوح البينية، كالتوصيلات عن بُعد المحدودة الوظائف والأذون؛

- توضيح المواصفات الأمنية للسطح البيني للخدمة، بما في ذلك اسم السطح البيني ومَعلماته ومتطلباته الأمنية، على أن تفرض هذه المواصفات قيوداً على مَعلمات الدخل غير المأمونة وتكون قادرة على التعامل مع الحالات الاستثنائية؛
- منح القدرة على تدقيق سلوكيات النفاذ إلى السطوح البينية، والسطوح البينية القابلة للتشكيل الخاصة بخدمات البيانات؛
- اعتماد آليات أمنية، كتأمين القنوات أو تجفير عملية النقل، لتأمين السطوح البينية الأمنية بين الميادين.

2.3.8 المتطلبات التعزيزية

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- دعم فرض متطلبات تدقيقية في عملية النفاذ إلى السطوح البينية، وتوفير وظائف التدقيق والتنظيم اللازمة للنفاذ إليها؛
- اعتماد أسلوب الإرسال المجفَّر في إرسال بيانات السطوح البينية فيما بين الميادين الأمنية في النظام؛
- إجراء عمليتي مراقبة ومعالجة تلقائيتين للنفاذ إلى السطوح البينية كعمليتين أساسيتين.

4.8 التدابير الأمنية اللازمة للنظام الإيكولوجي للبيانات الضخمة كخدمة

1.4.8 التخطيط الأمني

تنقسم مرحلة التخطيط الأمني إلى ثلاث مراحل فرعية أخرى، هي:

- تحليل المتطلبات – في هذه المرحلة الفرعية، تُحدَّد متطلبات العمل والمتطلبات الأمنية، وتوضَّح، وتُعرَّف؛
- تصميم الحلول – يُصمَّم الحل الأمني (تُصمَّم الحلول الأمنية) في هذه المرحلة الفرعية؛
- تقييم الحلول – هنا يُقيَّم الحل الأمني (تُقيَّم الحلول الأمنية).

وبعد انتهاء المرحلة الفرعية الأخيرة، يمكن لمورد خدمات البيانات الضخمة الانتقال إلى مرحلة بناء الأمن بغرض تنفيذ الحل الأمني، أو العودة إلى المرحلة الفرعية السابقة ألا وهي تصميم الحلول من أجل تعديل الحل المصمَّم أو تحسينه.

1.1.4.8 تحليل المتطلبات

1.1.1.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- تحديد نطاق أنشطة عمل خدمات البيانات الضخمة والمتطلبات المقابلة للبنى التحتية للبيانات الضخمة من الإعدادات الأمنية الأساسية؛
- تعريف التهديدات والمخاطر الأمنية المحددة التي قد تتعرض لها البنية التحتية للبيانات الضخمة وتحديد مواطن الضعف الأمني فيها ثم توضيح التدابير التقنية والإدارية اللازمة لخدمات البيانات الضخمة؛
- تحديد أولويات تنفيذ المتطلبات الأمنية للبنى التحتية للبيانات الضخمة.

2.1.1.4.8 المتطلَّب التعزيزي

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- وضع إجراءات لإدارة تحليل واستعراض المتطلبات الأمنية المتعلقة بالبنى التحتية للبيانات الضخمة، وضمان سلامة ومعقولية هذه المتطلبات.

2.1.4.8 تصميم الحلول

1.2.1.4.8 المتطلَّب العام

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- استحداث مواصفات أمنية تقنية للبنى التحتية للبيانات الضخمة وبيان الوظائف والسطوح البينية والمعلمات الأمنية بوضوح.

2.2.1.4.8 المتطلّبان التعزيزيان

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- إثبات فعالية المواصفات الأمنية التقنية وضمان عدم إمكانية تجاوز الآليات الأمنية في آليات التنفيذ؛
- تحديث الحلول الأمنية في الوقت السليم في حال تغيّر المتطلبات أو تحسّن التكنولوجيا، إلى حين الانتهاء من تقييم هذه الحلول.

