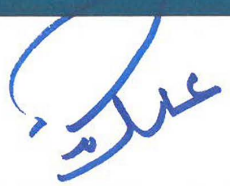
البنك المركزي الأردني
CENTRAL BANK OF JORDAN

الإطار التنظيمي لاستخدامات الذكاء الاصطناعي للقطاع المصرفي الأردني

النسخة ١,٠ - تموز ٢٠٢٥

الاعتماد	التاريخ	النسخة
	تموز , ٢٠٢٥	النسخة ١,٠

الفهرس

الملخص التنفيذي ٥

المقدمة..... ٦

النطاق ٦

قائمة المصطلحات..... ٧

المسؤوليات ٩

الجمهور المستهدف..... ٩

الأهداف ٩

١. الحوكمة والإشراف..... ١٠

١,١ هيكل حوكمة الذكاء الاصطناعي ١٠

١,٢ تحديد مسؤوليات أعضاء اللجنة ١٠

١,٣ النهج القائم على المخاطر..... ١١

٢. الأخلاقيات والشفافية ١٢

٢,١ الأخلاقيات..... ١٢

٢,٢ قابلية التفسير والإفصاح ١٢

٢,٣ استقلالية العميل وحقوق الانسحاب ١٣

٢,٤ المساءلة..... ١٣

٢,٥ الدقة والتحيز ١٣

٢,٦ تقييمات الأثر الدورية..... ١٣

٣. الامتثال التنظيمي ١٤

٣,١ المواءمة مع الأنظمة والتشريعات المحلية والدولية ١٤

التشريعات المحلية ١٤

الامتثال الدولي وحوكمة الذكاء الاصطناعي عبر الحدود ١٤

٣,٢ الالتزام بالمعايير الدولية ١٤

٤. إدارة البيانات ١٥

٤,١ خصوصية وأمن البيانات..... ١٥

إخفاء الهوية والتشفير..... ١٥

تقليل البيانات والاحتفاظ بها..... ١٥

٤,٢ جودة البيانات وسلامتها..... ١٦

إطار حوكمة البيانات ١٦

التوثيق وإمكانية التتبع ١٦

٥. التطوير والنشر الآمن ١٧

٥,١ أمن نظام الذكاء الاصطناعي ١٧

نهج دورة الحياة الآمنة ١٧

٥,٢ التحقق من النماذج واختبارها ١٧

اختبار الدقة والتحيز والمتانة ١٧

آليات الفشل الآمن (Fail-Safe Mechanisms) ١٨

المعايرة (Calibration) ١٨

٥,٣ المراقبة المستمرة والتدقيق ١٩

المراقبة المستمرة للأداء ١٩

٥,٤ الإشراف البشري على أنظمة الذكاء الاصطناعي ١٩

٦. الاستجابة للحوادث، واستمرارية الأعمال، والتعافي من الكوارث ٢٠

٦,١ خطة إدارة الحوادث ٢٠

بروتوكولات الحوادث الخاصة بالذكاء الاصطناعي ٢٠

مشاركة المعلومات والتقارير التنظيمية ٢٠

٦,٢ تخطيط استمرارية الأعمال ٢٠

دمج استمرارية الأعمال مع عمليات الذكاء الاصطناعي ٢٠

التمارين الدورية واختبارات الإجهاد ٢٠

٧. إدارة مخاطر الأطراف الخارجية ٢١

٧,١ تقييم مخاطر المزودين ٢١

العناية الواجبة (Due Diligence) ٢١

توزيع الاعتمادية على المزوّدين والشفافية ٢١

الالتزامات التعاقدية ٢٢

٨. التعاون والتوعية والتدريب ٢٣

٨,١ إشراك أصحاب المصلحة ٢٣

التعاون الدولي ٢٣

التعليم وبناء القدرات ٢٣

شهادات اعتماد لمتخصصي الذكاء الاصطناعي ٢٣

حملات التوعية ٢٣

٩. المراجعة والتحسين المستمر ٢٤

التواصل والتقارير ٢٤

معلومات التواصل ٢٤

الملخص التنفيذي

يشهد قطاع الخدمات المالية تحولاً متسارعاً نحو دمج تقنيات الذكاء الاصطناعي(AI) ، وهو ما يستدعي وجود إطار عمل منظم ومرن يضمن التبنّي المسؤول لهذه التقنيات، ويحد من المخاطر المحتملة، ويُحقق قيمة مستدامة على المدى الطويل. ومن هذا المنطلق، يهدف إطار الذكاء الاصطناعي في القطاع المصرفي الأردني، إلى توجيه المؤسسات نحو حوكمة وتوظيف وتوسيع قدراتها في الذكاء الاصطناعي بطريقة آمنة ومرنة.

يتناول الإطار التوجيهات الاستراتيجية والتشغيلية عبر محاور رئيسية تشمل: الحوكمة، الأخلاقيات، الامتثال، إدارة البيانات، الأمن، الاستجابة للحوادث، ومخاطر الأطراف الثالثة. كما يركز على ضرورة إنشاء هيكل حوكمة واضح لحوكمة الذكاء الاصطناعي، وتحديد المسؤوليات، وتبني نهج قائم على المخاطر لضمان الرقابة والإشراف في جميع مراحل التنفيذ.

ويُعد إدماج المبادئ الأخلاقية - مثل العدالة، وقابلية التفسير، وحق اتخاذ القرار، والتخفيف من التحيّز – في تصميم وتشغيل أنظمة الذكاء الاصطناعي محوراً أساسياً في هذا الإطار. كما يتضمن أحكاماً لضمان الشفافية، والدقة، وحق العملاء في الاعتراض على القرارات المؤتمتة عندما يكون ذلك مناسباً.

ومن جهة اخرى، يؤكد الإطار ضرورة التوافق مع التشريعات المحلية ذات الصلة، إلى جانب التأكد من امتثال أنظمة الذكاء الاصطناعي للمعايير المعترف بها في مجالات خصوصية البيانات، وجودتها، وأمن التشغيل. كما ينص على تبنّي ممارسات تطوير آمنة من خلال آليات دقيقة للتحقق والاختبار والمراقبة المستمرة لضمان الموثوقية.

علاوة على ذلك، يتناول الإطار ضرورة توافر قدرات متخصصة للاستجابة للحوادث، وإدماج الذكاء الاصطناعي ضمن خطط استمرارية الأعمال، ووضع بروتوكولات لإدارة مخاطر الأطراف الثالثة بما يحكم علاقات ومخاطر الموردين. ويؤكد أيضاً على أهمية إشراك أصحاب المصلحة، وبناء القدرات، والشهادات المهنية، ونشر الوعي على جميع مستويات المنظومة المصرفية.

وأخيراً، يدعو الإطار المؤسسات المصرفية الى تبني منهجية قائمة على ترسيخ ثقافة التحسين المستدام، والشفافية، وتشجيع الابتكار بما يواكب تطورات الذكاء الاصطناعي في القطاع.

يُعد هذا الإطار بمثابة خارطة طريق أساسية لدعم التحول الاستراتيجي للقطاع المصرفي من خلال الذكاء الاصطناعي، بما يضمن اتساق تطبيقه مع المصالح الوطنية، والمرونة التشغيلية، وثقة الجمهور.

