دليل الحوكمة لمبادرة "عين الصقر" لتعزيز أمن وسلامة قطاع الطيران

دليل الحوكمة الرقمية الشامل للتوأمة الرقمية في قطاع الطيران
مبادرة "عين الصقر"

الإصدار: 1.0
التاريخ: أغسطس 2025

إعداد: فريق عين الصقر
إشراف: اللجنة المنظمة لهاكاثون الطيران
بالشراكة مع: اللجنة المنظمة لهاكاثون الطيران

الفهرس

تمهيد:

يشهد قطاع الطيران العالمي اليوم تحولات جوهرية تعيد صياغة مفاهيم الأمان والكفاءة والاستدامة، مدفوعةً بتقنيات الثورة الصناعية الرابعة، وعلى رأسها الذكاء الاصطناعي والتوأمة الرقمية. وفي ظل هذه المتغيرات، تتقدم المملكة العربية السعودية بخطى واثقة لترسيخ ريادتها الإقليمية والدولية، مستندةً إلى رؤية المملكة 2030، التي جعلت من التحول الرقمي ركيزة أساسية للتميز السيادي والمؤسسي.

من هذا المنطلق، وُلدت مبادرة **"عين الصقر"** كاستجابة استراتيجية ذكية لمتطلبات العصر الجديد، حيث لم تعد سلامة وأمن الطيران مجرّد استجابة للحدث، بل تحولت إلى منظومة استباقية رقمية عالية الحسّ، تتنبأ بالمخاطر قبل وقوعها، وتستشرف السيناريوهات الحرجة، وتوجه الموارد بكفاءة لحظية. هذه المبادرة ليست مشروعًا تقنيًا عابرًا، بل تمثل تحولًا بنيويًا في فلسفة التشغيل والإدارة في أحد أكثر القطاعات حيوية وتعقيدًا.

تُعد التوأمة الرقمية جوهر هذا التحول. فهي ليست فقط نسخة افتراضية عن الواقع الفيزيائي، بل كيان رقمي حيّ يتطور مع الزمن، يُغذّى ببيانات آنية من الحساسات، ويستخدم الخوارزميات التحليلية والتنبؤية لدعم اتخاذ القرار. ومع ذلك، فإن التوأم الرقمي، رغم إمكانياته الهائلة، قد يُصبح عبئًا أو خطرًا إذا لم يُدار ضمن إطار حوكمي رشيد ومتكامل. ومن هنا تبرز أهمية هذا الدليل: فهو ليس وثيقة إدارية جامدة، بل هو **"دستور تشغيلي ذكي"** يحكم العلاقة بين الإنسان والتقنية والبيئة، ويضمن أن تعمل كافة المكونات - من أبسط أجهزة الاستشعار إلى أعقد نماذج الذكاء الاصطناعي - بتناغم وانضباط وشفافية.

لقد صُمّم هذا الدليل ليكون أداة تمكين، لا أداة تقييد. إنه يوفّر بنية حوكمة مرنة، تدعم التجريب المنضبط، وتسهل الابتكار المسؤول، وتبني الثقة بين مختلف أصحاب المصلحة: من المسافر العادي، إلى مشغل المطار، وصولًا إلى الشركاء الدوليين والمؤسسات الرقابية. كما يسهم في حماية السيادة الرقمية الوطنية على البنى التحتية الحيوية، ويؤسس لقيم الشفافية والامتثال والأداء العالي.

أخيرًا، لا يقتصر هذا الإطار الحوكمي على معالجة التحديات المحلية، بل يستلهم أفضل الممارسات العالمية (من ICAO، وIATA، وISO، وNIST)، ويُعيد مواءمتها ضمن سياق وطني سعودي أصيل، يوازن بين الطموح التقني والخصوصية التنظيمية والثقافية. وعليه، فإن **هذا الدليل يمثل خارطة طريق استراتيجية لبناء مطارات ذكية، متكاملة، وآمنة**، ويشكل مرجعية معيارية يمكن الاستشهاد بها إقليميًا وعالميًا كنموذج رائد للحوكمة الرقمية في قطاع الطيران.

قائمة التعريفات والاختصارات

GACA – الهيئة العامة للطيران المدني

الجهة التنظيمية العليا لقطاع الطيران المدني في المملكة العربية السعودية، والمسؤولة عن وضع السياسات والإطار التشريعي لضمان سلامة وأمن وكفاءة العمليات الجوية. وتُعد المرجعية الرئيسية لاعتماد السياسات المتعلقة بالتوأمة الرقمية وحوكمتها.

SDAIA – الهيئة السعودية للبيانات والذكاء الاصطناعي

الجهة الوطنية المختصة بتنظيم قطاع البيانات والذكاء الاصطناعي، وتمتلك صلاحيات تشريعية وتنفيذية لإرساء قواعد السيادة الرقمية، وحوكمة البيانات الضخمة، وتطوير الأطر الأخلاقية والتقنية لتوظيف الذكاء الاصطناعي بأمان وموثوقية.

ICAO – منظمة الطيران المدني الدولي

الوكالة المتخصصة التابعة للأمم المتحدة والمسؤولة عن وضع المعايير الدولية للطيران المدني. تلعب دورًا محوريًا في مواءمة حوكمة التوأم الرقمي مع متطلبات الأمن والسلامة الجوية وفق اتفاقية شيكاغو والملاحق التابعة لها، وعلى رأسها الملحق (Annex 17).

IATA – الاتحاد الدولي للنقل الجوي

منظمة تمثل شركات الطيران التجارية عالميًا، وتصدر أدلة وإرشادات تشغيلية تعزز الكفاءة التشغيلية والسلامة في المطارات وشركات الطيران، بما في ذلك التوصيات المتعلقة بالتكامل بين الأنظمة الرقمية والعمليات التشغيلية.

ISO – المنظمة الدولية للمعايير

هيئة عالمية غير حكومية تضع المعايير الفنية والتنظيمية، بما في ذلك المعايير المتعلقة بأمن المعلومات (ISO/IEC 27001)، والصحة والسلامة المهنية (ISO 45001)، وهي مرجعية أساسية في بناء إطار الحوكمة الرقمية.

NIST – المعهد الوطني للمعايير والتقنية

مؤسسة بحثية أمريكية رائدة، تُعد مرجعًا دوليًا في إطار الأمن السيبراني للقطاعات الحيوية، ويُعتمد إطارها (NIST Cybersecurity Framework) كإطار مرجعي لحماية التوأم الرقمي من التهديدات السيبرانية المتقدمة.

AI – الذكاء الاصطناعي (Artificial Intelligence)

فرع متقدم من علوم الحوسبة يُمكّن الأنظمة الرقمية من التعلم، التنبؤ، واتخاذ القرارات بشكل ذاتي. يشكل

"العقل" التحليلي للتوأمة الرقمية، ويُستخدم في رصد المخاطر، تحسين الحركة الجوية، وتوجيه الموارد بكفاءة تنبؤية.

IoT – إنترنت الأشياء (Internet of Things)

شبكة من الأجهزة والمستشعرات المتصلة التي تجمع البيانات البيئية والتشغيلية لحظيًا. تمثل "الأعصاب الحسية" للتوأم الرقمي، وتزود النظام بالمدخلات اللحظية الضرورية لتحليل الواقع الفيزيائي بشكل دقيق.

Edge Computing – الحوسبة الطرفية

تقنية معالجة البيانات على مستوى الأجهزة القريبة من المصدر (مثل الكاميرات والمستشعرات) بدلاً من إرسالها إلى الخوادم المركزية. تتيح استجابات أسرع في البيئات الحساسة مثل المطارات، وتُعزز من مرونة التوأم الرقمي.

Digital Twin – التوأمة الرقمية

نموذج رقمي ديناميكي يعكس الواقع الفيزيائي (مثل مطار أو نظام ملاحة جوية) في الزمن الحقيقي، ويُستخدم للمراقبة، المحاكاة، التنبؤ، وصنع القرار. يُعد حجر الأساس في مبادرة "عين الصقر" للتحول إلى بيئة تشغيلية استباقية.

KPIs – مؤشرات الأداء الرئيسية (Key Performance Indicators)

مجموعة من المؤشرات الكمية التي تُستخدم لقياس كفاءة وفعالية أداء النظم الرقمية، بما في ذلك وقت الاستجابة، معدلات الحوادث، جودة البيانات، ومستوى الامتثال. تُعتبر مؤشرات KPIs أداة جوهرية في حوكمة الأداء والتحسين المستمر.

C4i – القيادة والسيطرة والاتصالات والحاسبات والذكاء

مفهوم استراتيجي متكامل يصف البنية التنظيمية للقيادة والتحكم في البيئات التشغيلية الحرجة. يُعد الإطار المفاهيمي الذي يُلهم تصميم التوأم الرقمي في بيئة الطيران، لضمان الاستجابة الذكية والسيطرة في الحالات الطارئة.

SOPs – إجراءات التشغيل القياسية (Standard Operating Procedures)

مجموعة من الإجراءات المكتوبة والمعتمدة لتنفيذ المهام التشغيلية بطريقة موحدة وآمنة. ويُعد دمجها في نظم التوأمة الرقمية عنصرًا حاسمًا لضمان الالتزام، التكرار الموثوق، والتحسين التراكمي.

أولًا: المحاور الرئيسية لدليل الحوكمة الرقمية في قطاع الطيران

الإطار المؤسسي والتنظيمي للحوكمة الرقمية

إن بناء إطار مؤسسي وتنظيمي فعّال لحوكمة التوأمة الرقمية لا يُعد خيارًا تنظيميًا فحسب، بل يمثل حجر الزاوية في ضمان استدامة وسلامة وكفاءة البيئة الرقمية الذكية، خصوصًا في قطاع سيادي حساس كقطاع الطيران. يهدف هذا الإطار إلى ترسيخ الانضباط المؤسسي، وضبط توزيع الصلاحيات والمسؤوليات، وتأسيس منظومة متكاملة تتسم بالشفافية والمساءلة والتكامل المؤسسي.

1. السياسات العامة للحوكمة الرقمية

تُشكّل السياسات العامة الإطار الأعلى الذي تنبثق منه كافة الضوابط والإجراءات التنفيذية. وينبغي أن تركز على:

- **مبادئ السيادة الرقمية:** ضمان أن تكون جميع البيانات والأنظمة ضمن نطاق التحكم الوطني الكامل، وبما يتماشى مع تنظيمات الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA).
- **مرتكزات الحوكمة الفعّالة:** كالشفافية، المساءلة، الامتثال، الاستجابة اللحظية، وقابلية التوسع.
- **التدرج التشريعي:** من المبادئ العامة، إلى القواعد التنظيمية، وصولًا إلى أدلة التشغيل وSOPs، بما يضمن التماسك بين المستويات الثلاثة للتشريع الرقمي.

كما يجب أن تُراعي هذه السياسات التكامل مع السياسات التقنية والتشغيلية، بحيث لا تُفصل الحوكمة عن واقع البيئة التشغيلية الحية للمطار.

2. تحديد الأدوار والمسؤوليات

في بيئة التوأمة الرقمية، لا يمكن ترك المسؤوليات غامضة أو متداخلة؛ بل يجب تحديدها بدقة، مع الأخذ في الاعتبار تعقيد سلسلة القيمة الرقمية. ويتضمن ذلك:

- **الوحدة الوطنية للحوكمة الرقمية:** الجهة المرجعية العليا التي تقود تطوير السياسات، وتدير إطار الحوكمة، وتقوم بمراجعة الأداء والامتثال بشكل دوري.
- **مالك التوأم الرقمي (Digital Twin Owner):** مسؤول عن التكامل بين الواقع الفيزيائي والنموذج الرقمي، وضمان صحة البيانات والعمليات التحليلية.
- **مدير أمن المعلومات:** يتولى مسؤولية الأمن السيبراني، وضمان التوافق مع معايير NIST وISO/IEC 27001.
- **الجهات التشغيلية:** تشمل مديري المطار، وفرق التشغيل، ومقدمي الخدمات الأرضية، والذين يجب أن تُدمج أدوارهم ضمن بيئة الحوكمة الرقمية من خلال مصفوفات مسؤوليات واضحة (مثل RACI).