3.1.4.8 تقييم الحلول

1.3.1.4.8 المتطلَّب العام

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- استعراض المقترحات الأمنية المتعلقة بالبنى التحتية للبيانات الضخمة بانتظام، بما في ذلك المقترحات المتصلة بالمعمارية الأمنية والإعدادات الأمنية الأساسية، وضمان الوفاء بالمتطلبات الأمنية في الوقت ذاته.

2.3.1.4.8 المتطلَّب التعزيزي

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- إنشاء نظام للتقييم الأمني وتحديد مجموعة من عوامل التقييم الرئيسية.

2.4.8 بناء الأمن

1.2.4.8 المعمارية الأمنية

1.1.2.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- إنشاء المعمارية الأمنية لخدمات البيانات الضخمة، وضمان صلاحية عملية تصميمها وإعمال خدمات أمن البيانات الضخمة على النحو المبين في المعمارية الأمنية؛
- ضمان اتساق المجالات الأمنية المبيَّنة في وثائق المعمارية الأمنية مع متطلبات كل من المعمارية الوظيفية لتطبيقات البيانات الضخمة والمعمارية الوظيفية الأمنية لهذه البيانات؛
- ضمان أن تُبين وثائق المعمارية الأمنية عملية تهيئة الوظائف الأمنية في تطبيقات ومعمارية البيانات الضخمة، ومن ثَم توفير الأمن اللازم لتهيئة المنصة والتطبيقات للتشغيل.

2.1.2.4.8 المتطلَّبان التعزيزيان

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- ضمان أن المعلومات الواردة في الوثائق المبيِّنة للمعمارية الأمنية كافية للشهادة بقدرة الوظيفة الأمنية لخدمات البيانات الضخمة على حماية نفسها من تلاعب أي أطراف غير موثوق بها؛
- ضمان أن الوثائق المبيِّنة للمعمارية الأمنية تقدم تحليلاً كافياً لإثبات عدم إمكانية تجاوز الآليات المصمَّمة للوظيفة الأمنية لخدمات البيانات الضخمة، وأن الوظائف الأمنية المقدمة في نظام البيانات الضخمة قد أُعمِلت إعمالاً صحيحاً.

2.2.4.8 المواصفات الوظيفية

1.2.2.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- تقديم مواصفات وظيفية دقيقة وواضحة، وتوضيح أوجه التقابل بين المواصفات الوظيفية لخدمات البيانات الضخمة ومتطلبات هذه الخدمات من الوظائف الأمنية؛

- ضمان أن المواصفات الوظيفية المقدمة تبيّن الوظائف الأمنية لخدمات البيانات الضخمة بياناً شاملاً، وتوضح العلاقة القائمة مع سلسلة الإمداد بالبيانات، وكذلك مكونات الخدمات؛
- ضمان أن المواصفات الوظيفية المقدمة تبيّن أهداف تصميم جميع السطوح البينية لتطبيقات الوظائف الأمنية لخدمات البيانات الضخمة، وأساليب تنفيذها، وتحدد جميع المعلمات المتصلة بالسطوح البينية للوظائف الأمنية.

3.2.4.8 نشر الأمن

1.3.2.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- إنشاء عملية توفير الأمن اللازمة ليقدِّم المطوِّرون التطبيقات التي صمّموها إلى نظام خدمات البيانات الضخمة؛
- بيان الوظائف والسلطات الخاضعة للمراقبة، المسندة إلى كل من الأدوار المتصلة بخدمات البيانات الضخمة في عملية نشر الأمن؛
- توضيح الوظائف والسطوح البينية المتاحة لكل من الأدوار المتصلة بخدمات البيانات الضخمة، وبيان القيمة الأمنية على النحو المناسب، وخاصة لجميع المعلمات الأمنية التي يتحكّم فيها المستعمِلون؛
- بيان جميع أدوار مستعملي خدمات البيانات الضخمة، وضمان الإعمال الكافي للسياسات الأمنية المبيَّنة في المواصفات والسياسات الأمنية اللازمة لضمان أمن البيئة التشغيلية.