المقدمة

في ظل تطور المشـــهد الرقمي المتســـارع، يواجه القطاع المالي الأردني تحديًا مزدوجًا يتمثل في تبنّي أحدث الابتكارات التقنية لتحسـين جودة الخدمات، وفي الوقت ذاته التعامل مع المخاطر الناشـئة والمعقدة. وفي هذا السـياق المتغير والمتسـارع، يبرز الذكاء الاصـــطناعي (AI) كقوة محركة للتحول، حيث يقدم حلولًا مبتكرة تســـهم في تحســـين تجربة العملاء، وتعزيز إدارة المخاطر، ودفع عجلة النمو المؤسسي، واحداث ثورة في العمليات التشغيلية.

ومع ذلك، فإن دمج الذكاء الاصطناعي في الخدمات المالية لا يخلو من التحديات. إذ تشكل احتمالية التحيّز في الخوارزميات، وقابلية الأنظمة للهجمات العدائية، وغموض آليات عمل الذكاء الاصـطناعي، عوائق حقيقية أمام التوظيف الآمن والفعال لهذه التقنيات. وإدراكًا لهذه المخاطر، يلتزم البنك المركزي الأردني (CBJ) بدعم التبني المسؤول للذكاء الاصطناعي، بما يضمن سير الابتكارات التكنولوجية الابتكار جنبًا إلى جنب مع الحوكمة الفعالة، وإدارة المخاطر، والامتثال التنظيمي.

إن وجود إطار حوكمة منظم للذكاء الاصـــطناعي يســـهم في ضـــمان الامتثال للمتطلبات التنظيمية الوطنية والدولية، وفي الوقت ذاته يعزز مواءمة مبادرات الذكاء الاصـطناعي مع الأهداف الاسـتراتيجية على مسـتوى المؤسـسـات والقطاع ككل. ويمكن لحوكمة الذكاء الاصـطناعي أن تُبنى على الأطر والسـياسـات وآليات الرقابة القائمة، بدلًا من تطويرها، بما يسـهم في خلق نهج تنظيمي مرن وقابل للتكيف، يدعم الابتكار ويحافظ على الاستقرار المالي.

وانطلاقًا من هذا الأســـاس، يواصـــل البنك المركزي الأردني التزامه بتمكين الابتكار في التكنولوجيا المالية، مع الحرص على الحفاظ على بيئة مالية آمنة مسـتقرة وشـفافة. ومن خلال تبني هذا الإطار، يمكن للمؤسـسـات المصرفية توظيف قدرات الذكاء الاصطناعي التحويلية بشكل مسؤول وفعال، مع ضمان الانسجام الكامل مع الأهداف التنظيمية الوطنية وأفضل الممارسات العالمية.

النطاق

ينطبق هذا الإطار التنظيمي على اسـتخدام تقنيات الذكاء الاصـطناعي من قبل المؤسـسـات المصرفية الخاضـعة لإشراف ورقابة البنك المركزي الأردني (CBJ) . ويشـــمل هذا الإطار مختلف الســـيناريوهات التي تقوم فيها الجهة بتطوير وتطبيق أنظمة الذكاء الاصطناعي داخليًا، أو الحصول عليها من مزوّدين خارجيين، أو التعاقد مع أطراف خارجية لتنفيذ عمليات أو مهام تعتمد بشكل مباشر على الذكاء الاصطناعي.

قائمة المصطلحات

المصطلح	التعريف
المساءلة (Accountability)	تشير المساءلة وفقاً لتعريف منظمة التعاون الاقتصادي والتنمية (OECD)، إلى الالتزام المتوقع من الأفراد أو المؤسسات بضمان التشغيل السليم لأنظمة الذكاء الاصطناعي التي يصممونها أو يطورونها أو يديرونها أو ينشرونها، وذلك طيلة دورة حياة النظام، ووفقًا لأدوارهم والأطر التنظيمية المعمول بها، وذلك بإثبات هذا الالتزام من خلال الممارسات الفعلية والقرارات المدروسة (مثل توثيق القرارات الرئيسية خلال دورة حياة النظام أو إجراء أو إتاحة التدقيق عند الاقتضاء).
نظام الذكاء الاصطناعي (AI System)	وفقًا لتعريف OECD، هو نظام قائم على الآلة، يهدف بشكل صريح أو ضمني إلى استنتاج مخرجات – مثل التنبؤات أو المحتوى أو التوصيات أو القرارات – انطلاقًا من المدخلات التي يستلمها، بحيث تؤثر هذه المخرجات على البيئات المادية أو الرقمية. وتختلف أنظمة الذكاء الاصطناعي في درجة استقلاليتها وقدرتها على التكيّف بعد تشغيلها.
التحيّز (Bias)	يُشير إلى أداء غير متكافئ للنموذج بشكل منهجي، سواء كان أعلى أو أدنى، مما يؤثر سلبًا على فرد أو فئة معينة من المستخدمين. وقد تنشأ هذه الانحيازات من البيانات التدريبية، أو اختيارات التصميم، أو نتائج غير مقصودة تظهر أثناء تشغيل النظام.
الجهة (Entity)	يُقصد بها المؤسسات المصرفية الخاضعة لإشراف ورقابة البنك المركزي الأردني (CBJ).
قابلية التفسير (Explainability)	حسب تعريف OECD، تعني تمكين الأشخاص المتأثرين بمخرجات نظام الذكاء الاصطناعي من فهم الآلية التي تم استخدامها للوصول إلى هذه المخرجات.
العدالة (Fairness)	بحسب تعريف OECD، تشير العدالة إلى الالتزام بحماية حقوق الإنسان، وضمان منع التمييز، وتحقيق المساواة عبر دورة حياة النظام. ويتطلب ذلك تصميم ونشر الأنظمة بطريقة تحترم كرامة الأفراد، والخصوصية، والتنوّع، وتمنع التحيّز والإقصاء والنتائج غير العادلة. كما تشمل العدالة توفير آليات رقابة بشرية وضمانات للحد من سوء

	الاستخدام وضمان الامتثال الأخلاقي والقانوني بما يتماشى مع القيم الديمقراطية وسيادة القانون.
الذكاء الاصطناعي التوليدي (Generative AI - GenAI)	وفق تعريف OECD، هو نوع من الذكاء الاصطناعي قادر على إنشاء محتوى جديد في أشكال متعددة مثل النصوص، والصور، والفيديوهات، والموسيقى.
الهَلوسة (Hallucination)	الحالات التي تنتج فيها نماذج الذكاء الاصطناعي التوليدي مخرجات تبدو صحيحة من حيث الشكل، لكنها غير دقيقة من الناحية الواقعية أو تحتوي على معلومات خاطئة تبدو حقيقية.
تقييم الأثر (Assessment Impact)	عملية تقييم تهدف إلى تحديد وفهم وتوثيق وتخفيف الأثر الأخلاقي والقانوني والاقتصادي والمجتمعي المحتمل لنظام الذكاء الاصطناعي في سياق استخدام معين.
النماذج (Models)	تُشير إلى الخوارزميات المحددة التي تُستخدم لاتخاذ قرارات قائمة على الذكاء الاصطناعي.
الشفافية (Transparency)	حسب تعريف OECD، تعني الشفافية في الذكاء الاصطناعي إعلام الأفراد بوضوح عند تفاعلهم مع نظام ذكاء اصطناعي، وتوفير تفسيرات مفهومة حول كيفية تطوير هذا النظام، وطريقة عمله واتخاذه للقرارات، مع مراعاة الحدود التقنية ومتطلبات حماية الملكية الفكرية.
المستخدم (User)	شخص طبيعي، سواء كان مستهلكًا أو موظفًا، أو شخصًا اعتباريًا.