يُشترط توثيق هذه الأدوار داخل أدلة تشغيلية رسمية، واعتمادها ضمن الإطار المؤسسي العام.

3. التوافق مع الجهات الرقابية (مثل ICAO، SDAIA، GACA)

من غير الممكن بناء حوكمة رقمية فعّالة دون توافق تام مع الجهات التنظيمية ذات العلاقة، والتي تختلف من حيث التخصص والولاية التنظيمية، وتشمل:

- **الهيئة العامة للطيران المدني (GACA):** تضع الإطار التنظيمي العام لسلامة وأمن الطيران، ويجب مواءمة الحوكمة الرقمية مع لوائحها، لا سيما في الجوانب المتعلقة بعمليات التفتيش، الاعتماد، والمخاطر التشغيلية.
- **SDAIA:** تؤطر حوكمة البيانات والسيادة الرقمية، بما يشمل السياسات الوطنية للبيانات، المصادقة على المعالجات الذكية، وضمان التوافق مع مبادئ الذكاء الاصطناعي المسؤول.
- **ICAO:** تُمثّل المرجعية العالمية في تنظيم قطاع الطيران المدني، ويجب التوافق مع ملاحقها الفنية مثل Annex 17 للأمن، وAnnex 14 للسلامة، لضمان الاعتراف الدولي بالحوكمة الوطنية.

يُعد التوافق مع هذه الجهات عامل تمكين استراتيجي، يضمن القبول المحلي والدولي لمنظومة التوأمة الرقمية، ويفتح المجال أمام عمليات الترخيص، التوسعة، والتشغيل العابر للحدود.

خلاصة المحور

إن الإطار المؤسسي والتنظيمي للحوكمة الرقمية ليس مجرد تشكيل هيكلي أو تنظيمي، بل هو منظومة حيوية تضمن أن تعمل التقنيات المتقدمة ضمن حدود واضحة، بفاعلية واستدامة. وعليه، فإن نجاح مبادرة "عين الصقر" يعتمد على مدى نضج هذا الإطار، وانسجامه مع السياقات التنظيمية الوطنية والدولية، ومدى قدرته على التفاعل مع التغيرات الديناميكية في بيئة الطيران الرقمي.

📘 حوكمة البيانات الرقمية

تُعد البيانات القلب النابض لمنظومة التوأمة الرقمية، فهي الوقود الذي يُشغّل المحاكاة، ويُغذّي التحليلات التنبؤية، ويُنتج المعرفة التشغيلية. وفي بيئة عالية الحساسية مثل المطارات، يصبح التحكم في البيانات ومعاييرها وأمنها أولوية استراتيجية لا تقبل التهاون. ولهذا، تركز الحوكمة الرقمية على ثلاث ركائز جوهرية: **تصنيف البيانات، إدارة الوصول، والتوافق مع الأطر العالمية للأمن السيبراني.**

1. تصنيف البيانات الأمنية والتشغيلية

في بيئة التوأمة الرقمية، تتنوع البيانات من حيث طبيعتها وحساسيتها، ما يستوجب إطارًا منهجيًا واضحًا لتصنيفها وفق مستويات الأهمية والخطر. يشمل التصنيف:

- **البيانات السيادية (Sovereign Data):** مثل خرائط البنى التحتية، بيانات الحركة الجوية، معلومات الدفاع المدني، وهي بيانات محمية بمستوى عالٍ من السرية ولا يُسمح بتداولها إلا وفق اشتراطات أمنية مشددة.
- **البيانات التشغيلية (Operational Data):** مثل بيانات الجدولة، الصيانة، حالات الطوارئ، ومؤشرات الأداء اللحظي. تُستخدم لدعم اتخاذ القرار اليومي، وتُعد حساسة من حيث الوقت والدقة.
- **البيانات التفاعلية والسلوكية (Behavioral/Engagement Data):** الناتجة عن تفاعل المسافرين والزوار مع المرافق الرقمية (مثل الكاميرات البيومترية، بوابات السفر الذكية، إنترنت الأشياء). تتطلب ضوابط خصوصية صارمة، خصوصًا عند تحليلها بنماذج الذكاء الاصطناعي.
- **البيانات العامة (Public/Open Data):** التي يمكن إتاحتها لأغراض البحث أو التوعية (مثل تقارير الأداء السنوية)، ولكن يجب أن تخضع لمراجعة منعًا لتسريب معلومات غير مقصودة.

ينبغي أن يُرفق بكل نوع من البيانات تسمية تصنيفية واضحة (Data Tagging)، وسياسة تعامل محددة، يتم تطبيقها تلقائيًا من خلال محركات الحوكمة الذكية في التوأم الرقمي.

2. ضوابط الوصول وإدارة صلاحيات المستخدمين

إدارة الوصول ليست فقط أداة للتحكم، بل هي خط الدفاع الأول ضد المخاطر التشغيلية والهجمات السيبرانية. ويشترط في الحوكمة الفعالة أن تتضمن:

- **مبدأ "أقل صلاحية" (Least Privilege):** بحيث يُمنح كل مستخدم أقل مستوى من الصلاحية اللازمة لأداء مهامه فقط، مع قيود زمنية ومكانية عند الضرورة.
- **إدارة هويات المستخدمين (Identity Management):** باستخدام تقنيات متعددة العوامل (MFA)، وربط الهوية الرقمية بمستوى التصنيف الأمني الوظيفي.
- **التفويض الديناميكي (Dynamic Role Assignment):** حيث يتم تعديل الصلاحيات تلقائيًا وفقًا للسياق التشغيلي، مثل تغيير المهام في حالات الطوارئ، أو تبدّل جداول العمل.
- **التتبع الكامل (Full Auditability):** لكل عملية وصول أو تعديل أو حذف، مع سجل رقمي غير قابل للتلاعب يُستخدم في التحقيقات أو التقييمات الأمنية.
- **الفصل بين البيئات (Environment Segregation):** بحيث يُفصل بين بيانات التطوير، والاختبار، والتشغيل الفعلي، لتقليل فرص الخطأ أو الاختراق.

تُدار هذه السياسات من خلال أنظمة GRC (الحوكمة والمخاطر والامتثال) المدمجة في نواة التوأم الرقمي.

3. التوافق مع معايير الأمان السيبراني (ISO 27001، NIST)

لضمان اعتماد الحوكمة محليًا ودوليًا، يجب أن يكون الإطار ملتزمًا بأرقى المعايير العالمية، ومنها:

- **ISO/IEC 27001:** المعيار الدولي لنظم إدارة أمن المعلومات، ويغطي الجوانب المتعلقة بضمان سرية وتكامل وتوافر البيانات (CIA Triad). ويجب أن يتضمن دليل الحوكمة متطلبات هذا المعيار ضمن السياسات التشغيلية، مع التزام بالتدقيق السنوي والتحسين المستمر.
- **NIST Cybersecurity Framework:** يقدم منهجًا مرنًا ومتكاملاً لإدارة مخاطر الأمن السيبراني، عبر خمس وظائف رئيسية: التحديد، الحماية، الكشف، الاستجابة، والتعافي. ويمكن مواءمة هذه الوظائف مع حالات الاستخدام اليومية في بيئة المطار، مثل اختراق أنظمة المراقبة أو تعطّل مكونات IoT.

كما ينبغي الاستفادة من أدوات التقييم الذاتي (Cyber Maturity Assessment Tools) لقياس مستوى التوافق الدوري، وربط نتائجها بمؤشرات الأداء في وحدة الحوكمة.

خلاصة المحور

إن حوكمة البيانات الرقمية ليست عملية تقنية معزولة، بل نظام عصبي حيوي يمكّن المنظومة من التفاعل الذكي، ويحميها من الانكشاف، ويمنحها ثقة الجهات التنظيمية والمجتمع. وتظل فعالية التوأمة الرقمية مرهونة بصرامة الحوكمة ووضوح التصنيف، ودقة إدارة الوصول، والتزام لا يتزعزع بمعايير الأمان العالمية.

📘 حوكمة منظومة التوأمة الرقمية

تمثل التوأمة الرقمية نقلة نوعية في تشغيل وإدارة المطارات، حيث تنصهر النماذج الرقمية الذكية مع الواقع الفيزيائي لتشكيل منظومة تشغيلية متكاملة وديناميكية. غير أن هذه القدرات الهائلة لا تُثمر بكامل فعاليتها إلا إذا كانت محكومة بإطار رشيد يضمن تكامل الأنظمة، صحة البيانات، وسلامة قراراتها. وهنا تأتي حوكمة منظومة التوأم الرقمي كعنصر مفصلي في ضمان الكفاءة، الموثوقية، والسيادة الرقمية على البيئة التشغيلية.

1. تكامل الأنظمة التشغيلية والرقمية

التوأم الرقمي ليس منصة منفصلة، بل منظومة تعتمد على الترابط الكامل بين البنية التحتية الفيزيائية، ونظم المعلومات التشغيلية، والحلول الرقمية التحليلية. وتتحقق الحوكمة في هذا المحور عبر:

- **خريطة تكامل الأنظمة (System Integration Blueprint):** توضح العلاقات الفنية والمنطقية بين أنظمة إدارة المطار (AODB)، أنظمة الأمن والسلامة، أجهزة الاستشعار (IoT)، ومنصات الذكاء الاصطناعي.

- **حوكمة واجهات الربط (API Governance):** ضمان أن تكون كافة واجهات الربط موثوقة وآمنة ومُوثقة بشكل مركزي، مع تحديد سياسات واضحة لإدارة الإصدارات، ومراقبة التفاعل بين الأنظمة.
- **التزامن الزمني الموحد (Time Synchronization):** فرض التزام زمني موحد على جميع مصادر البيانات لضمان أن تكون المشاهدات الرقمية المعروضة في التوأم متزامنة لحظيًا مع الأحداث الفعلية.
- **نظام إدارة التغيير (Change Management):** أي تحديث على الأنظمة الفيزيائية أو الرقمية يجب أن يخضع لإجراءات مراجعة ومصادقة مشتركة، تضمن عدم الإخلال بتكامل المنظومة.

2. مراقبة البيانات اللحظية عبر التوأم الرقمي

الحوكمة الحقيقية للتوأم الرقمي تبدأ من البيانات ذاتها؛ دقتها، استمراريتها، وسياقيتها. ويشمل ذلك:

- **مصفوفة مصادر البيانات (Data Source Matrix):** تحدد كل جهاز أو نظام يزوّد التوأم الرقمي بالبيانات، ونوع البيانات، وتكرار التحديث، وآلية التحقق من صحتها.
- **خوارزميات كشف الانحراف (Anomaly Detection):** يتم تفعيلها داخل التوأم لرصد أي بيانات خارجة عن النطاق المتوقع (مثل تغير مفاجئ في تدفق الركاب أو توقف أحد الحساسات)، بما يضمن الاكتشاف المبكر للحالات غير الطبيعية.
- **مؤشرات صحة البيانات (Data Quality KPIs):** تُقاس بشكل لحظي، وتشمل مؤشرات مثل: معدل التأخر الزمني في التحديث، نسبة البيانات الناقصة، معدل التكرار أو التضارب.
- **لوحات متابعة تشغيلية لحظية (Live Operational Dashboards):** تمكّن الجهات المعنية من متابعة الأداء في الزمن الحقيقي، ضمن واجهات تفاعلية تعتمد على بنية التوأم الرقمي.

الحوكمة هنا لا تقتصر على المتابعة، بل تشمل القدرة على "تجميد" بيانات المشهد اللحظي وتحليله بأثر رجعي، لدعم التحقيقات وتحسين القرارات المستقبلية.