4.2.4.8 حماية الحدود

1.4.2.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- تخطيط ميدان أمني وحدود للدفاع الأمني بما يتسّق مع المستوى الأمني، بما في ذلك سياسات المراقبة الأمنية وسياسات الإدارة؛
- تخطيط ميدان أمني وحدود للدفاع الأمني فيما يتعلق بمراقبة الأعمال وعزل التطبيقات، بما في ذلك سياسات المراقبة الأمنية وسياسات الإدارة؛
- نشر مرافق لحماية الأمن في حدود الميدان الأمني للكشف عن الحوادث الشاذة والانتهاكات المحتملة وما إلى ذلك، والحماية منها؛
- اعتماد آليات دفاع أمني مقارَنة صارمة بين الميادين الأمنية مثل الاستيقان من الهوية، وإدارة التوصيل، والسياسة الأمنية المتعلقة بالتحكم في النفاذ إلى الشبكة، ومنع الاقتحامات، والفحص المتعلق بتسرّب المعلومات وسلامة الحدود؛
- استحداث سياسة لإدارة عمليات تحديث مرافق الدفاع الأمني واعتماد الأساليب اللازمة لضمان تنفيذ هذه السياسة.

2.4.2.4.8 المتطلّبان التعزيزيان

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- وضع تدابير وآليات لحماية الحدود مكيّفة بحسب احتياجات الأشخاص وموجهة إلى حائزين متعددين؛
- تحديد ميدان أمني أو ميادين أمني فرعي وآلية لعزل البيانات فيما بين الميادين الأمنية وآلية للتحكم في النفاذ من أجل المستعمِلين أو صاحبي الأدوار المصرَّح لهم.

5.2.4.8 إدارة الوثائق

1.5.2.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- في نظام خدمات البيانات الضخمة، تنفيذ إدارة الوثائق التي يشمل نطاقها استراتيجيات المنظمة المعنية وقواعدها وسياساتها وبرامج أنظمتها وأدلة التنفيذ الخاصة بها؛

- تحديد عمليات إنشاء الوثائق واستعراضها والموافقة عليها ونشرها وحفظها، وتوضيح المسؤوليات الأمنية المتصلة بكل من عمليات إدارة الوثائق؛
- تحديد وسط تخزين الوثائق ومتطلباتها الزمنية، بما يضمن تيسرها واكتمالها.
- الانتظام في استعراض الوثائق وتحديثها والموافقة عليها ونشرها، بما يضمن اطِّلاع المستعمِلين على معلومات محدَّثة عن آخر النسخ منها؛
- تعيين هيئات لتتولى مسؤولية إنشاء نظام لإدارة الوثائق وصيانته، وإسناد مسؤولية أعمال الصيانة المتصلة بتغير نُسخ الوثائق إليها؛
- إدارة تصنيف وثائق النظام.

2.5.2.4.8 المتطلّبان التعزيزيان

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- توفير منصّة لإدارة الوثائق في إطار عمل مورد الخدمة، تمنح أذوناً لعرض الوثائق تختلف باختلاف الأدوار؛
- ضمان إجراء ما يلزم من تحديث للوثائق ذات الصلة وتحديد لنُسخها عند تحديث المنتجات أو الخدمات.