المسؤوليات

هذا الإطار صادر ومملوك من قبل البنك المركزي الأردني (CBJ). ويتولى البنك المركزي مسؤولية تقييم مدى فاعلية تنفيذ هذا الإطار لدى الجهات المعنية، وضمان الالتزام بتطبيقه بشكل فعّال. في المقابل، تقع على عاتق الجهات الخاضعة لإشراف ورقابة البنك مسؤولية تبنّي الإطار، ودمجه ضمن عملياتها التشغيلية، والحفاظ على استمرارية تطبيقه.

كما يتولى البنك المركزي الأردني أيضاً مسؤولية الإشراف على مواءمة الإطار بشكل مستمر مع الاتجاهات والمعايير العالمية الناشئة، من خلال تعزيز قنوات التواصل مع أصحاب المصلحة لمراجعة وتحديث الإطار بما يعكس التطورات المستجدة في البيئة التنظيمية.

وفي نطاق مهامه، يُكلّف البنك المركزي بالحفاظ على سرية المعلومات الحساسة والمصنفة التي يتم جمعها من الجهات المصرفية. يتم التعامل مع أي خرق لهذه المعلومات كحادث أمني يتم معالجته وفقًا لبروتوكولات الاستجابة للحوادث المعتمدة.

الجمهور المستهدف

يستهدف هذا الإطار جميع الأدوار داخل الجهة المعنية والتي تشارك في تصميم وتطوير ونشر وحوكمة أنظمة الذكاء الاصطناعي. وتشمل هذه الأدوار – دون أن تقتصر عليها – مجلس الإدارة، الإدارة التنفيذية والعليا، مالكي الأعمال وأصول المعلومات، مسؤولي المخاطر والامتثال، مهندسي الذكاء الاصطناعي وتعلم الآلة، علماء البيانات، إضافة إلى فرق أمن المعلومات وتقنية المعلومات.

الأهداف

يحدد هذا الإطار الأهداف العامة التالية:

١. **تعزيز تبنّي الذكاء الاصطناعي المسؤول والأخلاقي :** تشجيع الابتكار في مجال الذكاء الاصطناعي بما يتماشى مع قيم المملكة الأردنية الهاشمية، وضمان أن تكون القرارات المدعومة بالذكاء الاصطناعي متوافقة مع المعايير الأخلاقية.

٢. **ضمان الشفافية، المساءلة، والعدالة :**وضع آليات تتيح تفسير وتدقيق المنتجات والخدمات المالية المعتمدة على الذكاء الاصطناعي.

٣. **حماية خصوصية البيانات، الأمن، وحقوق المستخدم :**ضمان سرية وأمن وسلامة بيانات العملاء، بما يتوافق مع التشريعات الوطنية وأفضل الممارسات الدولية.

٤. **الحد من المخاطر المالية والتشغيلية والسمعة المؤسسية :**إنشاء عمليات لإدارة ومراقبة مخاطر الذكاء الاصطناعي بهدف حماية الاستقرار المالي والحفاظ على ثقة الجمهور بالخدمات المعززة بالذكاء الاصطناعي.

٥. **الامتثال للمعايير والأطر الدولية :**دمج أفضل الممارسات التنظيمية العالمية المعمول بها، وتعزيز التعاون العابر للحدود.

٦. **تعزيز أمن وصمود أنظمة الذكاء الاصطناعي :**ضمان تصميم وتطوير وتشغيل أنظمة الذكاء الاصطناعي وفق ضوابط قوية للأمن السيبراني، بما يكفل التصدي للتهديدات، وضمان استمرارية الخدمة، والحفاظ على الثقة في الأنظمة المعززة بالذكاء الاصطناعي

١. الحوكمة والاشراف

يُؤكد هذا الإطار على ضرورة إنشاء هياكل حوكمة متينة للذكاء الاصطناعي.

١,١ هيكل حوكمة الذكاء الاصطناعي

- ينبغي على كل جهة إنشاء لجنة تُشرف على أنشطة الذكاء الاصطناعي أو تفوّض هذه المسؤولية إلى جهة مختصة داخل الهيكل المؤسسي لضمان الحوكمة الفعّالة.
- المواءمة الاستراتيجية: يجب على كل جهة التأكد من أن مبادرات الذكاء الاصطناعي تتماشى مع الأهداف الاستراتيجية العامة للمؤسسة ومستوى تقبلها للمخاطر.

١,٢ تحديد مسؤوليات أعضاء اللجنة

تُعد لجنة الذكاء الاصـطناعي أو الجهة المكافئة لها جهة محورية في حوكمة وتوجيه اسـتخدام تقنيات الذكاء الاصـطناعي بشكل فعّال وأخلاقي داخلها. ولضمان أن تُدار الوظائف الجوهرية ضمن دورة حياة الذكاء الاصطناعي بمستوى مناسب من الإشراف على مستوى مجلس الإدارة، ينبغي على اللجنة المذكورة تقديم توجيه عالي المستوى وإشراف فعّال على المحاور التالية:

- **حوكمة الذكاء الاصطناعي والإشراف الأخلاقي:** الإشراف على النهج الأخلاقي والاستراتيجي للجهة فيما يخص الذكاء الاصطناعي، بما يشمل اعتماد أطر الحوكمة ذات الصلة، وضمان توافق السياسات مع الأهداف المؤسسية والمتطلبات التنظيمية، وتعزيز الشفافية والعدالة، ومراقبة تصميم الخوارزميات لتفادي التحيّز، وإدارة استخدام البيانات بما يضمن الخصوصية والامتثال، والتواصل مع أصحاب المصلحة لدعم المعايير القانونية والأخلاقية.
- **إدارة البيانات وحوكمتها:** الإشراف على ممارسات حوكمة البيانات على مستوى المؤسسة لضمان جودة البيانات ودقتها وسلامتها، واستخدامها بطريقة متوافقة مع الأطر التنظيمية عبر جميع أنظمة الذكاء الاصطناعي. ويشمل ذلك دعم مبادرات الذكاء الاصطناعي من خلال تطبيق ممارسات بيانات فعّالة، وضمان التوافق مع الأنظمة والتشريعات الخاصة بحماية البيانات.
- **أمن وصمود أنظمة الذكاء الاصطناعي:** الإشراف على تدابير الأمن السيبراني والجاهزية الخاصة بأنظمة الذكاء الاصطناعي، بما في ذلك معالجة مخاطر الأمن السيبراني من خلال التخطيط الاستراتيجي، والجاهزية للاستجابة للحوادث، ومراعاة استمرارية الأعمال، وتضمين الضوابط المناسبة في جميع مراحل دورة حياة النظام.
- **تكامل البنية التحتية والتقنية للذكاء الاصطناعي:** الإشراف على التكامل الاستراتيجي والمواءمة التشغيلية لأنظمة الذكاء الاصطناعي ضمن البنية التحتية التقنية للجهة. ويشمل ذلك التأكد من أن النماذج قابلة للتوسعة والاستدامة، وتخضع للصيانة المستمرة، وتُدار بمساءلة واضحة عن الأداء الفني والامتثال.