3. دعم اتخاذ القرار المبني على الواقع الرقمي

تُعد التوأمة الرقمية أكثر من مجرد أداة عرض؛ إنها بنية معرفية متكاملة قادرة على دعم القرارات الحرجة بشكل مبني على واقع رقمي مدعوم بالبيانات. وتُفعَّل هذه القدرة من خلال:

- **نماذج القرار المدعومة بالسياق (Context-Aware Decision Models):** تأخذ في الاعتبار ليس فقط بيانات الحدث، بل السياق الأوسع المحيط به (مثل الطقس، الكثافة المرورية، مستوى التأهب الأمني).
- **خوارزميات التنبؤ الذكي (Predictive Intelligence):** تتنبأ بالحالات التشغيلية الحرجة (مثل ازدحام المسافرين في نقاط التفتيش) وتقترح إجراءات استباقية.
- **مصفوفات السيناريوهات (Scenario Matrices):** تربط الحالات اللحظية بخطط استجابة جاهزة (مثل تغيير توجيه الركاب، استدعاء طواقم إضافية)، مما يعزز سرعة الاستجابة ودقتها.
- **حوكمة القرار الآلي (Automated Decision Governance):** تحدد بوضوح متى يُسمح للنظام باتخاذ إجراء مباشر (مثل فتح ممر احتياطي)، ومتى يتطلب الأمر تدخلًا بشريًا معتمدًا.

هذا النمط من الحوكمة يعزز من الاعتمادية ويُقلل من الوقت المهدور في التحليل البشري، خاصة في البيئات عالية التغيير والتعقيد.

خلاصة المحور

إن حوكمة منظومة التوأمة الرقمية لا تعني فقط حماية النظام، بل تعني تفعيله كمنصة تشغيلية ذكية، تتفاعل مع الواقع لحظيًا، وتُغذّي القرارات بالمعلومات الدقيقة، وتعمل كجسر معرفي بين التقنية والعمليات التشغيلية. وبهذا، تنتقل بيئة المطار من مجرد "مُستقبِل للحدث" إلى بيئة **استباقية متكيفة**، تقودها البيانات وتدعمها الحوكمة.

📘 حوكمة الأمن والسلامة التشغيلية

في بيئة مطارات المستقبل، لم تعد السلامة والأمن مجرّد مهام تنفيذية معزولة، بل أصبحت منظومة استراتيجية رقمية متكاملة، تُدار وفقًا لفلسفة الاستباق لا الاستجابة، وتعتمد على البيانات اللحظية والتحليل الذكي أكثر من الاعتماد على المراقبة البشرية وحدها. إن حوكمة الأمن والسلامة التشغيلية في هذا السياق تمثل الإطار المسؤول عن مواءمة هذه المتغيرات، وضمان أن تعمل كل مكونات المنظومة بتناغم وتكامل ومرونة قصوى، مع الالتزام الكامل بالمعايير الوطنية والدولية.

1. قيادة موحدة للسلامة والأمن

التمييز التقليدي بين "السلامة" (Safety) و"الأمن" (Security) لم يعد ملائمًا في البيئة الرقمية الهجينة. التهديدات السيبرانية أصبحت قادرة على إحداث أضرار مادية، والحوادث التشغيلية قد تنتج عن اختراق معلوماتي. لذلك، تفرض الحوكمة الحديثة:

- **قيادة موحدة (Integrated Command):** تجمع بين فرق السلامة، الأمن المادي، الأمن السيبراني، والطوارئ التشغيلية ضمن مركز تنسيق واحد (مثل C4i Center)، يعمل وفق سياسات موحدة واتصالات لحظية.
- **هيكل تنظيمي متقاطع (Cross-Functional Governance):** يعتمد على فرق مختصة متعددة الخلفيات (أمنية، رقمية، فنية) تعمل وفق مصفوفة مسؤوليات متداخلة لضمان كفاءة الأداء وتكامل المعلومات.
- **منظومة تفويض واضحة:** تحدد من يملك القرار في الحالات التشغيلية الحرجة، مع خطط استمرارية أعمال مدمجة ضمن الإطار الأمني (Business Continuity within Security Doctrine).

هذا النموذج من القيادة الموحّدة يضمن سرعة الاستجابة وتقليص الفجوات التشغيلية عند وقوع الحوادث، ويُسهّل اتخاذ القرارات الحيوية المبنية على صورة تشغيلية مشتركة (Common Operational Picture).

2. رصد استباقي وتحليل التهديدات

المنظومات التقليدية تعمل بعد وقوع التهديد، بينما تعمل التوأمة الرقمية على **التنبيه المبكر والتصعيد الاستباقي** بناءً على نمذجة المخاطر. ولتحقيق ذلك، تشمل الحوكمة:

- **نظام استخبارات المخاطر (Threat Intelligence Engine):** يرتبط بمصادر داخلية وخارجية (مثل CERT الوطنية، ومراكز تحليل التهديدات الإقليمية) لرصد الأنماط التهديدية ومؤشرات الإنذار المبكر.
- **خريطة المخاطر التشغيلية (Operational Risk Map):** تُحدث لحظيًا ضمن التوأم الرقمي، بناءً على بيانات البيئة (الطقس، الكثافة، الأحداث الجارية) والأنظمة (مثل انقطاع أحد أجهزة الفحص أو تجاوز عتبة الزحام).
- **نماذج محاكاة التهديدات (Threat Simulation Scenarios):** تُستخدم للتدريب، واختبار الجاهزية، وتقييم قدرة المنظومة على التصدي للحوادث المركبة (مثل اندماج تهديد فيزيائي مع اختراق معلوماتي).
- **مصفوفة تصعيد استباقي (Proactive Escalation Matrix):** تُحدد فيها الإجراءات التي يتم تفعيلها تلقائيًا أو يدويًا عند رصد تهديدات محتملة، مع تدرج زمني وعملي في التصعيد.

الرصد الاستباقي لا يحمي فقط البنية التحتية، بل يرفع كفاءة التشغيل، ويقلل الخسائر، ويبني ثقة المستخدم في بيئة المطار.

3. استخدام تقنيات الذكاء الاصطناعي والرؤية الحاسوبية

الاعتماد على العنصر البشري وحده في الرصد لم يعد مجديًا في بيئة معقدة وواسعة كالبيئة المطارِية. ولهذا، تُدمج الحوكمة الرقمية للأمن والسلامة التشغيلية بأحدث تقنيات الذكاء الاصطناعي والرؤية الحاسوبية (Computer Vision)، وذلك عبر:

- **تحليل الفيديو الذكي (Intelligent Video Analytics):** لرصد السلوكيات غير المعتادة، مثل التجمعات غير المبررة، الأجسام المتروكة، أو الحركات العدائية.
- **نماذج التنبؤ السلوكي (Behavioral Prediction Models):** تعتمد على خوارزميات تعلّم الآلة، لتوقّع الأنماط غير الآمنة بناءً على التفاعل مع البوابات، الممرات، ومرافق الانتظار.
- **كشف الأنشطة الممنوعة (Anomaly Detection for Prohibited Acts):** مثل التدخين في مناطق محظورة، أو الدخول غير المصرح به عبر مخارج الطوارئ، باستخدام تقنيات رؤية حاسوبية مدربة على بيئة المطار الفعلية.
- **دمج الذكاء الاصطناعي مع IoT:** مثل ربط بيانات الكاميرات مع مستشعرات الحركة والصوت والحرارة، لتكوين صورة شاملة عالية الدقة تُعرض في التوأم الرقمي لحظيًا.

تخضع هذه الأنظمة لمراقبة أخلاقية وتنظيمية صارمة ضمن إطار الحوكمة، لضمان احترام الخصوصية، وتفادي التحيزات، والالتزام الكامل بمعايير SDAIA وISO.

خلاصة المحور

ليست حوكمة الأمن والسلامة التشغيلية مجرد التزام تنظيمي، بل هي أداة سيادية متقدمة تعكس مدى جاهزية الدولة في حماية أحد أهم أصولها الحيوية. وعبر التوأمة الرقمية، تنتقل هذه الحوكمة من الرد الفعلي إلى **الاستشراف الرقمي،** ومن المراقبة السلبية إلى **التحليل التنبؤي الذكي،** ومن التجزئة إلى **القيادة الموحدة عالية التكامل.** إنها منظومة لا تحمي فقط المطارات، بل تصنع مستقبلًا أكثر أمانًا وكفاءة.

📘 حوكمة الامتثال التنظيمي

تهدف هذه الحوكمة إلى ضمان التوافق الكامل مع القوانين واللوائح والمواصفات الفنية الوطنية والعالمية، من خلال إطار رقابي ذكي، قائم على المراقبة اللحظية، والتحليل الآلي، والتصحيح التلقائي، بما يتجاوز المفهوم التقليدي للتدقيق إلى منظومة مستمرة للتقييم والضبط.

1. تدقيق دوري للامتثال بناءً على معايير ISO وICAO

الحوكمة الفعالة تبدأ من الالتزام المستمر وليس الموسمي، ولهذا يجب أن تُبنى منظومة الامتثال على مراجعات منظمة وفق معايير دولية، تشمل:

- **ISO 27001:** لضمان التزام منظومة التوأم الرقمي بسياسات أمن المعلومات، وحماية الخصوصية، وضبط الوصول.
- **ISO 45001:** للتوافق مع أنظمة السلامة والصحة المهنية، لا سيما في المناطق التشغيلية الحساسة داخل المطار.
- **ICAO Annexes (خاصة Annex 17 & 19):** المتعلقة بالأمن، وإدارة السلامة التشغيلية، حيث تُلزم الدول الأعضاء بتنفيذ برامج وطنية رقابية صارمة (National Oversight Program).

ويجب أن تُنفذ عمليات التدقيق عبر:

- **جداول تدقيق مرنة (Rolling Audit Schedules):** مدمجة في التوأم الرقمي، تُحدَّث بناءً على مستوى الخطورة والامتثال السابق.
- **فرق امتثال رقمية (Digital Compliance Teams):** تستخدم أدوات تحليل قائمة على الذكاء الاصطناعي لرصد المخالفات وتتبع أنماط الخروج عن المعايير.
- **نماذج تقييم المخاطر المرتبطة بالامتثال (Compliance Risk Models):** تساعد في توجيه التدقيق إلى المناطق الحرجة والأكثر عرضة للمخاطر.

2. تقارير امتثال ذكية وتلقائية

التحول من التقارير اليدوية إلى تقارير ذكية وتلقائية يمثل نقلة جوهرية في حوكمة الامتثال. ويشمل ذلك:

- **تقارير لحظية قائمة على البيانات التشغيلية الحية:** تُولَّد تلقائيًا من التوأم الرقمي عند حصول حدث أو تجاوز معين (مثلاً: تجاوز عدد الركاب الحد المسموح به عند نقطة تفتيش دون تدقيق كافٍ).
- **مؤشرات امتثال ديناميكية (Dynamic Compliance KPIs):** مثل زمن معالجة المخالفات، عدد الحوادث غير المبلغ عنها، ونسبة استكمال خطط العمل التصحيحية (CAPs).

- **لوحات تحكم امتثال تنفيذية (Compliance Dashboards):** تُوفر للقيادة التنفيذية والمراقبين الخارجيين صورة لحظية عن الوضع التنظيمي، مع القدرة على تحليل الاتجاهات الزمنية.
- **قابلية التصدير والتكامل (Interoperable Compliance Reporting):** تُمكّن من إرسال التقارير مباشرة إلى أنظمة الجهات الرقابية كـ GACA وSDAIA، بما يتوافق مع بروتوكولات تبادل البيانات الآمنة.

3. آليات تصحيح لحظية للمخالفات

تكمن قوة الحوكمة الذكية في قدرتها على الاكتشاف والتصحيح دون تأخير. ولهذا، يجب أن تشمل المنظومة:

- **محركات قواعد الامتثال (Compliance Rule Engines):** تراقب البيانات الواردة من أنظمة التشغيل، وتفعّل تلقائيًا إجراءات تصحيحية عند رصد أي خرق.
- **سيناريوهات تصحيح آلي (Auto-Remediation Scenarios):** مثل إعادة تهيئة صلاحيات دخول أحد المستخدمين عند اكتشاف نشاط غير اعتيادي، أو إرسال إنذار تلقائي لفريق الأمن حال تخطي منطقة حظر.
- **خطط العمل الفورية (Instant Corrective Action Plans):** تُولد تلقائيًا من التوأم الرقمي، وتتوزع على الجهات المسؤولة مع تحديد المهام والمهل الزمنية.
- **حلقة تعلم مستمر (Continuous Compliance Learning Loop):** تقوم المنظومة بتحليل المخالفات المتكررة، وتُقترح تعديلات على السياسات أو التدريب أو إجراءات التشغيل.