3.4.8 التشغيل الأمني

1.3.4.8 إدارة تشكيل الأنظمة

1.1.3.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- وضع إجراءات لإدارة تشكيل الأنظمة وتنفيذها، وإنشاء هيكل تنظيمي لإدارته، وتوضيح أدوار مديري التشكيل ومسؤولياتهم كمديري الأنظمة، ومشغِّليها، والموظفين المعنيين بأمنها، ومُدققيها، ومديري قواعد البيانات، وغيرها من الأدوار؛
- تحديد عملية الموافقة على إدارة التشكيل وعمليتي تشغيلها وتدقيقها، وذلك وفقاً لمتطلبات العمل والكيانات المعنية بالإدارة، مثل بنود تشكيل المضيف، وبنود تشكيل الشبكات، ووحدات خدمات التطبيقات وغير ذلك من عمليات تحديد تشكيل الأنظمة، وتشكيل المحتوى، وأنشطة التغيير المتصلة بذلك؛
- وفقاً لنتائج التقييم، إعداد قائمة تشكيل للإعدادات الأساسية للوظائف الأمنية في نظام البيانات الضخمة وقائمة محتوى للتحقق اليومي من التشكيل، يُجرى طبقاً لهما التشكيل اللازم للوظائف الأمنية في نظام البيانات الضخمة وفقاً لمبدأ أقل امتياز؛
- وفقاً لاتفاق مبرم على مستوى خدمات البيانات الضخمة، تشكيل مَعلمات منتج تكنولوجيا المعلومات ذي الصلة في نظام للبيانات الضخمة، وتسجيل المعلومات المتعلقة بالتشكيل الأمني الحالي في هذا النظام والاحتفاظ بهذه المعلومات؛
- وفقاً لاستراتيجيات الاستخدام، تقييد استراتيجيات شراء البرمجيات وسياسات منح تصاريحه، وحظر أو تقييد استخدام البرمجيات لوظائف أو منافذ أو بروتوكولات أو خدمات معينة في نظام للبيانات الضخمة؛
- توضيح قوائم التشكيل المتحكَّم فيه التي يلزم تغييرها بانتظام، والانتظام في تحديث بنود التشكيل المهمة المتصلة بأمن المعلومات في نظام للبيانات الضخمة، مثل قاعدة بيانات مكافحة الفيروسات، وقاعدة البيانات المتعلقة بقواعد الكشف عن الاقتحامات، وقاعدة البيانات المتعلقة بقواعد استخدام جدران الحماية، وقاعدة البيانات المتعلقة بمواطن الضعف؛
- استعراض التغييرات المقترح إجراؤها في التشكيلات التي يتحكّم فيها نظام البيانات الضخمة، والموافقة عليها أو رفضها وفقاً لنتائج تحليل آثارها الأمنية، وتسجيل قرارات التغيير؛
- تقييد صلاحيات مطوِّري الأنظمة ومُجمِّعيها فيما يتعلق بإحداث تغييرات مباشرةً في نظام للبيانات الضخمة وما يتصل به من عتاد وبرمجيات وبرمجيات ثابتة في بيئة الإنتاج، وتدقيق التشكيلات، وتغيير الأحداث؛
- قبل تنفيذ التشكيل أو التغيير، اختبار بنود التشكيل المتحكَّم فيه وبنود التغيير، والتحقق من صلاحيتها، وتسجيلها، وتحليل بنود تغيير النظام لتقدير آثارها المحتملة على أمن خدمات البيانات الضخمة؛

- رصد التغيرات الطارئة على مَعلمات إعدادات التشكيل، وتفعيل وظائف المراقبة والإنذار والدفاع وغيرها من وظائف التجهيزات الأمنية بقدر معقول؛
- وضع تدابير للاستجابة فيما يتصل بالتعامل مع التغييرات غير المصرَّح بها، تشمل الموظفين المعنيين بإحداث التغييرات، واستعادة تشكيل محدد من قبل أو وقف تشغيل نظام المعلومات المتأثر في الحالات القصوى.