- **الامتثال التنظيمي والقانوني:** الإشراف على التزام الجهة بالمتطلبات القانونية والتنظيمية المرتبطة بالذكاء الاصطناعي، بما يشمل الامتثال لنقل البيانات عبر الحدود، والإشراف على الشراكات التقنية، ومراعاة حقوق الملكية الفكرية، وضمان التوافق مع تعليمات البنك المركزي الأردني والأطر الدولية ذات الصلة.

- **إدارة مخاطر الذكاء الاصطناعي:** الإشراف على مخاطر الذكاء الاصطناعي ضمن إطار إدارة المخاطر المؤسسية الشامل، بما يشمل توجيه عمليات تحديد المخاطر، وتقييمها، وتخفيفها، ومراقبتها، وضمان توافقها مع المعايير الأخلاقية والتنظيمية والاستراتيجية.

في حال عدم توفر دور أو مسؤول مخصص للإشراف على هذه المجالات داخل الجهة، يجب إنشاء مثل هذا الدور أو تعيين جهة مختصة. وفي حال تعذّر ذلك، ينبغي إسناد هذه المسؤوليات إلى لجان أو أدوار مناسبة داخل الجهة لضمان التغطية الكاملة والفعّالة.

١,٣ نهج قائم على المخاطر

لضمان نموذج حوكمة مسؤول وفعال للذكاء الاصطناعي، يجب على كل مؤسسة اعتماد نهج قائم على المخاطر لإدارة تطبيقات الذكاء الاصطناعي. ويتضمن ذلك ما يلي:

- يجب على المؤسسة وضع إطار قائم على المخاطر لتصنيف تطبيقات الذكاء الاصطناعي استنادًا إلى مستوى تأثيرها المحتمل (منخفض، متوسط، أو مرتفع)، وتطوير استراتيجيات إشراف ملائمة لكل تصنيف.

- ينبغي على المؤسسة دمج تقييمات مخاطر الذكاء الاصطناعي ضمن إطار إدارة المخاطر القائم لديها، بما يضمن معالجة مخاطر الذكاء الاصطناعي جنبًا إلى جنب مع المخاطر التقليدية الأخرى.

- ينبغي على الجهة تحديد خطوط مساءلة واضحة لضمان فاعلية الحوكمة، والامتثال، ورصد الأداء التشغيلي للأنظمة المعتمدة على الذكاء الاصطناعي.

- ينبغي على الجهة تبنّي نماذج الذكاء الاصطناعي بشكل تدريجي، والبدء بتطبيقها في الأنظمة غير الحرجة، بدلاً من نشرها على نطاق واسع منذ البداية، وذلك لضمان الجاهزية الكاملة قبل التوسع في نطاق الاستخدام. أما في الأنظمة الحرجة، فيجب دمج آليات "المستخدم البشري ضمن الحلقة (Human-in-the-Loop – HITL) " لضمان وجود إشراف بشري وتدخل عند الحاجة.

٢. الأخلاقيات والشفافية

لضمان التطبيق المسؤول لتقنيات الذكاء الاصطناعي، يجب على المؤسسات الالتزام بالمعايير الأخلاقية، وتعزيز مبادئ العدالة وعدم التمييز، وتقديم إفصاحات واضحة وشفافة حول استخدام الذكاء الاصطناعي ضمن عمليات اتخاذ القرار.

٢,١ الأخلاقيات

- ينبغي على المؤسسة تصميم وتشغيل أنظمة الذكاء الاصطناعي بما يراعي مصلحة المستهلك، وذلك وفقًا للتعليمات والتشريعات الصادرة عن البنك المركزي الأردني (CBJ) في هذا الشأن.
- ينبغي على المؤسسة التأكد من أن القرارات المعتمدة على الذكاء الاصطناعي تلتزم – على الأقل – بذات المعايير الأخلاقية المطبّقة على القرارات البشرية، بما يشمل مبادئ العدالة، الشفافية، المساءلة، وعدم التمييز.
- ينبغي على المؤسسة أخذ أفضل الممارسات العالمية ذات الصلة بعين الاعتبار لدعم العدالة الخوارزمية ومنع التمييز.
- ينبغي على المؤسسة تطوير سياسات شاملة خاصة بالذكاء الاصطناعي، تُحدد ضوابط الاستخدام، والاعتبارات الأخلاقية، ومتطلبات الامتثال، بما يضمن اتساقها مع معايير المؤسسة الأخلاقية، وقيمها، ومدونات السلوك المعتمدة لديها.

٢,٢ قابلية التفسير والإفصاح

- ينبغي على المؤسسة التأكد من أن أنظمة الذكاء الاصطناعي التي تُحدث أثرًا جوهريًا على العملاء – مثل نماذج التقييم الائتمانية أو أنظمة مكافحة الاحتيال – قادرة على إنتاج مخرجات قابلة للتفسير.
- ينبغي على المؤسسة توضيح آليات اتخاذ القرار المعتمدة على الذكاء الاصطناعي بشكل واضح لأصحاب المصلحة المعنيين – حيثما ينطبق – بهدف تعزيز الشفافية.
- ينبغي على المؤسسة تقديم إشعارات واضحة وبارزة للعملاء عند تعاملهم مع أنظمة قائمة على الذكاء الاصطناعي. ويجب أن يتم هذا الإفصاح في نقطة التفاعل (Point Of Interaction)، لضمان أن العملاء على دراية باستخدام نماذج الذكاء الاصطناعي في عمليات اتخاذ القرار، بما في ذلك كيفية تأثير البيانات المستخدمة في اتخاذ القرار والنتائج المحتملة المترتبة عليه.
- ينبغي على المؤسسة ضمان أن تكون قابلية التفسير موجهة بحسب فئة المستخدم. حيث يجب أن يحصل المستخدمون العامون على تفسيرات مبسطة وواضحة لقرارات الذكاء الاصطناعي، يجب أن يتاح للمستخدمين الفنيين إمكانية الوصول الى التفاصيل التشغيلية الدقيقة الخاصة بالنماذج، ويجب تزويد الجهات التنظيمية بتقارير تدقيق شاملة حول عمليات اتخاذ القرار لضمان الشفافية والامتثال.