هذه الآليات تعزز من قدرة المطار على الحفاظ على مستوى عالٍ من الامتثال، وتقليل الغرامات، وتعزيز الثقة لدى الشركاء المحليين والدوليين.

خلاصة المحور

ليست حوكمة الامتثال مجرد واجب رقابي، بل هي درع استراتيجي يضمن تشغيلًا آمنًا، مستدامًا، ومعتمدًا. وفي ظل التوأمة الرقمية، لم تعد الامتثال مسألة تقرير دوري، بل نظام عصبي لحظي يربط الأنظمة بالقوانين، ويوجه التشغيل بالمساءلة، ويمنح قادة المطار رؤية دقيقة تُلبي معايير ICAO، SDAIA، GACA، وISO في آنٍ واحد. إنه الامتثال الذكي، الحي، والمُمكَّن رقميًا.

📘 حوكمة الأداء والتحسين المستمر (Kaizen)

تُعرّف حوكمة الأداء والتحسين المستمر بأنها الإطار الذي يُمكِّن المنظمات من قياس نتائجها في الزمن الحقيقي، واكتشاف الانحرافات التشغيلية، وتفعيل آليات التعلم والإصلاح الفوري على مستوى النظام بأكمله. في بيئة "عين الصقر"، تتحول هذه الحوكمة إلى بنية تشغيلية تتنفس وتتعلم وتتطور مع كل لحظة تشغيلية.

1. مؤشرات أداء (KPIs) لحظية وشفافة

في بيئة رقمية متزامنة مثل التوأم الرقمي، تصبح مؤشرات الأداء التشغيلية أداة لاكتشاف الفُرص لا مجرد وسيلة للقياس. ويشمل ذلك:

- **لوحات مؤشرات تفاعلية لحظية (Live Dashboards):** مرتبطة مباشرة بالمصادر التشغيلية (مثل IoT، أنظمة AODB، بوابات الدخول)، وتُعرض بواجهات مرئية موجهة لكل مستوى إداري (التحكم الميداني، الإدارة الوسطى، القيادة العليا).
- **تصنيف ذكي للمؤشرات:**
  - مؤشرات الكفاءة (Efficiency KPIs): مثل متوسط زمن مرور الراكب عبر نقاط التفتيش، استهلاك الطاقة في المدرجات.
  - مؤشرات السلامة والأمان (Safety & Security KPIs): مثل عدد الإنذارات الحقيقية مقابل الإنذارات الكاذبة.
  - مؤشرات الامتثال والجودة (Compliance KPIs): مثل نسبة تطبيق إجراءات SOP دون تجاوز.
- **رؤية شفافة عبر المستويات:** حيث يمكن لكل فئة وظيفية رؤية مؤشرات أدائها الخاصة في الزمن الحقيقي، مما يعزز من **الملكية الفردية والجماعية للأداء**.
- **رصد الانحرافات تلقائيًا (Automated Deviation Detection):** تُنبه الفرق التشغيلية مباشرة حال حدوث أي تجاوز للقيم المستهدفة.

2. دورات مراجعة وتحسين وفقًا لنموذج 3M (Muda، Mura، Muri)

يُعد نموذج 3M أداة فعالة لتحليل جذور الهدر والاختلال في العمليات التشغيلية، ويُفعّل في بيئة التوأم الرقمي من خلال:

- **Muda (الهدر Waste):** مثل استخدام مفرط للطاقة أو الموارد البشرية في مواقع قليلة الحركة. يمكن رصده عبر تحليلات تدفق التشغيل والموارد.
- **Mura (التفاوت Irregularity):** مثل تفاوت أوقات الانتظار في نفس نقطة التفتيش بين ورديات مختلفة. يتم تحليله من خلال الربط بين بيانات الأداء وسجلات المناوبات.

- **Muri (التحميل الزائد Overburden):** كوجود ضغط تشغيلي زائد على منطقة أو طاقم معين، ويمكن كشفه بتحليل توزيع الأحمال مقابل قدرات الموارد.

تُستخدم خوارزميات تحليل العمليات داخل التوأم الرقمي لاكتشاف هذه الحالات تلقائيًا، وتُفعَّل اجتماعات مراجعة دورية بناء على نتائجها، يتم خلالها:

- **تحليل السبب الجذري (Root Cause Analysis)**
- **تصميم تدخلات تصحيحية**
- **اختبار أثر التحسين رقمياً قبل تنفيذه ميدانيًا (A/B Digital Simulation)**

3. ثقافة التعلّم والتحسين المستمر من أرض الميدان

التحسين المستمر لا يُفرض من الأعلى، بل يُبنى من "أرض الميدان" عبر تمكين العاملين ودمج ملاحظاتهم وتجاربهم، وتشمل الحوكمة في هذا الجانب:

- **منصة رقمية لتقديم مقترحات التحسين (Kaizen Digital Portal):** تمكّن كل موظف، من أصغر مشغل إلى قادة النوبات، من تسجيل أفكاره وتحدياته التشغيلية ومقترحات التحسين عبر التوأم الرقمي مباشرة.
- **نظام مكافآت معنوية ومادية:** لتحفيز ثقافة التحسين من القاعدة إلى القمة، مرتبط بمستوى تبنّي المقترحات ومدى تأثيرها التشغيلي أو المالي.
- **إدارة معرفة تشاركية (Collaborative Knowledge Base):** تُسجل فيها التجارب السابقة، ودروس التحسين، وقصص النجاح، وتُتاح كمراجع قابلة للبحث ضمن المنصة التشغيلية.
- **ورش عمل تحسينية دورية (Kaizen Blitz):** يتم تنظيمها رقميًا داخل التوأم لمحاكاة التغييرات المقترحة وتحليل أثرها، قبل تحويلها إلى مبادرات تنفيذية.

خلاصة المحور

في بيئة المطارات الذكية، لا يُقاس النجاح فقط بالتحكم في العمليات، بل بالقدرة على **التعلّم منها وتحسينها باستمرار**. ومع وجود التوأم الرقمي، لم تعد الحوكمة التحسينية نظرية أو مؤجلة، بل أصبحت حية ومُفعّلة لحظيًا. فهي تدير الأداء بالبيانات، وتستثمر العقول من أرض الميدان، وتبني ثقافة تشغيلية ترى في كل تحدٍّ فرصةً للتحسين، وفي كل لحظة تشغيلية درسًا للتحوّل.

📘 حوكمة الأمن السيبراني

تمثل حوكمة الأمن السيبراني الإطار المنهجي الذي يضمن أن كل مكون رقمي في منظومة التوأمة الرقمية—من أجهزة الاستشعار الطرفية إلى مراكز الذكاء الاصطناعي المركزية—يخضع لسياسات صارمة، وإجراءات دقيقة، واستجابات لحظية، تحميه من أي محاولة اختراق أو تعطيل أو تلاعب بالبيانات.

1. حماية البنية التحتية الرقمية من التهديدات

تشمل البنية التحتية الرقمية لمبادرة "عين الصقر" أنظمة حوسبة طرفية، شبكات الاتصالات، قواعد البيانات، التوأم الرقمي، والذكاء الاصطناعي، وكلها تعمل كمنظومة مترابطة، مما يجعل الحماية الأمنية مسألة شاملة غير قابلة للتجزئة. وتُبنى الحوكمة هنا على ركائز أساسية:

- **إطار الأمن السيبراني الوطني (NCA/NIST-Aligned):** يجب أن تتوافق كافة سياسات الحماية مع ضوابط الهيئة الوطنية للأمن السيبراني (NCA) ومعايير NIST، بما يشمل تحديد أصول المعلومات الحرجة، وتصنيف المخاطر، وتحديد مستويات الحماية المطلوبة.
- **مصفوفة طبقات الحماية (Defense-in-Depth):** تبدأ من حماية نقطة النهاية (End Points)، مرورًا بشبكات الاتصالات، ووصولًا إلى خوارزميات الذكاء الاصطناعي، ويُستخدم فيها تقنيات التشفير، والجدران النارية، ومراقبة التهديدات النشطة.
- **مبادئ "Zero Trust":** لا يُفترض الثقة بأي جهاز أو مستخدم داخل النظام دون تحقق مستمر، مع إدارة دقيقة للهوية (IAM)، وضوابط وصول قائمة على الدور والموقع والسياق.
- **تقييمات دورية للأمن السيبراني (Cybersecurity Maturity Assessments):** تُنفّذ بشكل نصف سنوي على كافة مكونات التوأم الرقمي لتقييم مستوى الحماية والنضج، وتحديد نقاط الضعف المحتملة.

2. استخدام Blockchain، SIEM، وشبكات مغلقة

تعتمد الحوكمة المتقدمة على بنية تقنية مرنة ولكن مؤمنة بعمق، وتُوظّف في ذلك مجموعة من الأدوات المتطورة:

- **أنظمة إدارة معلومات الأمن والأحداث (SIEM):** تقوم بجمع وتحليل السجلات من جميع الأنظمة، وتستخدم التحليلات السلوكية والذكاء الاصطناعي لاكتشاف التهديدات غير المعروفة مسبقًا، وربطها بسيناريوهات واقعية في التوأم الرقمي.
- **تقنيات البلوك تشين (Blockchain):** تُستخدم لحماية سلامة سجلات التشغيل والقرارات الحرجة، مثل توثيق توقيت واتجاه قرار إغلاق إحدى البوابات أو نقل الطائرة، مما يمنع التلاعب بالبيانات ويُوفر سجلًا شفافًا غير قابل للتزوير.

- **الشبكات المغلقة (Air-Gapped/Segmented Networks):** تُستخدم لعزل الأنظمة الحرجة (مثل أنظمة التحكم في المدرجات أو نقاط التفتيش الأمنية) عن الإنترنت، بما يمنع الهجمات الخارجية، ويدعم تشغيل آمن حتى في حال الانقطاع الكلي.
- **مراكز عمليات الأمن (SOC):** تعمل بالتكامل مع التوأم الرقمي لمتابعة التهديدات لحظيًا، وتُتيح إنشاء بيئة رقمية موازية لتحليل أي سلوك سيبراني مشبوه في بيئة اختبار قبل أن يؤثر على التشغيل الفعلي.

3. استجابة لحظية للتهديدات السيبرانية

تتحول الحوكمة من مجرد وقائية إلى استباقية وتفاعلية، من خلال بنية استجابة حية ومتكاملة، تشمل:

- **نظام استجابة تلقائي مدفوع بالذكاء الاصطناعي (AI-Driven Incident Response):** يُفعّل فور رصد تهديد حرج، فيقوم بعزل الأنظمة، إعادة ضبط الصلاحيات، أو تشغيل الوضع الآمن (Fail-Safe Mode) لحماية العمليات الحرجة.
- **تكامل مع التوأم الرقمي للتصعيد الفوري:** حال رصد حادثة سيبرانية في منطقة معينة (مثل اختراق قارئ بطاقة في إحدى البوابات)، يُظهر التوأم الرقمي الحادثة بصريًا، ويُفعّل مسارات الطوارئ تلقائيًا على مستوى التشغيل.
- **محاكاة دورية لهجمات سيبرانية (Cybersecurity Drills):** تُنفّذ عبر التوأم الرقمي لمحاكاة سيناريوهات معقدة (مثل هجمات رفض الخدمة الموزعة، أو اختراق خوارزمية الذكاء الاصطناعي)، واختبار الجاهزية البشرية والتقنية.
- **نظام استدعاء الأزمات السيبرانية (Cyber-Contingency Plan):** يحدد آليات الإبلاغ، والتصعيد، والتواصل مع الجهات الوطنية المختصة مثل NCA، خلال الدقائق الأولى من وقوع التهديد.