2.1.3.4.8 المتطلبات التعزيزية

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- تقييم المخاطر المتصلة بآثار إدارة التشكيل تقييماً منتظماً أو كلما طرأت تغيّرات كبيرة على معمارية العمل أو معمارية النظام، ومراجعة متطلبات تشكيل الإعدادات الأساسية ومحتويات التشكيل وفقاً لنتائج هذا التقييم، كتقييم المخاطر ومراجعة متطلبات التشكيل مرة واحدة في السنة على الأقل؛
- تقييم استراتيجية تقييم المخاطر وآثار تنفيذ هذه الاستراتيجية تقييماً منتظماً أو كلما طرأت تغيرات كبيرة على معمارية العمل أو معمارية النظام – ووفقاً لنتائج هذا التقييم، مراجعة إجراءات إدارة تشكيل النظام، وتعديل هيكل إدارة المنظمة، وتشكيل عملية الإدارة، واتخاذ غير ذلك من الإجراءات ؛
- استعراض تشكيلات أنظمة البيانات الضخمة بانتظام لتحديد الوظائف أو المنافذ أو البروتوكولات أو بنود تشكيل الخدمات، غير الضرورية أو غير المأمونة؛
- استخدام أدوات، أو آليات أوتوماتية، لتشكيل الأنظمة تهدف إلى إدارة مَعلمات بنود التشكيل وتطبيقها والتحقق منها، على نحو مركزي؛
- امتلاك القدرة على ملاحظة التغيرات الطارئة على البنى التحتية للبيانات الضخمة وحالة الموارد الافتراضية، في زمن حدوثها الفعلي، والقدرة على تعديل تشكيل استراتيجيات أمن خدمات الأنظمة تلقائياً.

2.3.4.8 استعمال خدمات الأطراف الثالثة

1.2.3.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- وضع سياسة لإدارة الأمن تتعلق بالشركاء في خدمات الأطراف الثالثة؛
- إنشاء آليات لقبول موردي خدمات الأطراف الثالثة وتقييمهم ومنحهم درجات تقييمية؛
- إبرام اتفاقات تعاون مع موردي خدمات الأطراف الثالثة بشأن مكونات الأنظمة، وتوضيح التزاماتهم ومسؤولياتهم كتجنّب الإفراط في إشراكهم في التشغيل الأمني لنظام البيانات الضخمة، مثلاً؛
- ضمان أن تفهم مكونات خدمات الأطراف الثالثة تدابير أمن المعلومات في نظام البيانات الضخمة، وتُنفذ التدابير الأمنية اللازمة تنفيذاً صحيحاً، وتجتاز الاختبارات التي تُجريها هيئات تقييم كأطراف ثالثة؛
- الاشتراك مع مقدمي خدمات الأطراف الثالثة في وضع سياسات بشأن أمن استخدام مكونات هذه الخدمات، وتوضيح شروط استخدامها، ونطاق نفاذ المكونات الخارجية إلى الأنظمة؛
- اعتماد ما يلزم من تدابير تقنية أو تدابير لإدارة الأمن تضمن التصريح لمستعملي البيانات الضخمة بالنفاذ إلى موارد الأنظمة والبيانات عبر مكونات الخدمات الخارجية وتمكينهم من ذلك؛
- تدقيق المعلومات، كتلك المتعلقة بالمستعمِلين والعمليات المخطَّطة والحالية لمكونات الخدمات الخارجية، وضمان إمكانية تتبّع خدمات البيانات الضخمة.

2.2.3.4.8 المتطلبات التعزيزية

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- تقييم مؤهلات موردي خدمات الأطراف الثالثة وقدراتهم الأمنية، والاشتراك مع موردي مكونات الخدمات الخارجية في إنشاء آلية تعاونية للاستجابة في حالات الطوارئ؛
- ضمان أن تدرك مكونات الخدمات الخارجية التدابير الأمنية التي تقتضيها استراتيجيات وخطط أمن المعلومات في نظام البيانات الضخمة، وتجتاز الاختبارات التي تُجريها هيئات تقييم كأطراف ثالثة؛
- تقييد استخدام الموظفين المصرَّح لهم موارد البيانات الحساسة في مكونات الخدمات الخارجية، ومنها وسط التخزين وملفات البيانات وغيرها من موارد البيانات التي يتحكّم فيها موردو خدمات البيانات الضخمة هؤلاء.

3.3.4.8 أمن سلسلة إمداد تكنولوجيا المعلومات

1.3.3.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- وضع سياسات وتدابير بشأن أمن سلسلة إمداد تكنولوجيا المعلومات، وتوضيح آليات ومؤشرات الترشيح وأساليب التقييم؛
- توضيح ما يضطلع به المشاركون في سلسلة إمداد تكنولوجيا المعلومات من أدوار وعمليات تتعلق بالحصول على البيانات وخدمات الأنظمة ذات الصلة؛
- اعتماد التدابير التقنية والإدارية اللازمة لإحلال سلسلة الإمداد، وضمان فعالية الاستجابة في حال وقوع حوادث تتعلق بها.