٢,٣ استقلالية العميل وحقوق الانسحاب

- ينبغي على المؤسسة توفير خيارات واضحة للعملاء تسمح لهم بـ "الانسحاب" أو اختيار خدمات بديلة في حال عدم رغبتهم بالتعامل مع أنظمة تعتمد على الذكاء الاصطناعي، مع ضمان تقديم إجراءات بسيطة تُمكّنهم من اختيار الخدمات التقليدية أو غير المؤتمتة – حيثما يكون ذلك ممكنًا.

- ينبغي على المؤسسة التأكد من أن تمكين العميل من الانسحاب من العمليات المؤتمتة لا يؤدي إلى المساس بحقوقه في الحصول على الخدمات المصرفية الأساسية.

- ينبغي على المؤسسة ضمان قدرة العملاء على الوصول إلى بياناتهم الشخصية، وتصحيحها، وطلب حذفها – حيثما ينطبق – وذلك بما يتوافق مع الالتزامات القانونية والتنظيمية، لا سيما في سياق استخدام أنظمة الذكاء الاصطناعي التوليد (Generative AI).

٢,٤ المساءلة

- ينبغي على المؤسسة التأكد من أن استخدام أنظمة الذكاء الاصطناعي في عمليات اتخاذ القرار يتم بموافقة الإدارة الداخلية المختصة.

- ينبغي على المؤسسة أن تتحمّل المسؤولية الكاملة عن القرارات المدعومة بالذكاء الاصطناعي، سواء تم تطوير النظام داخليًا أو الحصول عليه من مصدر خارجي.

- ينبغي على المؤسسة الحفاظ على قنوات تواصل مفتوحة تمكّن العملاء من تقديم الاستفسارات أو طلبات المراجعة بشأن القرارات المتخذة عبر أنظمة الذكاء الاصطناعي التي تؤثر عليهم.

- ينبغي على المؤسسة تعيين "مالك نظام الذكاء الاصطناعي" لكل نظام مستخدم، بحيث يكون مسؤولًا عن حوكمة النظام، أدائه، التزامه التنظيمي، ومواءمته الأخلاقية طيلة دورة حياته.

٢,٥ الدقة والتحيز

- ينبغي على المؤسسة إجراء مراجعة وتحقق دوري للبيانات والنماذج والقرارات الناتجة عن أنظمة الذكاء الاصطناعي، بهدف الكشف عن أي تحيّزات ومعالجتها، بما يضمن تحقيق العدالة في النتائج والمخرجات.

٢,٦ تقييمات الأثر الدورية

- ينبغي على المؤسسة إجراء تقييمات أثر دورية لتقنيات الذكاء الاصطناعي بما يتناسب مع مستوى المخاطر المرتبط بكل تطبيق، وذلك لتقييم مخاطر الخصوصية، واحتمالات التحيّز، أو أي انحراف عن أهداف الاستخدام المقصود أو معايير العدالة. ويجب أن تخضع تطبيقات الذكاء الاصطناعي عالية المخاطر لمراجعات أكثر تكرارًا وعمقًا لضمان نشرها بشكل مسؤول ومتوافق مع المبادئ الأخلاقية.

٣. الامتثال التنظيمي

تُسهم هذه الممارسات في ضمان أن يتم تصميم وتطوير وتشغيل أنظمة الذكاء الاصطناعي بما يتوافق مع القوانين والأنظمة والمعايير المعتمدة على المستويين التنظيمي والصناعي، بما يعزز الامتثال، ويُقلل من المخاطر القانونية والتشغيلية، ويُرسخ ثقة العملاء والجهات الرقابية.

٣,١ المواءمة مع الأنظمة والتشريعات المحلية والدولية

بالإضافة إلى هذا الإطار، ينبغي على المؤسسة التأكد من الالتزام بالأنظمة والتشريعات التالية وأي تعديلات لاحقة عليها:

التشريعات المحلية

- جميع الأنظمة، الإرشادات، الأطر التنظيمية، التعاميم، والتشريعات الأمنية الخاصة بالقطاع الصادرة عن البنك المركزي الأردني (CBJ) والواجب تطبيقها بحسب طبيعة نشاط المؤسسة.
- كافة القوانين والتشريعات الوطنية المتعلقة بالأمن السيبراني وحماية خصوصية البيانات الصادرة عن الجهات المختصة، بما في ذلك قانون حماية البيانات الشخصية رقم (٢٤) لسنة ٢٠٢٣، وأي تعليمات تنفيذية أو إرشادات مصاحبة له.

الامتثال الدولي وحوكمة الذكاء الاصطناعي عبر الحدود

يجب على المؤسسات التي تعمل على المستوى الدولي أو تتعاون مع مؤسسات أجنبية تقييم ودمج المتطلبات التنظيمية المحلية الخاصة بالذكاء الاصطناعي في الدول ذات العلاقة، لضمان الامتثال العابر للحدود.

ينبغي وضع سياسات مؤسسية تُمكّن من المتابعة المنتظمة للتغيرات في البيئة التنظيمية – محليًا ودوليًا – ومعالجتها بشكل استباقي، بما يضمن أن أنظمة الذكاء الاصطناعي تظل متوافقة مع المتطلبات القانونية والتنظيمية في جميع الولايات القضائية التي تنشط بها المؤسسة.

٣,٢ الالتزام بالمعايير الدولية

٣,٣ يُوصى بأن تعتمد المؤسسة أفضل الممارسات الدولية المعمول بها – حيثما ينطبق – مثل معايير ISO/IEC ، وإرشادات بنك التسويات الدولية (BIS) ، ومركز تحليل و مشاركة معلومات الخدمات المالية(FS-ISAC) ، ومنظمة التعاون الاقتصادي والتنمية (OECD) ، وصندوق النقد الدولي (IMF) ، وذلك لضمان إدارة فعّالة لمخاطر الذكاء الاصطناعي، وتعزيز أمن المعلومات، وتطبيق ضوابط جودة فعالة على أنظمة الذكاء الاصطناعي.

٤. إدارة البيانات

يوضح هذا الإطار أفضل الممارسات المتعلقة بخصوصية البيانات، وحمايتها، وجودتها، وسلامتها. ويجب على المؤسسات تطبيق سياسات قوية لحوكمة البيانات تضمن إدارة البيانات بشكل منظم وآمن، مع التأكيد على الاستخدام الأخلاقي والمسؤول للبيانات ضمن جميع مراحل تطوير وتشغيل أنظمة الذكاء الاصطناعي.

٤,١ خصوصية وأمن البيانات

إخفاء الهوية والتشفير

- ينبغي على المؤسسة الحد من استخدام البيانات شديدة الحساسية أو البيانات الشخصية (PII) في تدريب نماذج الذكاء الاصطناعي، ما لم يكن ذلك ضروريًا، مع التأكد من تطبيق تدابير حماية مناسبة لتلك البيانات.
- ينبغي على المؤسسة استخدام تقنيات مثل إخفاء الهوية، وإخفاء الهوية الجزئي(Pseudonymization) ، أو غيرها من الأساليب المعززة للخصوصية، بهدف تقليل مخاطر الكشف غير المصرح به للبيانات.
- ينبغي على المؤسسة اعتماد تقنيات تشفير قوية لحماية البيانات أثناء التخزين والنقل، بما يتوافق مع المعايير المعترف بها دوليًا، لضمان أمن البيانات وسريتها.
- ينبغي على المؤسسة تطبيق ضوابط صارمة للوصول إلى البيانات، تضمن أن البيانات المستخدمة ضمن أنظمة الذكاء الاصطناعي لا يمكن الوصول إليها إلا من قبل الموظفين المخوّلين فقط.