خلاصة المحور

إن حوكمة الأمن السيبراني في بيئة التوأمة الرقمية لا تُبنى على فرضية "عدم التعرض للهجمات"، بل على يقين أنها ستحدث، وأن منظومتنا قادرة على **الكشف، والاحتواء، والتعافي** بسرعة وفعالية. وفي ظل بيئة تشغيلية مترابطة كقطاع الطيران، تصبح هذه الحوكمة أداة سيادية لحماية البيانات، وضمان سلامة الركاب، وتعزيز الثقة المحلية والدولية في بنية المطارات الذكية.

📘 حوكمة الشفافية والتقارير

تهدف هذه الحوكمة إلى إرساء منظومة تقريرية تعتمد على البيانات الحية، مدعومة بالتحليلات التنبؤية والبصرية، لتكون التقارير جزءًا من عملية اتخاذ القرار لا مجرد ناتج لاحق لها. وتتمحور هذه الحوكمة حول ثلاثة محاور استراتيجية:

1. تقارير لحظية موجهة لصنّاع القرار

صناعة القرار في بيئة طيران معقدة تتطلب الوصول إلى البيانات لا عندما تُطلب، بل عندما تحدث. ولذلك تُبنى حوكمة التقارير على:

- **نظام تقارير لحظي مدمج بالتوأم الرقمي:** حيث تُجمع البيانات مباشرة من المصادر التشغيلية (مثل بوابات الركاب، الأنظمة الأمنية، الطاقة، الطقس)، وتُحلل بشكل آلي، وتُرسل إلى الجهات المعنية خلال ثوانٍ من الحدث.
- **تقارير تنفيذية تفاعلية (Executive Briefings):** مصممة خصيصًا لكبار المسؤولين في هيئة الطيران المدني وقيادات المطارات، تتضمن ملخصات مرئية لحالة الأداء، أبرز الانحرافات، والقرارات المقترحة.
- **تقارير ظرفية فورية (Event-Based Reporting):** تُطلق تلقائيًا حال وقوع حدث غير اعتيادي، مثل تأخير جماعي في الرحلات أو اختراق أمني، وتشمل تحليلًا أوليًا للأسباب والتوصيات الآنية.
- **تكامل مع أنظمة إدارة القرار (Decision Support Systems):** بحيث تُدمج التقارير مباشرة في منصة دعم القرار، مع القدرة على اختبار "السيناريوهات البديلة" بناءً على البيانات الفعلية.

2. ربط مؤشرات الأداء باللوحات القيادية

لتحقيق الشفافية المؤسسية الفعّالة، لا بد من **تحويل البيانات إلى مؤشرات، والمؤشرات إلى قرارات**، من خلال:

- **لوحات تحكم قيادية (Strategic Command Dashboards):** تُخصص للمستويات العليا من الإدارة، وتتضمن عرضًا مرئيًا للمؤشرات الاستراتيجية في السلامة، الكفاءة، الأمن، والرضا، مع تحليل سياقي للتغيرات.
- **مؤشرات تنبؤية وتاريخية مدمجة:** تُظهر الأداء السابق مقابل التوقعات المستقبلية، بناءً على تحليل التوجهات والسياقات التشغيلية الموسمية أو الطارئة.
- **ربط المؤشرات بالأهداف الوطنية (Vision 2030 Alignment):** بحيث تُعرض مؤشرات الأداء الرئيسية (KPIs) ضمن سياق مساهمتها في تحقيق مستهدفات رؤية المملكة، مثل تحسين تجربة المسافر، ورفع كفاءة استغلال البنية التحتية.

- **نظام إشارات تنبيهية (Signal Indicators):** يحدد تلقائيًا المؤشرات التي تحتاج إلى تدخل تنفيذي، مع تصنيفها حسب الأولوية والسبب الجذري.

3. مشاركة عامة ومفتوحة للمؤشرات غير الحساسة

الشفافية لا تُبنى فقط داخل المؤسسة، بل أيضًا مع جمهورها الخارجي من شركاء، مسافرين، ومجتمع. وتشمل الحوكمة:

- **بوابة شفافية عامة (Public Transparency Portal):** تنشر مؤشرات الأداء غير الحساسة، مثل: دقة مواعيد الرحلات، زمن الانتظار في نقاط التفتيش، كفاءة استهلاك الطاقة.
- **تقارير دورية للمجتمع:** تُنشر عبر الموقع الإلكتروني أو تقارير الربع السنوي، تعكس فيها المبادرة التزامها بالتحسين المستمر، وتأثير مشاريعها التقنية على جودة الخدمة والسلامة.
- **واجهة برمجية مفتوحة (Open Data APIs):** تتيح للباحثين والشركات الناشئة الوصول الآمن إلى مجموعات بيانات معينة لتطوير حلول مبتكرة، مما يُفعّل مفهوم الاقتصاد الرقمي المعتمد على البيانات.
- **سياسات وضوابط مشاركة البيانات:** تُنظم ما يجوز نشره، وتحدد نطاق المسؤولية، وطرق التحقق، بما يضمن التوازن بين الشفافية وحماية الأمن السيبراني وخصوصية المستخدم.

خلاصة المحور

إن حوكمة الشفافية والتقارير ليست ترفًا تنظيميًا، بل عنصر حيوي لبناء بيئة تشغيلية ناضجة، مسؤولة، وتستجيب للمساءلة بالبيانات لا بالتبريرات. وفي ظل التوأمة الرقمية، تتحوّل التقارير إلى أعصاب رقمية تربط القادة بالحقيقة التشغيلية، وتربط المجتمع بثقة راسخة في أداء مؤسسات الطيران. تلك هي الشفافية الذكية... التي لا تُظهر كل شيء، بل تُظهر ما يجب، لمن يجب، في الوقت الذي يجب.

📘 حوكمة العلاقة مع المستفيد النهائي

تهدف هذه الحوكمة إلى مواءمة تصميم وتطوير وتشغيل منظومة التوأمة الرقمية مع متطلبات المستخدم الحقيقي، وتحقيق التوازن بين الكفاءة الرقمية وتجربة الاستخدام، من خلال استراتيجيات قائمة على **التصميم المتمركز حول الإنسان (Human-Centered Design)**، والتفاعل المستمر، والتمكين الشامل.

1. تصميم الحلول وفقًا لاحتياجات المسافرين والمشغلين والمراقبين

لكل فئة من المستخدمين أهداف مختلفة وسياقات تشغيلية متنوعة، ولهذا يجب أن تُبنى الحلول الرقمية ضمن بيئة "عين الصقر" بناءً على نماذج الاستخدام الواقعية، عبر:

- **تحليل رحلات المستخدم (User Journey Mapping):** رصد دقيق لكافة نقاط التفاعل بين المستخدم والنظام الرقمي، بدءًا من الحجز وحتى استلام الأمتعة، أو من دخول المشغل إلى نظام المراقبة وحتى تنفيذ التدخل التشغيلي.
- **تخصيص واجهات الاستخدام (UX Personalization):** تصميم واجهات مختلفة حسب نوع المستخدم (مسافر – موظف أمن – مراقب برج – مشغل خدمات أرضية)، مع مراعاة اللغات، وبيئة العمل، ودرجة الإلمام التقني.
- **اختبارات صلاحية الاستخدام الميدانية (Usability Field Tests):** تجارب مباشرة في بيئات تشغيلية حقيقية داخل المطارات لضمان أن الحلول الرقمية لا تعرقل، بل تسهّل العمليات وتُسرّع اتخاذ القرار.
- **التكامل مع الأجهزة المساعدة:** مثل دعم أنظمة المطار لتقنيات الوصول لذوي الإعاقة، من خلال التوأم الرقمي، عبر إشعارات صوتية، أو مسارات ذكية موجهة.

2. إشراك المستخدم في ملاحظات التحسين

المنظومات الذكية لا تتحسن فقط عبر التحليل الخوارزمي، بل من خلال **الصوت الإنساني** الذي يواجه التحديات مباشرة، ولهذا تُبنى آليات الحوكمة على:

- **قنوات تغذية راجعة متعددة (Feedback Channels):** تتضمن أجهزة ميدانية، تطبيقات الهاتف، وأدوات تقييم رقمية داخل النظام، تُتيح للمستخدم التعبير عن تجربته خلال أو بعد التفاعل.
- **تحليل انطباعات المستخدم (Sentiment & Behavioral Analytics):** استخدام تقنيات تحليل اللغة الطبيعية (NLP) لفهم نوعية الملاحظات (شكاوى، مقترحات، إشادة)، وربطها بالسياق التشغيلي الذي حدثت فيه.

- **مشاركة المستخدم في تصميم الحلول (Co-Creation Workshops):** إشراك ممثلين حقيقيين عن المسافرين والمشغلين في جلسات تطوير وتحسين المنصة الرقمية، مما يعزز القبول ويوفر رؤى واقعية عميقة.
- **استراتيجية التغذية المرتدة المغلقة (Closed Feedback Loop):** حيث يتم إعلام المستخدم بما حدث فعليًا بناءً على ملاحظته، مما يعزز ثقته ويحفز على التفاعل المستمر.

3. ضمان تجربة سلسة وآمنة وشفافة للمستخدم النهائي

الهدف النهائي هو تمكين كل مستفيد من **الوصول السلس للمعلومة، التنقل الذكي في البيئة، واتخاذ القرار بثقة**، ويتحقق ذلك من خلال:

- **الشفافية المعلوماتية (Operational Transparency):** مثل توفير وقت الانتظار المتوقع، حالة الرحلة، أو إشعارات التأخير، في الزمن الحقيقي.
- **الحماية السيبرانية الصديقة للمستخدم (User-Centric Security):** حيث تُصمم سياسات الأمان بطريقة لا تعرقل الاستخدام، مثل التحقق الحيوي الذكي عند البوابات دون لمس أو انتظار طويل.
- **مؤشرات تجربة المستخدم (UX KPIs):** مثل معدل رضا المستخدم، زمن التفاعل، نسبة الأعطال المُبلغ عنها، وتُدمج في لوحة القيادة التشغيلية للمراقبة اليومية.
- **المواءمة مع معايير الجودة العالمية (مثل ISO 9241):** لضمان أن التصميمات الرقمية لا تتعارض مع المبادئ العلمية لاستخدام الأنظمة البشرية.

خلاصة المحور

حوكمة العلاقة مع المستفيد النهائي ليست واجهة ناعمة للتقنية، بل هي ضمانة لتفعيلها الحقيقي على أرض الواقع. فهي تحول النظام من مجرد بنية معلوماتية إلى منظومة **متمحورة حول الإنسان**—تفهمه، تتفاعل معه، وتستجيب له. في مطارات تعتمد على التوأمة الرقمية، فإن المسافر الآمن، والمشغل الممكّن، والمراقب الواثق... هم جميعًا دعامات نجاح المنظومة، ومركز ثقل الحوكمة الرقمية المسؤولة.

📘 حوكمة الابتكار والتحول الرقمي

تهدف هذه الحوكمة إلى تحويل المبادرات الابتكارية من أفكار منعزلة إلى عمليات مؤسسية ممنهجة، تُدمج في صُلب التشغيل اليومي، وتُدار بمعايير حوكمة ذكية توازن بين **المخاطرة المحسوبة** والانضباط التشغيلي، مما يسمح بإطلاق إمكانات التوأم الرقمي على نحو استباقي ومستدام.