2.3.3.4.8 المتطلبات التعزيزية

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- إنشاء نموذج لسلسلة المعلومات يتعلق بتجميع البيانات، بما في ذلك استخراجها ودمجها والاستخدام الأمثل لمصادر بيانات سلسلة الإمداد؛
- إنشاء آلية لفحص وتقييم سلسلة الإمداد، وإجراء تقييمات للمخاطر وتقييمات أمنية بانتظام، مرة واحدة في السنة على الأقل مثلاً؛
- إنشاء آلية تغذية مرتدة لإدارة وتقييم جودة سلسلة الإمداد.

4.3.4.8 إدارة تصحيح الأنظمة

1.4.3.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- وضع إجراءات لإدارة التصحيح تشمل عمليات التنزيل والاختبار والتحليل والتوزيع والتثبيت والحفظ وغير ذلك من العمليات والمحتويات، وضمان الإدارة المعيارية لتصحيح الأنظمة؛
- إنشاء فريق لإدارة التصحيح؛ ومتابعة المعلومات المتعلقة بالكشف عن مواطن الضعف، وعمليات الاستجابة للأحداث الأمنية؛ وتنفيذ أعمال التنزيل والاختبار والتثبيت وغيرها من المهام التصحيحية وفقاً لجداول زمنية مناسبة؛
- إنشاء إطار لتوزيع التصحيحات في الأنظمة وإدارتها، وتوضيح آليات تنزيل وتحديث التصحيحات، مثل إدارة التصحيح المفعَّلة بوقوع حوادث أمنية في النظام، أو إدارة التصحيح المفعَّلة دورياً وفقاً لفترات زمنية محددة؛
- امتلاك القدرة على اختبار مدى توافق التصحيحات مع الأنظمة ذات الصلة قبل نشر هذه التصحيحات وتثبيتها؛ وتسجيل ما قد ينشأ من مشاكل أثناء عمليات تحديث التصحيحات؛
- وجود وظيفة فحص للتصحيحات؛ والتحقق من نجاح تثبيتها.

2.4.3.4.8 المتطلَّب التعزيزي

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- إنشاء نظام لإدارة التصحيح، وتحديثه، وتثبيت التصحيحات باستخدام البرمجيات.

5.3.4.8 خطة استمرارية الأعمال

1.5.3.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- الانتظام في تقييم المخاطر الناجمة عن الأعمال الجارية؛ وإعلام المستعمِلين بتلك المخاطر؛
- صوْغ وتنفيذ خطة مناسبة بشأن الدعم في حالات الكوارث، وفقاً لغايات العمل الاستراتيجية، توضِّح مستوى قدرات التعافي من الكوارث ومتطلباته واستراتيجياته في الأنظمة ذات الصلة؛
- تحليل آثار الأعمال وتقييم المخاطر بانتظام، وعقد دورات تدريبية تتعلق باستمرارية الأعمال.

2.5.3.4.8 المتطلّبان التعزيزيان

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- الانتظام في إجراء تجارب لتبديل الأنظمة في البنية التحتية المتصلة بخدمات البيانات الضخمة المشغَّلة؛ والاستخدام الأمثل لأنظمة دعم موارد البيانات والأنظمة وفقاً للمتطلبات الحالية؛
- تنظيم تدريبات بشأن خطط استمرارية الأعمال لفحص مدى سلامة هذه الخطط وإمكانية تشغيلها وفعاليتها، والتحقق من استمرارية الأعمال وتوفر أصول الأنظمة ذات الصلة.