تقليل البيانات والاحتفاظ بها

- ينبغي على المؤسسة جمع الحد الأدنى من البيانات اللازمة فقط لتشغيل العمليات المدعومة بالذكاء الاصطناعي، والاحتفاظ بهذه البيانات فقط طوال الفترة المطلوبة لتحقيق الأغراض المُعلنة.
- ينبغي على المؤسسة إجراء عمليات حذف دوري أو أرشفة آمنة للبيانات التي لم تعد ضرورية، مع توثيق هذه العمليات بشكل دقيق لضمان الامتثال التنظيمي وتعزيز المساءلة.

٤,٢ جودة البيانات وسلامتها

إطار حوكمة البيانات

- ينبغي على المؤسسة تطبيق سياسات حوكمة بيانات قوية، تحت إشراف رئيس إدارة البيانات (Chief Data Officer - CDO) أو أحد أعضاء الإدارة العليا المؤهلين، لضمان دقة البيانات، اكتمالها، حداثتها، توفرها، واتساقها عبر الأنظمة.

- ينبغي على المؤسسة اعتماد أفضل الممارسات لضمان جودة البيانات بشكل مستمر، بما في ذلك التأكد من أن البيانات قابلة للعرض وذات صلة ومحدّثة ودقيقة ومتسقة عبر جميع الأنظمة. كما يجب مراجعة البيانات السابقة (Historical Data) بعناية لتجنّب استخدام أنماط قديمة أو متحيّزة تؤثر سلبًا على أداء أنظمة الذكاء الاصطناعي.

التوثيق وإمكانية التتبع

- ينبغي على المؤسسة تعزيز إمكانية التتبع والمساءلة من خلال ضمان توثيق وتسجيل كافة البيانات، النماذج، القرارات، مدخلات المستخدم (User Prompt)، والتعديلات المعتمدة، بطريقة تُمكّن من مراجعتها وتدقيقها عند الحاجة.

- ينبغي على المؤسسة الاحتفاظ بسجلات واضحة لمصادر البيانات، وأساليب التنظيف والمعالجة المسبقة، وآليات التحكم في الإصدارات الخاصة بمجموعات التدريب والاختبار.

- ينبغي على المؤسسة تخزين سجلات التشغيل بطريقة آمنة وغير قابلة للتلاعب، بما يحفظ سلامة البيانات لغايات التدقيق التنظيمي أو التحقيقات الرسمية.

٥. التطوير والنشر الآمن

ضـــمان تطبيق تدابير الأمن الســـيبراني عبر جميع مراحل دورة حياة الذكاء الاصـــطناعي، بدءًا من التصـــميم وحتى التشغيل. ويجب على المؤسسة دمج بروتوكولات أمنية قوية، وإجراء اختبارات دورية، وضمان المراقبة المستمرة لأنظمة الذكاء الاصطناعي، بما يعزز الحماية من التهديدات، ويُحافظ على سلامة الأداء والامتثال التنظيمي.

٥,١ أمن نظام الذكاء الاصطناعي

نهج دورة الحياة الآمنة

- ينبغي على المؤسسة تطبيق تدابير الأمن السيبراني المنصوص عليها ضمن إطار الأمن السيبراني للقطاع المصرفي الاردني، وذلك لحماية أنظمة الذكاء الاصطناعي من مجموعة واسعة من التهديدات والثغرات الناشئة على امتداد جميع مراحل التشغيل.

- ينبغي على المؤسسة دمج ضوابط أمنية قوية وشاملة ضمن كامل دورة حياة نظام الذكاء الاصطناعي، بما يشمل – على سبيل المثال لا الحصر – مبدأ أقل الصلاحيات (Least Privilege) ، الأمن من خلال التصميم (Security by Design)، نموذج انعدام الثقة (Zero Trust)، ممارسات البرمجة الآمنة، تقييم الثغرات، منع تسرب البيانات (DLP)، الاختبار المستمر، ضوابط النشر، وأنظمة كشف التسلل المتقدمة. ويجب أن يمتد هذا النهج الأمني المتكامل ليشمل واجهات البرمجة (APIs) وأنماط استخدامها غير المعتادة، البنية التحتية الداعمة، مسارات البيانات، وإدارة النماذج، لضمان صمود النظام ضد التهديدات من بدءاً من مرحلة التطوير وحتى مرحلة الإيقاف.

- ينبغي على المؤسسة تخزين أصول النماذج – مثل بيانات التدريب ومعايير النماذج (Model Parameters) – في بيئات آمنة، مع تطبيق إجراءات التسجيل (Logging) وإدارة التغييرات لضمان سلامة البيانات والمساءلة المؤسسية.

٥,٢ التحقق من النماذج واختبارها

اختبار الدقة والتحيز والمتانة

- ينبغي على المؤسسة التحقق من صحة نماذج الذكاء الاصطناعي باستخدام سيناريوهات اختبار منظمة ومحاكاة ظروف التشغيل الواقعية، مع قياس مؤشرات الأداء مثل الدقة (Accuracy) ، الدقة الإيجابية (Precision)، الاسترجاع (Recall) وغيرها من المقاييس ذات الصلة.

- ينبغي على المؤسسة تقييم متانة أنظمة الذكاء الاصطناعي من خلال تطبيق منهجيات اختبار شاملة، تشمل الاختبار خارج العينة (Out-of-Sample Testing)، المقارنة المعيارية (Benchmarking) ، تحليل الحساسية، اختبار الإجهاد، اختبار تنوّع البيانات، تقييم الحالات الحدّية (Edge Cases) ، تحليل انحراف المفهوم (Concept Drift) ، واختبار التوافق التشغيلي (Interoperability Testing).

- ينبغي على المؤسسة دمج تقنيات التعلم العدائي (Adversarial Learning) ضمن مراحل تدريب النماذج واختبارها، بهدف تعزيز قدرتها على مواجهة الهجمات أو المدخلات المصممة للتلاعب، وضمان صمود الأنظمة أمام محاولات الاستغلال.

- ينبغي على المؤسسة إجراء اختبارات اختراق دورية وتقييمات للثغرات على خدمات الذكاء الاصطناعي والبنية التحتية الداعمة، بما في ذلك معالجة تحديات الهَلوسة (Hallucination) والتحايل على القيود الأمنية (Jailbreaking) في نماذج الذكاء الاصطناعي التوليدي.

آليات الفشل الآمن (Fail-Safe Mechanisms)

- ينبغي على المؤسسة تصميم أنظمة الذكاء الاصطناعي لتتضمن إجراءات احتياطية أو مراجعة بشرية، بما يضمن الحد من الأخطاء المنهجية أو سوء الاستخدام.