1. تسريع الابتكار من خلال الحوكمة الذكية

في النماذج التقليدية، كانت الحوكمة تُنظر إليها كعنصر يبطئ الابتكار. أما في هذا الإطار، فالحوكمة الذكية تتحوّل إلى محفّز للابتكار من خلال:

- **سياسات ابتكار مرنة (Adaptive Governance Policies):** تتيح مساحة آمنة للتجريب، دون التضحية بالامتثال، عبر نماذج ترخيص مرحلي (Stage-Gated Innovation) توازن بين الحماس التقني والسلامة التشغيلية.
- **بوابة الابتكار المؤسسية (Innovation Portal):** منصة داخلية مفتوحة تتيح للعاملين والشركاء رفع الأفكار، متابعة تقييمها، وقياس أثرها، ضمن دورة حوكمة واضحة.
- **حوكمة التمويل الابتكاري (Innovation Budget Governance):** تُخصص ميزانيات مجزأة للتجريب، تُصرف على مراحل وفق مؤشرات أداء الابتكار (Innovation KPIs) بدلاً من مؤشرات التشغيل التقليدية.
- **إدارة المحافظ الابتكارية (Innovation Portfolio Management):** تُدار كمحافظ مشاريع استثمارية، ويتم تقييم جدواها باستمرار ضمن بيئة التوأمة الرقمية، مما يسهل وقف الأفكار غير المجدية وتوسيع المجدية منها.

2. بناء بيئة مرنة قابلة للتجريب والاختبار

لا يمكن للتحول الرقمي أن يُقلِّد النماذج القديمة، بل يتطلب بيئة تشغيلية **قابلة للفشل الذكي** والتجريب السريع، ويشمل ذلك:

- **مناطق الاختبار الرقمي (Digital Sandboxes):** بيئات معزولة عن التشغيل الفعلي، يمكن فيها تجربة حلول مبتكرة أو خوارزميات ذكاء اصطناعي دون التأثير على الأنظمة الحية.
- **التوأم التجريبي (Pilot Digital Twin):** نسخة موازية غير حرجة من التوأم الرقمي تُستخدم لاختبار سيناريوهات جديدة، مثل تعديل تدفق الركاب أو إدخال خوارزميات تحسين أمني.
- **أطر حوكمة تجريبية (Experimental Governance Frameworks):** تُستخدم لتسريع اختبار النماذج الأولية، وتُحدّد فيها معايير السلامة، وآليات المصادقة، واشتراطات الخروج أو التوسّع.

- **دورات تطوير سريعة (Agile & Lean Experimentation):** ترتكز على التنفيذ السريع (Sprint-Based Pilots)، وتحليل النتائج ضمن دورة زمنية قصيرة، مع مراجعة فورية للجدوى.

3. ربط الحوكمة بمنهجيات التصميم والابتكار الميداني

الابتكار الحقيقي لا يولد في قاعات الاجتماعات، بل في مواقع التشغيل، ومن هذا المنطلق، تركّز الحوكمة على:

- **منهجيات التصميم التشاركي (Participatory Design):** إشراك المستخدمين النهائيين في تصميم الحلول من البداية، لضمان ملاءمتها للسياق الحقيقي، وتعزيز التبنّي التشغيلي.
- **التكامل مع نماذج التفكير التصميمي (Design Thinking):** حيث تمر الأفكار بمراحل "الفهم – التحديد – التخيّل – النموذج – الاختبار"، وتُدار ضمن آليات حوكمة خفيفة تحفّز السرعة دون التضحية بالموثوقية.
- **منصات الأفكار المفتوحة (Open Innovation Platforms):** تُتيح إشراك مزودي التقنية، الجامعات، والشركات الناشئة في تطوير الحلول داخل بيئة مؤمنة ومراقبة، مما يعزز التنوع والمرونة.
- **دمج الابتكار ضمن الأداء المؤسسي:** تُصبح مؤشرات "التحسين، والاختبار، والتبني" جزءًا من مؤشرات الأداء الرسمية للفرق، مما يجعل الابتكار مسؤولية جماعية لا مبادرات فردية.

خلاصة المحور

حوكمة الابتكار ليست مسألة تنظيمية، بل **محرّك استراتيجي** يُمكّن منظومة التوأمة الرقمية من التكيّف، النمو، والقيادة. وهي تضمن أن تظل مبادرة "عين الصقر" في حالة تطور مستمر، قادرة على مواجهة التعقيدات المستقبلية من خلال الابتكار الميداني، والحوكمة الرشيقة، والعقلية التجريبية. وبهذا، يتحوّل الابتكار من نشاط جانبي إلى **ثقافة تشغيلية** محكومة، مرنة، ومستدامة.

📘 11. حوكمة دورة حياة التوأم الرقمي (Digital Twin Lifecycle Governance)

في سياق بيئة تشغيلية حيوية كقطاع الطيران، فإن التوأم الرقمي لا يُعد منتجًا نهائيًا جامدًا، بل هو **كائن رقمي ديناميكي يتطور ويتفاعل** باستمرار مع واقعه الفيزيائي، ويعيد تشكيل قرارات التشغيل والصيانة والسلامة. من هنا، لا تقتصر الحوكمة على مراقبة أداء التوأم الرقمي بعد إطلاقه، بل يجب أن تمتد لتغطي **كامل دورة حياته** من الفكرة وحتى الإحلال، بما يضمن دقة النماذج، موثوقية البيانات، واستدامة القيمة.

1. حوكمة الإنشاء والاعتماد (Origination & Validation)

تنطلق دورة حياة التوأم الرقمي من لحظة تصميمه الأولي وجمع بياناته. وهنا تبرز أهمية الحوكمة في ضبط جودة المدخلات وبناء النموذج الرقمي على أسس واقعية:

- **معايير صارمة لجمع البيانات (Data Acquisition Protocols):** تُفرض مواصفات دقيقة لجمع البيانات الهندسية والتشغيلية من مصادر متعددة مثل: تقنيات LiDAR، حساسات إنترنت الأشياء (IoT)، أنظمة التحكم الصناعية (SCADA)، وغيرها. تُحدّد دقة البيانات المكانية، تكرار التحديث، ونسب الخطأ المقبولة.
- **مصداقية النموذج (Model Fidelity Assurance):** تُطبّق اختبارات لتقييم مدى تطابق النموذج الرقمي مع الأصل الفيزيائي، بما يشمل التكوين الهيكلي، تدفقات الحركة، وتوزيع الأحمال.
- **آليات التحقق والمصادقة (Validation & Verification):** يُنشأ مسار مزدوج لفحص النموذج قبل اعتماده:
  - **التحقق (Verification):** يضمن أن النموذج بُني بالشكل الصحيح (Does the system do what we think it does؟).
  - **المصادقة (Validation):** تضمن أن النموذج يعكس الواقع بدقة (Does the system do what the user needs؟).
- **اعتمادية النماذج قبل الإنتاج (Pre-Deployment Certification):** لا يُطلق أي توأم رقمي (أو تحديث جوهري عليه) دون اجتيازه لمستوى اعتماد حوكمي موثق، يتضمن مراجعة من لجنة فنية مستقلة.

2. حوكمة التشغيل والمزامنة (Operation & Synchronization)

بعد إطلاق التوأم الرقمي، تتحول الحوكمة إلى دور ديناميكي يضمن أن يبقى النموذج متصلًا بالواقع:

- **بروتوكولات المزامنة اللحظية (Real-Time Synchronization Protocols):** تُحدد آليات الدمج الفوري بين بيانات الأصل الفيزيائي والتوأم الرقمي عبر واجهات API مؤمنة، مع مراقبة جودة الاتصال ودرجة التحديث اللحظي.
- **مصفوفة الانحرافات المسموحة (Deviation Threshold Matrix):** تُحدد نسب الانحراف المقبولة بين ما يعكسه التوأم الرقمي وما يحدث فعليًا على الأرض (مثلاً، فرق زمني 3 ثوانٍ، انحراف في تدفق الحركة بنسبة 2%). أي تجاوز يُفعّل تنبيهات آلية ويُوجّه لإعادة المعايرة.
- **نظام تتبّع الأحداث الحاسمة (Critical Events Logging):** يتم تسجيل كل تغيير جوهري يحدث في الأصل المادي (توسعة، إغلاق بوابة، صيانة غير مجدولة) ويُعاد إسقاطه فورًا على التوأم مع توثيق رقمي كامل.

3. حوكمة التقادم والإحلال (Decommissioning & Replacement)

كل نموذج رقمي، مهما بلغت دقته، يصبح عرضة للتقادم نتيجة التغييرات الهيكلية أو التكنولوجية، ولذا تضمن الحوكمة ما يلي:

- **سياسات إحلال مبنية على الأحداث (Event-Driven Decommissioning):** لا يُسمح باستخدام نموذج توأمي تجاوزت دقته أو صلاحيته التشغيلية الحد الأدنى المحدد، ويتم استبداله تلقائيًا أو ترقيته عبر دورة تجديد حوكمي معتمدة.
- **إجراءات أرشفة آمنة (Secure Archiving):** تُنقل النسخ القديمة إلى مستودعات رقمية مؤمنة مع تسجيل كافة تفاصيل الاستخدام، قرارات الاعتماد، والسجلات التشغيلية، للحفاظ على الشفافية والتحليل المستقبلي.
- **تحليل أثر التغيير (Change Impact Analysis):** قبل سحب أي نسخة من الخدمة، يُنفّذ تحليل دقيق لتأثيرها على العمليات المرتبطة، ويُوضع جدول زمني للانتقال السلس دون تعطل.

🔍 خلاصة المحور

دورة حياة التوأم الرقمي ليست سلسلة خطية، بل **حلقة مغلقة من الاعتماد، التشغيل، والمراجعة المستمرة**. وعليه، فإن حوكمة هذه الدورة تضمن أن يظل التوأم الرقمي مرآة حية ودقيقة للواقع، وليس مجرد نسخة جامدة. في بيئة كقطاع الطيران، حيث القرارات تُتخذ في ثوانٍ وتؤثر على حياة الآلاف، تصبح **الحوكمة الدائرية للتوأم الرقمي** هي الضامن الأعلى للدقة، السلامة، والكفاءة التشغيلية.

12. حوكمة نماذج الذكاء الاصطناعي والخوارزميات (AI & Algorithm Governance / ModelOps)

في منظومات التوأمة الرقمية المتقدمة، يشكّل الذكاء الاصطناعي ليس فقط أداة تحليل، بل "العقل الفاعل" الذي يقود القرارات، ويوجّه الموارد، ويتنبأ بالمخاطر. ولكن كلما ازداد الاعتماد على الذكاء الاصطناعي، ازداد معه خطر الخطأ أو الانحراف أو التحيّز. من هنا، تُعد **حوكمة نماذج الذكاء الاصطناعي والخوارزميات (ModelOps Governance)** من أعمدة الحوكمة الرقمية المتقدمة، لما لها من دور في ضمان أن هذه النماذج لا تعمل فقط بكفاءة، بل تعمل أيضًا بعدالة، شفافية، ومسؤولية.

1. التحقق من صحة النماذج (Model Validation)

تبدأ الحوكمة من لحظة إنشاء النموذج، حيث يُشترط وجود آليات مستقلة تُراجع وتُقيّم النموذج قبل إدخاله في بيئة تشغيلية حقيقية:

- **اختبار الدقة التنبؤية (Predictive Accuracy):** تُستخدم مجموعات بيانات مستقلة لاختبار أداء النموذج خارج نطاق تدريبه، مع مقارنة نتائجه ببيانات الواقع التشغيلي.
- **تحليل الحساسية (Sensitivity Testing):** تقييم مدى تأثر النموذج بالتغيرات الطفيفة في المدخلات؛ لضمان الثبات والاستقرار.
- **اعتماد النماذج (Model Certification):** لا يُسمح باستخدام أي نموذج ذكاء اصطناعي في بيئة حساسة (كالأمن والسلامة) ما لم يجتز إجراءات اعتماد صارمة توثق قدراته وحدوده.
- **فصل تطوير النموذج عن اعتماده (Separation of Duties):** الجهة التي تطور النموذج لا تملك صلاحية اعتماده؛ ما يرسّخ الحيادية ويمنع تضارب المصالح.