4.4.8 التدقيق الأمني

ينبغي لموردي خدمات البيانات الضخمة (BDSP) إجراء عمليات تدقيق أمني بانتظام في كامل أجزاء النظام الإيكولوجي للبيانات الضخمة كخدمة. ويمكن أن يتولى إجراء عمليات التدقيق فريق تدقيق داخلي مستقل أو مدقّقون كأطراف ثالثة (هم الشركاء في خدمات البيانات الضخمة (BDSN)). وينبغي أن يتمكن مستعملو خدمات البيانات الضخمة (BDSU) من الاطلاع على نتائج التدقيق على النحو المناسب.

1.4.4.8 إدارة استراتيجيات التدقيق

1.1.4.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- صوْغ استراتيجيات ووضع إجراءات للتدقيق تشمل سلوكيات أنظمة البيانات الضخمة وأنشطة البيانات في خدمات البيانات الضخمة، بما في ذلك أهداف التدقيق والكيانات الخاضعة له وعملياته وأسلوبه ووتيرته، والأدوار والمسؤوليات، والالتزامات الإدارية، المتصلة به، وعمليات التنسيق المشارِكة في سلسلة الإمداد، وتحليل مدى الامتثال.
- إنشاء عمليات لإدارة التغيير تتعلق باستراتيجيات التدقيق وإجراءاته، وتسجيل حالة هذه الاستراتيجيات والإجراءات والسياسات المتعلقة بأداء التغيير ووصفه وما إلى ذلك، منذ بدء تنفيذها حتى انتهائه، بالتفصيل، واستعراض وتحديث استراتيجيات التدقيق وإجراءاته بانتظام؛
- توضيح امتيازات المستعمِلين ومسؤولياتهم في استراتيجيات التدقيق وإجراءاته، وتحديد إجراء منح الامتيازات المتصل بهذه الاستراتيجيات والإجراءات، وأداء استراتيجيات التدقيق، والأدوار المتصلة بإدارة بيانات التدقيق.

2.1.4.4.8 المتطلبات التعزيزية

ينبغي لموردي خدمات البيانات الضخمة (BDSP) الاضطلاع بما يلي:

- وضع إجراءات تدقيق وآليات تنسيق بشأن أمن سلسلة الإمداد بالبيانات، وضمان إمكانية تتبّع أحداث التدقيق؛
- الانتظام في التحقق من تنفيذ استراتيجيات التدقيق وإجراءاته وتقييمه؛
- تعيين مدققين مستقلين لأمن الأنظمة ينبغي لهم إجراء عمليات تدقيق أمني لخدمات البيانات الضخمة بانتظام؛
- امتلاك تكنولوجيات وأدوات تحليل مدى الامتثال اللازمة لتنفيذ استراتيجيات التدقيق وإجراءاته، بالاستناد إلى بيانات التدقيق.

2.4.4.8 توليد بيانات التدقيق

1.2.4.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- صوْغ لوائح بشأن تسجيل بيانات التدقيق، وتوضيح الهيكل والنسق التنظيميين لبيانات التدقيق؛
- توضيح الأحداث القابلة للتدقيق المتصلة بأعمال أنظمة البيانات الضخمة، مثل تسجيل دخول المستعمِلين، وإدارة الحسابات، ونفاذ الضيوف، وتغيير الاستراتيجيات، ومنح التصاريح للوظائف المتمتِّعة بامتيازات، وتحديث الوحدات النمطية للخدمات؛
- توضيح الأحداث القابلة للتدقيق المتصلة بأنشطة البيانات في خدمات البيانات الضخمة، مثل جمع البيانات، والنفاذ إليها، وتخزينها، ونقلها، ومعالجتها، والاحتفاظ بها، وتدميرها؛
- ضمان أن تشمل سجلات بيانات التدقيق على الأقل توقيتات العمليات والكيانات القائمة بها وأنماط العمليات والكيانات المستهدفة بها ونتائجها؛
- امتلاك القدرة على تدقيق التفاصيل العديدة في عمليات البيانات وأعمال خدمات الأنظمة؛
- الاحتفاظ بعلامات زمنية في سجلات التدقيق يمكن التعويل عليها. وينبغي أن تفي التفاصيل الزمنية بمتطلبات التدقيق؛
- امتلاك القدرة على انتقاء الأحداث القابلة للتدقيق وفحصها؛
- التحديث بانتظام لسياسات تسجيل البيانات والأحداث القابلة للتدقيق وسجلات التدقيق.