- ينبغي على المؤسسة تطوير استراتيجيات طوارئ تشمل آليات إيقاف فوري (Kill Switch) تتيح التدخل البشري المباشر عند حدوث أعطال أو سلوك غير متوقع، لا سيما في التطبيقات الحرجة، بهدف منع وقوع أخطاء جوهرية أو حالات إساءة استخدام.

- ينبغي على المؤسسة تطبيق آليات المستخدم البشري ضمن الحلقة – (Human-on-the-Loop (HOTL) لضمان وجود إشراف بشري مستمر خلال تشغيل أنظمة الذكاء الاصطناعي، وخصوصًا في الحالات ذات الحساسية التشغيلية أو التنظيمية العالية.

- ينبغي على المؤسسة معالجة المشكلات المكتشفة بسرعة وكفاءة، مع توثيق الحلول والإجراءات المتخذة بما في ذلك حالات قبول المخاطر عند الاقتضاء، لدعم الامتثال والمساءلة.

المعايرة (Calibration)

- ينبغي على المؤسسة تحديث نماذج الذكاء الاصطناعي بشكل دوري بما يتماشى مع تغيرات ظروف السوق، المتطلبات التنظيمية، وسلوكيات المستخدمين.

٥,٣ المراقبة المستمرة والتدقيق

المراقبة المستمرة للأداء

- ينبغي على المؤسسة مراقبة أداء أنظمة الذكاء الاصطناعي بشكل مستمر، مع تحديد مستوى المراقبة وفقًا لحالة الاستخدام ومستوى المخاطر. ويجب استخدام تنبيهات مؤتمتة – حيثما أمكن – لرصد الانحرافات أو تراجع دقة النموذج، بما يضمن التدخل الفوري والحد من المخاطر.

- ينبغي على المؤسسة تقييم أداء أنظمة الذكاء الاصطناعي بصفة دورية، مع توثيق نتائج التقييم والمراجعة لتعزيز الشفافية والتحسين المستمر.

٥,٤ الإشراف البشري على أنظمة الذكاء الاصطناعي

- ينبغي على المؤسسة تضمين آليات "الإنسان ضمن الحلقة (Human-in-the-Loop - HITL) " و"الإنسان فوق الحلقة (Human-on-the-Loop - HOTL) "بما يتناسب مع درجة أهمية النظام ومستوى المخاطر المرتبطة به، بحيث يتم ضمان وجود إشراف وتدخل بشري عند الحاجة في الأنظمة الحرجة، مع إخضاع الأنظمة عالية المخاطر لمراقبة بشرية مستمرة أثناء تشغيل الذكاء الاصطناعي.

٦. الاستجابة للحوادث، واستمرارية الأعمال، والتعافي من الكوارث

تُوجّه المؤسسات إلى تطوير خطط لإدارة الحوادث، وتحديد أدوار ومسؤوليات واضحة للتعامل مع الأعطال أو الانحرافات الناتجة عن أنظمة الذكاء الاصطناعي، مع ضمان استمرارية الأعمال في مواجهة أي اضطرابات قد تنشأ عن هذه الأنظمة.

٦,١ خطة إدارة الحوادث

بروتوكولات الحوادث الخاصة بالذكاء الاصطناعي

- ينبغي على المؤسسة تطوير إجراءات مخصصة للتعامل مع الحوادث المرتبطة بالذكاء الاصطناعي، أو دمجها ضمن إجراءات الاستجابة للحوادث المعتمدة على مستوى المؤسسة، بما يتماشى مع الأطر والمعايير التنظيمية ذات الصلة.

مشاركة المعلومات والتقارير التنظيمية

- ينبغي على المؤسسة إنشاء سجل مركزي خاص بحوادث الذكاء الاصطناعي، يُستخدم لتوثيق الحوادث، الثغرات، والمخاوف الأمنية المرتبطة بتطبيقات الذكاء الاصطناعي.
- ينبغي على المؤسسة إخطار وحدة الاستجابة للحوادث السيبرانية للقطاع المالي والمصرفي (FinCERT) / البنك المركزي الأردني (CBJ) بشكل فوري بأي حادث مرتبط بالذكاء الاصطناعي، وفقًا للتعليمات الصادرة عن البنك المركزي بالخصوص.
- ينبغي على المؤسسة مشاركة معلومات التهديدات وأفضل الممارسات ذات الصلة مع مجتمع القطاع المالي، بما يتماشى مع تطور مخاطر الذكاء الاصطناعي.

٦,٢ تخطيط استمرارية الأعمال

دمج استمرارية الأعمال مع عمليات الذكاء الاصطناعي

- ينبغي على المؤسسة تحديث خطط استمرارية الأعمال والتعافي من الكوارث لتشمل تطبيقات الذكاء الاصطناعي المصنفة على أنها حرجة للعمليات المصرفية اليومية.

التمارين الدورية واختبارات الإجهاد

- ينبغي على المؤسسة تنفيذ تمارين قائمة على سيناريوهات تشغيلية، بما في ذلك أسوأ الاحتمالات مثل فشل أنظمة الذكاء الاصطناعي أو الهجمات السيبرانية الموجهة.
- ينبغي على المؤسسة تقييم مستوى الجاهزية بهدف تقليل الانقطاعات التشغيلية وحماية البنية التحتية الحرجة.

٧. إدارة مخاطر الأطراف الخارجية

تشمل هذه الممارسات تقييم ومراقبة مزوّدي الخدمات الخارجيين الذين يساهمون في تصميم أو تطوير أو تشغيل أنظمة الذكاء الاصطناعي لدى المؤسسة، وذلك لضمان امتثالهم للمعايير الأمنية والتنظيمية، وتقليل المخاطر الناتجة عن الاعتماد على أطراف خارجية في مكونات حرجة من منظومة الذكاء الاصطناعي.

٧,١ تقييم مخاطر المزودين

العناية الواجبة (Due Diligence)

- ينبغي على المؤسسة إجراء تقييمات دقيقة وشاملة لحلول الذكاء الاصطناعي المقدمة من المزوّدين الخارجيين، مع التأكد من امتثالهم لتعليمات **البنك المركزي الأردني (CBJ)** وأي تشريعات محلية ذات صلة، وذلك وفقًا لحساسية النموذج وأهميته.
- ينبغي على المؤسسة التحقق من الاعتمادات، وضوابط حماية البيانات، والسجل التوثيقي الذي يثبت أن المزوّد يدير نماذج الذكاء الاصطناعي بشكل مسؤول ومتوافق مع المعايير.
- ينبغي على المؤسسة التأكد من أن الأطراف الثالثة المسند إليها الخدمات تملك المهارات والخبرات الفنية اللازمة.
- ينبغي على المؤسسة تقييم مستوى الشفافية وقابلية التفسير في نماذج الذكاء الاصطناعي، والتأكد من قدرة المزوّد على تقديم تفسيرات مفهومة لآليات اتخاذ القرار متى كان ذلك ممكنًا.
- ينبغي على المؤسسة تقييم أساليب المزوّد في اكتشاف ومعالجة التحيّزات داخل النماذج، لضمان منع التمييز وتعزيز العدالة.
- ينبغي على المؤسسة التحقق من أن المزوّد يُطبق إجراءات قوية لاختبار النماذج والتحقق من صحتها لضمان الدقة والموثوقية.
- ينبغي على المؤسسة التأكد من أن المزوّد يمتلك آلية واضحة لتحديث وصيانة نماذج الذكاء الاصطناعي، بما يشمل التعامل مع المكوّنات أو التقنيات التي تم إيقافها أو تجاوزها.
- ينبغي على المؤسسة التأكد من التزام المزوّد بـ ممارسات الذكاء الاصطناعي الأخلاقية، بما في ذلك العدالة، والمساءلة، والشفافية في تشغيل الأنظمة.