2. رصد الانحراف والتحيز (Drift & Bias Monitoring)

مع مرور الوقت، تتغير الأنماط والسلوكيات، مما يجعل النموذج عرضة للانحراف أو التحيّز، وهنا تأتي أهمية:

- **رصد الانحراف الزمني (Model Drift Detection):** مراقبة دورية لأداء النموذج في الميدان مقارنةً بأدائه في وقت التدريب، مع آليات تنبيه فوري عند تراجع مستوى الدقة.
- **اكتشاف التحيّزات السلوكية (Bias Auditing):** تحليل قرارات النموذج للتحقق من غياب التحيزات تجاه فئة معينة (مثل جنسية، عمر، نمط سفر...)، خصوصًا في الأنظمة التنبؤية المرتبطة بالأمن أو تخصيص الموارد.
- **خوارزميات التصحيح الذاتي (Self-Correcting Models):** يُفضّل استخدام نماذج ديناميكية قادرة على التكيف التدريجي (Online Learning)، بشرط ضبطها بحدود تمنع الانحراف غير المرغوب.
- **إدارة الأخطار الخوارزمية (Algorithmic Risk Management):** إدراج مؤشرات المخاطر الخوارزمية ضمن لوحات القيادة التنفيذية.

3. قابلية التفسير والشفافية (Explainability - XAI)

في بيئات حساسة مثل المطارات، **لا يُكتفى بأن يتخذ الذكاء الاصطناعي قرارًا صحيحًا، بل يجب أن يُشرح سبب هذا القرار:**

- **تفسير الخوارزميات المعقّدة (Explainability Layer):** استخدام أدوات تفسير مثل SHAP أو LIME لتوضيح ما الذي دفع النموذج لاتخاذ قرار معين (مثل تصنيف راكب كمشتبه به، أو اقتراح تغيير في خطة التشغيل).

- **نماذج تفسيريّة افتراضيًا (XAI by Design):** يُفضّل في البيئات عالية التأثير استخدام نماذج قابلة للتفسير بطبيعتها (مثل الأشجار العشوائية) على النماذج الصندوقية المغلقة (Black-Box Models).
- **إلزامية التوثيق التفسيري:** كل قرار يصدر عن الذكاء الاصطناعي في السياقات الحرجة يجب أن يكون مصحوبًا بتفسير قابل للتدقيق والمراجعة لاحقًا.

4. سجل الخوارزميات (Algorithm Registry)

كما تُسجّل الطائرات والصيانة والبيانات التشغيلية، يجب أيضًا **تسجيل الخوارزميات بوصفها أصولًا تشغيلية**:

- **سجل مركزي محدث (Central Algorithm Registry):** يحتوي على جميع النماذج المعتمدة، مع تفاصيل مثل الإصدار، تاريخ التدريب، نوع البيانات، مستوى الأداء، وحدود الاستخدام.
- **تتبع الأثر (Traceability):** القدرة على تتبع كل قرار خوارزمي إلى النموذج الذي صدر عنه، وبياناته التدريبية، ونسخته المحددة.
- **توثيق التحديثات الخوارزمية (Change Log):** يُسجل كل تحديث طرأ على نموذج ما، سواء في المعمارية، أو البيانات، أو الأوزان، مع أسباب التعديل.
- **ضبط صلاحيات الاستخدام:** لا يجوز لأي جهة تشغيل خوارزمية دون صلاحية حوكميّة واضحة، تمنحها بناءً على نوع الاستخدام ومستوى الخطورة.

✅ خلاصة المحور

حوكمة الذكاء الاصطناعي لا تتمثل في كبح الابتكار، بل في **تمكين الذكاء الاصطناعي المسؤول، العادل، والمُبرر**. ففي بيئة تعتمد فيها سلامة الملاحة الجوية وأمن المسافرين على قرارات آلية متسارعة، لا بد من أن تكون تلك القرارات دقيقة، خاضعة للمراجعة، ويمكن تفسيرها عند الحاجة. ومن خلال هذا المحور، يتم بناء جسر من الثقة بين العقل الخوارزمي وصاحب القرار البشري، ما يُشكّل الأساس لتحوّل رقمي موثوق ومستدام.

13. الإطار الأخلاقي والمسؤولية المجتمعية (Ethical & Societal Responsibility Framework)

في عصر تتسارع فيه تقنيات الذكاء الاصطناعي والتوأمة الرقمية، تصبح الثقة العامة حجر الزاوية لنجاح أي منظومة رقمية. فلا قيمة لأدق النماذج الحسابية أو لأحدث أنظمة المراقبة إذا افتقرت إلى **إطار أخلاقي راسخ** يضمن الاستخدام العادل، الشفاف، والمسؤول للتقنية. من هنا تأتي أهمية هذا المحور بوصفه **درعًا واقيًا للقيم الإنسانية** في قلب التحول الرقمي، وأحد المكونات الجوهرية للحوكمة الرقمية الرشيدة في قطاع حساس كقطاع الطيران.

1. مبادئ الاستخدام الأخلاقي للبيانات

تبدأ الحوكمة الأخلاقية من وضع **ميثاق واضح لاستخدام البيانات**، يُراعي خصوصية الأفراد، ويحترم الحريات، ويرتكز على الشفافية والمساءلة:

- **ضوابط جمع البيانات البيومترية والسلوكية:** يُحظر جمع أي نوع من هذه البيانات دون غرض مشروع واضح، وموافقة مستنيرة (Informed Consent)، وضمان أمني صارم لحمايتها من التسرب أو إساءة الاستخدام.
- **منع التمييز في المعالجة (Non-Discrimination):** يجب أن تُصمم الخوارزميات بحيث لا تؤدي إلى قرارات متحيزة ضد فئات معينة (بناءً على الجنسية، العمر، الجنس، الخلفية الاجتماعية...).
- **الحدود القانونية والأخلاقية (Ethical Boundaries):** تُحدّد بدقة الحالات المسموح بها قانونًا وأخلاقيًا لاستخدام بيانات الحركة والسلوك، كجزء من منظومة تحليل المخاطر، مع توفير بدائل غير شخصية متى أمكن.
- **مبدأ "الخصوصية منذ التصميم" (Privacy by Design):** يُدمج احترام الخصوصية كعنصر أساسي في تصميم الأنظمة من بدايتها، وليس كإضافة لاحقة.

2. لجنة المراجعة الأخلاقية (Ethics Review Board)

الحوكمة الأخلاقية لا يمكن أن تُترك لقرارات فردية أو ممارسات غير خاضعة للمساءلة. لذا، يُشكّل هذا الإطار لجنة مستقلة تُراجع القرارات ذات الأثر المجتمعي العالي:

- **تكوين متعدد التخصصات:** تضم اللجنة خبراء في القانون، علم الاجتماع، علم النفس، تقنيات الذكاء الاصطناعي، الأمن السيبراني، وحماية الخصوصية.
- **صلاحيات المراجعة والتعليق:** تملك اللجنة صلاحية رفض أو تعديل أي تطبيق رقمي يتجاوز الحدود الأخلاقية أو يتسبب في ضرر اجتماعي غير مبرر، حتى وإن كان قانونيًا في ظاهره.

- **آلية مراجعة دورية:** لا تُراجع اللجنة الحالات الجديدة فقط، بل تجري مراجعات دورية على التطبيقات الرقمية الجارية لضمان استمرار توافقها مع المبادئ الأخلاقية المعتمدة.
- **الشفافية في أعمال اللجنة:** تُنشر تقارير دورية تلخص قرارات اللجنة ومبرراتها دون الإخلال بالسرية، ما يعزز الثقة المجتمعية.

3. حوكمة القرارات المستقلة (Autonomous Decision Governance)

مع تزايد الاعتماد على الأنظمة المؤتمتة، تظهر الحاجة إلى **ضوابط دقيقة تحدد متى وكيف يمكن للنظام أن يتخذ قرارات مستقلة دون تدخل بشري**:

- **تصنيف مستويات الاستقلالية:** يتم تصنيف كل نظام أو خوارزمية حسب قدرتها على اتخاذ القرار، مع تعريف مستويات "التحكم البشري" المطلوبة (مثلاً: إشراف كامل، إشراف جزئي، استقلالية كاملة في ظروف طارئة فقط).
- **قيود على القرارات الحساسة:** يُمنع على أي نظام آلي اتخاذ قرارات تؤثر على الحقوق الفردية (مثل منع صعود الراكب، أو إرسال إشعار أمني) دون تحقق بشري منطقّي، إلا في حالات طوارئ محددة وموثقة.
- **سجلات القرار الآلي (Decision Logs):** يتم تسجيل كل قرار مستقل يتخذه النظام، مع المعطيات التي بُني عليها، وتُراجع هذه السجلات دوريًا للتأكد من توافقها مع القيم المؤسسية والأخلاقية.
- **نظام الاستئناف البشري (Human Appeal Mechanism):** يُمنح المستفيد (راكب، موظف، طرف ثالث) حق الاعتراض على قرار آلي والمطالبة بمراجعة بشرية محايدة.

✅ خلاصة المحور

الإطار الأخلاقي ليس ترفًا تنظيميًا، بل هو **الضمان الأعمق لاستدامة الثقة** في الأنظمة الذكية. وهو ما يضمن أن يبقى التقدم الرقمي خادمًا للإنسان لا متحكمًا فيه، ويحول التقنية من أداة مراقبة إلى أداة تمكين. ومن خلال هذا المحور، يتم ترسيخ مبادئ "الحوكمة المسؤولة" التي توازن بين كفاءة الأداء وكرامة الإنسان، وبين الذكاء الخوارزمي وحكمة البشر.

📘 14. حوكمة المرونة والاستجابة للأزمات السيبرانية-المادية

(Cyber-Physical Resilience Governance)

في بيئة رقمية متصلة ومعتمدة كليًا على التوأمة الرقمية والأنظمة الذكية، لم تعد التهديدات السيبرانية وحدها مصدر القلق؛ بل نشأت فئة جديدة من المخاطر تعرف بـ **التهديدات السيبرانية-المادية (Cyber-Physical Threats)**، حيث يمتد الأثر السيبراني مباشرة إلى البنى التحتية الفيزيائية — كأن يؤدي تلاعب في نموذج

رقمي إلى تعطيل حركة المسافرين، أو إلى تعطيل نظام الإنذار المبكر. لهذا السبب، يتطلب ضمان **المرونة السيبرانية-المادية** حوكمة متقدمة ومتكاملة، تمتد عبر التخطيط، والرصد، والمحاكاة، والتعافي.

1. بروتوكولات الوضع الآمن (Fail-Safe Protocols)

لا يكفي إعداد الأنظمة للتشغيل في الظروف المثالية فقط، بل يجب تصميمها بحيث **تفشل بأمان** (Fail-Safe) عند مواجهة أعطال حرجة أو فقدان الاتصال:

- **تحديد حالات الفشل الحرجة:** تُصنف السيناريوهات التي تستدعي تفعيل "الوضع الآمن" مسبقًا، مثل فقد الاتصال بالتوأم الرقمي، أو انحراف جوهري في البيانات الحية، أو التناقض بين الواقع الرقمي والميداني.
- **التحوّل التلقائي إلى الوضع الآمن:** الأنظمة يجب أن تتحول تلقائيًا إلى وضع تشغيل احتياطي عند تحقق أحد سيناريوهات الخطر، مثل تشغيل إشارات طوارئ يدوية بدلًا من الرقمية، أو تفعيل نظام مستقل للتهوية أو الإنارة.
- **اختبار دوري للبروتوكولات:** تُجرى اختبارات دورية للتأكد من فعالية هذه البروتوكولات في حالات انقطاع الخدمة، أو فقدان البيانات، أو العبث المحتمل.
- **تصميم متعدد الطبقات للسلامة (Layered Safety Design):** بحيث لا يعتمد التشغيل الآمن على عنصر تقني واحد، بل على بنية متداخلة من أنظمة الوقاية والاستجابة.