2.2.4.4.8 المتطلبان التعزيزيان

ينبغي لموردي خدمات البيانات الضخمة الاضطلاع (BDSP) بما يلي:

- توفير سطوح بينية في الأنظمة ذات الصلة لنفاذ بيانات التدقيق الذي يُجريه طرف ثالث؛
- اعتماد تكنولوجيات تجفير لضمان عدم إبطال بيانات التدقيق.

3.4.4.8 حماية بيانات التدقيق

1.3.4.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:

- إتاحة أساليب وآليات لإدارة التخزين الدائم والمأمون لبيانات التدقيق الهائلة الحجم؛
- امتلاك القدرة على منح تصاريح النفاذ إلى بيانات التدقيق؛ والتصريح للهيئات المعنية بالنفاذ إلى بيانات التدقيق بالنفاذ إلى مديري التدقيق المحددين؛
- اعتماد تكنولوجيات أمنية أو تدابير للمراقبة الأمنية تضمن أصالة بيانات التدقيق؛
- إتاحة وظيفة حفظ بيانات التدقيق، ودعم أساليب وآليات التخزين المجفَّر خارج شبكة الإنترنت لبيانات التدقيق؛
- إتاحة استراتيجيات وأساليب لإدارة تخزين بيانات التدقيق بفعالية، وضغط البيانات، وما إلى ذلك؛

- تحسين إدارة النفاذ إلى بيانات التدقيق، وتسجيل جميع عمليات هذه البيانات؛
- امتلاك القدرة على إزالة مركزية بيانات التدقيق المصدَّرة؛
- ضمان فعالية سجلات التدقيق المخزَّنة في حال نضوب سعة تخزين بيانات التدقيق أو تعطلها أو تعرّضها لهجوم.

2.3.4.4.8 المتطلبان التعزيزيان

ينبغي لموردي خدمات البيانات الضخمة الاضطلاع (BDSP) بما يلي:
- امتلاك القدرة على التعافي من الكوارث عن بُعد والدعم في حالات الكوارث عن بُعد؛
- التمكّن من تقديم أدلة لإثبات أصالة بيانات التدقيق المقدمة واكتمالها.

4.4.4.8 التقارير التحليلية لعمليات التدقيق

1.4.4.4.8 المتطلبات العامة

يضطلع موردو خدمات البيانات الضخمة (BDSP) بما يلي:
- صوْغ استراتيجيات ووضع إجراءات لتدقيق سجلات التدقيق وتحليلها وتقديم تقارير عنها؛
- فحص سجلات التدقيق وتحليلها بانتظام، وإعداد تقارير تحليلية لعمليات التدقيق؛
- توزيع تقرير تحليلي على الموظفين المسؤولين المحددين في المنظمة المعنية، في حال اكتشاف أي تهديدات أمنية كبرى أو سلوكيات غير قانونية جسيمة أثناء عمليات التدقيق، وإبلاغ مديري المنظمة بها في أسرع وقت ممكن.

2.4.4.4.8 المتطلبان التعزيزيان

ينبغي لموردي خدمات البيانات الضخمة الاضطلاع (BDSP) بما يلي:
- رصد الأحداث القابلة للتدقيق وتحليلها في زمن وقوعها الفعلي، بهدف دعم رصد الأفعال المشبوهة والتصدي لها؛
- امتلاك القدرة على تحليل علاقات الترابط بين سجلات التدقيق المختلفة المصادر.

بيبليوغرافيا

[b-ITU-T M.3030] Recommendation ITU-T M.3030 (2002), *Telecommunications markup language (tML) framework*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3602] Recommendation ITU-T Y.3602 (2018), *Big data – Functional requirements for data provenance*.

[b-NIST SP 800-30] Special Publication NIST SP 800-30 (2012), *Guide for conducting risk assessments*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2021