توزيع الاعتمادية على المزوّدين والشفافية

- ينبغي على المؤسسة أن تكون حذِرة تجاه تمركز الاعتمادية على المزوّدين، وأن تسعى – قدر الإمكان – إلى توزيع مزوّدي حلول الذكاء الاصطناعي ضمن بيئتها التشغيلية. يساعد دمج تقنيات ومناهج، ومزوّدين

مختلفين في تقليل مخاطر التماثل السلوكي(Herding Behavior) ، وتجنّب الاعتماد المفرط على مزوّد واحد أو مجموعة ضيقة من المزوّدين، وضمان الصمود التشغيلي.

- ينبغي على المؤسسة أن تطلب من المزوّدين الخارجيين – حيثما ينطبق – تقديم قائمة مكونات نظام الذكاء الاصطناعي (AI Bill of Materials – AIBOM) لجميع الأنظمة أو الحلول المقدّمة، بما يضمن الشفافية وسهولة التتبع.

الالتزامات التعاقدية

- ينبغي على المؤسسة تضمين بنود تعاقدية صريحة تغطي المسؤوليات والمسائل القانونية، خصوصية البيانات، حقوق الملكية الفكرية، تقليل التحيّز، قابلية التفسير، والامتثال للمعايير ذات الصلة.
- ينبغي على المؤسسة التأكد من أن العقود مع المزوّدين تتضمن حقوق تدقيق واضحة، تتيح للمؤسسة تنفيذ مراجعات مباشرة أو الحصول على تقارير تدقيق صادرة عن مدققين مؤهلين.
- ينبغي على المؤسسة التأكد من أن العقود تتضمن أحكامًا تنظم التعاون في التحقيقات والاستجابة للحوادث، بما يضمن الوصول الفوري إلى المعلومات اللازمة والدعم الفني عند الحاجة.
- ينبغي على المؤسسة وضع استراتيجيات إنهاء شاملة تضمن انتقالًا سلسًا للبيانات والمعرفة في حال إنهاء التعاقد مع المزوّد.
- ينبغي على المؤسسة التأكد من الحد الأدنى من الانقطاع في الخدمات المعززة بالذكاء الاصطناعي أثناء عملية الانتقال بين المزوّدين.

٨. التعاون والتوعية والتدريب

يُعد إشراك أصحاب المصلحة والتثقيف المستمر عاملين أساسيين للبقاء على اطّلاع واستعداد دائم لمواكبة تطورات الذكاء الاصطناعي. ويشجّع هذا الإطار على التعاون مع مجتمعات الذكاء الاصطناعي المحلية والعالمية، مع التأكيد على أهمية الحصول على شهادات مهنية في الذكاء الاصطناعي وتعزيز الوعي المجتمعي من خلال حملات تثقيفية موجهة.

٨,١ إشراك أصحاب المصلحة

التعاون الدولي

- ينبغي على المؤسسة الانخراط بشكل فعّال مع مجتمعات الذكاء الاصطناعي المحلية والعالمية، والهيئات التنظيمية الدولية، ومجموعات العمل المتخصصة، وذلك بهدف متابعة التوجهات الناشئة في القطاع، وتبادل المعرفة والمعلومات، والتعاون في تطوير وتبني أفضل الممارسات.

التعليم وبناء القدرات

- ينبغي على المؤسسة توفير برامج تدريبية مستمرة لجميع العاملين المشاركين في دورة حياة الذكاء الاصطناعي، بما يشمل علماء البيانات، المدققين، المطورين، موظفي الأمن السيبراني، فرق الامتثال، والإدارة التنفيذية، وذلك في مجالات مثل: إدارة مخاطر الذكاء الاصطناعي، الأخلاقيات، تقليل التحيّز، قابلية التفسير، التهديدات الناشئة، والأمن السيبراني.

شهادات اعتماد لمتخصصي الذكاء الاصطناعي

- ينبغي على المؤسسة تشجيع أو إلزام الموظفين بالحصول على شهادات معتمدة في حوكمة الذكاء الاصطناعي، تقييم المخاطر، والأمن السيبراني، لضمان جاهزيتهم الفنية وتعزيز مستوى الامتثال والحوكمة ضمن بيئة عمل قائمة على الذكاء الاصطناعي.

حملات التوعية

- ينبغي على المؤسسة تنفيذ حملات توعوية موجهة للجمهور لتعريف العملاء بالخدمات المصرفية المعززة بالذكاء الاصطناعي، وحقوقهم المتعلقة بالخصوصية، وحماية بياناتهم.

- ينبغي على المؤسسة تزويد العملاء بإرشادات واضحة حول كيفية الاستخدام السليم للنظام أو النموذج، بما يعزز فهمهم ويُسهم في تجربة آمنة وشفافة.

٩. المراجعة والتحسين المستمر

يعدّ التحسين عملية مستمرة تفرضها الوتيرة المتسارعة لتطور التكنولوجيا، إلى جانب التغيرات التدريجية في تركيبة القطاع المالي مع ظهور أنواع جديدة من المؤسسات، المنتجات، والخدمات، فضلاً عن الاعتماد المتزايد على مزوّدي الخدمات من الأطراف الثالثة. وفي هذا السياق، سيتولى البنك المركزي الأردني (CBJ) مراجعة إطار عمل الذكاء الاصطناعي والوثائق والأدوات ذات الصلة بشكل دوري كل عامين، لضمان استمرارية الملاءمة والفعالية في مواجهة المتغيرات المستمرة.

يجوز للمؤسسات أيضًا طلب تحديث للإطار ، من خلال تقديم طلب رسمي معتمد من إدارة الذكاء الاصطناعي ولجنة الذكاء الاصطناعي في المؤسسة، وذلك لضمان توافق الإطار مع الاحتياجات التشغيلية أو التغيرات المستجدة في بيئة العمل.

التواصل والتقارير

ينبغي على المؤسسة تعيين ممثليها الرسميين للتواصل والتنسيق مع البنك المركزي الأردني (CBJ) فيما يتعلق بتنفيذ هذا الإطار. ويجب أن تشمل قائمة الممثلين رئيس إدارة الذكاء الاصطناعي (Chief AI Officer - CAIO) أو أي منصب ذي صلة ضمن الهيكل المؤسسي، لضمان الكفاءة في الإبلاغ والتطبيق العملي للإطار.

معلومات التواصل

يجب أن تُوجَّه جميع الاتصالات الرسمية الصادرة عن ممثلي المؤسسات الأعضاء إلى البريد الإلكتروني التالي:
fincert@cbj.gov.jo