2. محاكاة الهجمات السيبرانية-المادية

(Cyber-Physical Attack Simulation)

لتحقيق الجاهزية الحقيقية، لا بد من إخضاع المنظومة لسيناريوهات تهديد تحاكي الواقع بأقصى درجات التعقيد:

- **تمارين محاكاة هجومية ميدانية ورقمية:** تشمل تزييف بيانات الحساسات، إبطاء استجابة النظام، اختراق لوحة القيادة، أو تنفيذ سيناريو هجوم داخلي (Insider Threat).
- **التوأم الرقمي كمختبر محاكاة:** يتم توظيف التوأم نفسه لاختبار قدرة النظام على اكتشاف السلوك غير الطبيعي، واستجابة الفريق التشغيلي، وفعالية التنبيهات اللحظية.
- **تقييم الأداء في الأزمات:** بعد كل تمرين، يتم قياس مؤشرات رئيسية مثل زمن الكشف، دقة الاستجابة، معدل الخطأ البشري، ومرونة النظام.
- **تغذية راجعة للتطوير الفوري:** تُستخدم نتائج المحاكاة لتعديل السياسات والإجراءات، وتحديث النماذج التنبؤية، وتعزيز نقاط الضعف المكتشفة.

3. حوكمة التعافي (Recovery Governance)

حين يقع الحادث فعليًا — سواء كان اختراقًا سيبرانيًا أو فشلًا في التوأم الرقمي — فإن النجاح يُقاس **بسرعة وموثوقية التعافي**:

- **خطة استعادة الثقة الرقمية:** لا تقتصر الحوكمة على استعادة البيانات، بل تشمل إجراءات موجهة لبناء الثقة مجددًا في دقة وموثوقية التوأم الرقمي.
- **خوارزميات مقارنة ما قبل وما بعد الحادث:** تُستخدم أدوات تحليل لتحديد ما إذا كانت هناك تغييرات في سلوك البيانات أو المعطيات النمطية نتيجة للحادث.
- **آلية تجميد التشغيل الرقمي المؤتمت:** في حالات معينة، قد تتطلب الحوكمة تجميد التفاعل التلقائي مع الأنظمة الميدانية إلى حين التحقق الكامل من سلامة النموذج الرقمي.
- **سجلات استجابة وتحقيق شفاف:** توثيق تفصيلي لسير الحادث، القرارات المتخذة، الفرضيات، وسيناريوهات البدائل، يُستخدم لاحقًا في التقارير الداخلية والخارجية.

✅ خلاصة المحور

تتحقق **المرونة السيبرانية-المادية** حين تتكامل **الاستشراف المبكر، والتصميم الدفاعي الذكي، والجاهزية التشغيلية، وقدرة التعافي** ضمن منظومة واحدة. ومن خلال هذا الإطار الحوكمي، لا يُنظر إلى الهجمات كاحتمالات نادرة، بل كاختبارات حتمية للمنظومة بأكملها، يُستعد لها بذكاء، ويُستجاب لها بثقة، ويُتعافى منها بشفافية واستدامة.

📘 15. حوكمة القيمة المضافة والاستدامة المالية

(Value & Financial Sustainability Governance)

لا تكتمل أي مبادرة رقمية — مهما بلغت من الابتكار والدقة التقنية — ما لم تُترجم إلى **قيمة ملموسة ومستدامة** على أرض الواقع. وفي سياق قطاع الطيران، حيث تتداخل العمليات التشغيلية مع التكاليف الرأسمالية والصيانة والخدمات اللوجستية والركابية، تصبح **حوكمة القيمة المضافة** حجر الأساس لتحقيق الجدوى الاقتصادية وضمان استمرارية النمو والتطوير.

1. نمذجة العائد على الاستثمار (ROI Modeling)

ينبغي أن تكون **كل مبادرة رقمية ضمن التوأم الرقمي خاضعة لنموذج مالي حوكمي مرن** يُقيم الأداء المالي بناءً على نتائج قابلة للقياس، لا الافتراضات النظرية:

- **تحليل الجدوى الاقتصادية المتكامل:** يشمل تكاليف الإنشاء، التشغيل، التدريب، وأتمتة العمليات، في مقابل العوائد الناتجة من تقليل الحوادث، تحسين اتخاذ القرار، تقليص الأعطال غير المخططة، وتسريع إجراءات التشغيل.
- **احتساب العائد غير المباشر:** مثل ارتفاع رضا المسافرين، خفض تكاليف التأمين نتيجة تحسين معايير الأمان، أو انخفاض التكاليف البيئية الناتجة عن كفاءة الطاقة — وهي عناصر لا تظهر فورًا في البيانات المالية ولكنها تُحدث أثرًا استراتيجيًا بعيد المدى.
- **نماذج ROI دورية ومتعددة السيناريوهات:** تُحدَّث نماذج العائد بشكل ربع سنوي أو نصف سنوي وفق معطيات الأداء، مع تضمين سيناريوهات متغيرة تشمل نمو عدد الرحلات، تغير أسعار الوقود، أو تطور تكلفة التقنية.

2. مؤشرات أداء القيمة (Value KPIs)

القيمة المضافة يجب ألا تكون مجرد شعار؛ بل يجب **قياسها، وتتبعها، والإفصاح عنها** من خلال مؤشرات أداء مالية وتشغيلية دقيقة:

- **أمثلة على مؤشرات الأداء النوعية:**
  - نسبة انخفاض الإنفاق على الصيانة الوقائية.
  - متوسط زمن تعافي النظام بعد أي عطل (MTTR).
  - نسبة تقليل استهلاك الطاقة داخل المنشآت التشغيلية.
  - نسبة زيادة عدد المسافرين المخدومين في الساعة الواحدة (تحسين السعة).
  - نسبة خفض الحوادث التشغيلية عبر التحليل الاستباقي.
- **الربط بالتحفيز المؤسسي:** تُربط هذه المؤشرات بقرارات تمويل لاحقة، وتحفيزات فرق العمل، وتقييم أداء الشركاء والموردين، لضمان ارتباط كل جزء من المنظومة بهدف اقتصادي واضح.

3. آليات التمويل المستدام

من التحديات التي تُواجه المشاريع الرقمية الكبرى هي **الاعتماد على ميزانيات مؤقتة أو دعم مخصص غير متكرر**. لتجاوز هذا، يجب بناء **نموذج تمويل ذاتي مرن** قائم على الإنجاز والقيمة:

- **ميزانيات قائمة على القيمة المتحققة:** تُخصّص ميزانيات التطوير والتحسين فقط عند تحقق مؤشرات محددة من القيمة الاقتصادية، ما يضمن توجيه الإنفاق نحو النتائج لا العمليات.
- **إعادة تدوير العوائد:** يُعاد استثمار جزء من الوفر المالي المتحقق بفعل المبادرات الرقمية داخل نفس المنظومة لتحفيز التحسين المستمر — ما يخلق حلقة مغلقة من التمويل الذاتي.

- **مشاركة القطاع الخاص عبر نماذج PPP:** يمكن دمج الشركاء من مزودي التقنية والمستثمرين من خلال نماذج "الشراكة بين القطاعين العام والخاص"، بحيث يتحمّل القطاع الخاص جزءًا من **المخاطر** مقابل نسبة من العوائد، بما يحفز الابتكار دون تحميل الدولة أعباء مباشرة.

✅ خلاصة المحور

تؤكد حوكمة القيمة المضافة أن **التوأمة الرقمية ليست مشروعًا هندسيًا، بل استثمارًا استراتيجيًا طويل الأمد.** وبهذه الرؤية، تُصبح الحوكمة المالية وسيلة لضمان الاستمرارية، واستشراف الفرص، وتسريع دورة التحسين، لا مجرد آلية رقابية. وفي إطار مبادرة "عين الصقر"، يشكل هذا المحور حجر الزاوية لبناء منظومة طيران **ذكية، مستقلة، ومستدامة ماليًا** على المدى البعيد.

📘 ثانيًا: المكونات التكميلية لدليل الحوكمة

تشكل المكونات التكميلية لدليل الحوكمة الرقمية **البنية التحتية المؤسسية والعملياتية** اللازمة لتحويل الإطار النظري إلى واقع مطبّق ومستدام. إنها العناصر الداعمة التي تضمن استمرار تطبيق الحوكمة الرقمية على التوأمة الرقمية بطريقة مؤسسية، منضبطة، ومتطورة، وتنسجم مع أهداف رؤية المملكة 2030، ومع المعايير الدولية ذات الصلة.

1. الوحدة الوطنية للحوكمة الرقمية (تحت إشراف الهيئة العامة للطيران المدني - GACA)

تمثل هذه الوحدة الكيان المركزي المسؤول عن **قيادة، تنسيق، وتطوير منظومة الحوكمة الرقمية** في قطاع الطيران، وتكون مرجعًا تنظيميًا وفنيًا لكافة الجهات المعنية:

- تعمل على **توحيد المعايير والسياسات والإجراءات** الخاصة بالحوكمة الرقمية وتحديثها بشكل دوري.
- تنسق مع الجهات التنظيمية الأخرى كـ SDAIA، ووزارة الداخلية، والجهات السيادية لضمان الاتساق التشريعي والتقني.
- تضطلع بدور **الرقابة الحوكميّة الاستباقية** عبر المراجعة المستمرة للسياسات والنماذج الرقمية، وتحديثها وفق أفضل الممارسات.

2. دليل وطني موحد لحوكمة التوأمة الرقمية

لضمان التجانس المؤسسي عبر جميع المطارات والمنشآت، فإن وجود دليل موحد يعتبر أداة محورية للتمكين **الحوكمي**:

- يُعد هذا الدليل المرجع الأساسي لجميع أصحاب العلاقة: من المهندسين والمشغلين إلى خبراء البيانات والجهات الرقابية.

- يُبنى الدليل على أساس تكاملي يجمع بين: **الأمن السيبراني، الحوكمة المؤسسية، تحليل المخاطر، حوكمة البيانات، الذكاء الاصطناعي، والتشغيل الذكي.**
- يتضمن الدليل أيضًا نماذج تشغيلية مرجعية (Blueprints) وقوالب قابلة للتطبيق (Templates) لتسهيل عملية التبني والتنفيذ.

3. منظومة تدقيق مستمرة على التوأمة الرقمية

من دون **رقابة محكمة وتقييم دوري**، تبقى الحوكمة عرضة للاهتزاز. ولهذا، يجب تأسيس منظومة تدقيق شاملة تشمل:

- **تدقيق تقني شامل:** يغطي كفاءة النماذج، جودة البيانات، استجابة الأنظمة، وامتثال البنية الرقمية للمواصفات.
- **تدقيق تنظيمي وتشغيلي:** يراجع مدى التزام الجهات بالإجراءات والسياسات، وفعالية عمليات اتخاذ القرار، وامتثال ممارسات التشغيل الذكي.
- **مؤشرات تدقيق دورية:** تُربط بنتائج الأداء، ويتم تحليلها لاقتراح تحسينات جوهرية قابلة للتطبيق على مستوى المنصة أو النظام.

4. تطوير القدرات البشرية (الإدارية، التقنية، التشغيلية)

الموارد البشرية هي الوقود الحقيقي لأي منظومة رقمية، والحوكمة دون بناء قدرات تُعدّ ممارسة قاصرة. ولهذا:

- يتم تصميم **برامج تخصصية متقدمة** في: تحليل البيانات، حوكمة الذكاء الاصطناعي، أمن المعلومات، الرقابة التشغيلية، وقيادة الابتكار.
- تُعتمد آليات التدريب العملي والميداني عبر نماذج التوأم الرقمي الحيّ لتقريب المفاهيم النظرية من الواقع.
- **ترخيص وتأهيل الكفاءات** في مجال حوكمة التوأمة الرقمية، بالتعاون مع مؤسسات وطنية ودولية مثل الأكاديمية الوطنية للطيران، وجامعة SDAIA.

✅ **خلاصة المحور**

تُشكّل هذه المكونات التكميلية الأساس التنفيذي الفعلي لنجاح الحوكمة الرقمية. فهي ليست عناصر ثانوية، بل **عوامل تمكين رئيسية** تضمن الاستمرارية، وتعزز جودة التطبيق، وترفع من كفاءة الاستثمار في البنية الرقمية الوطنية. ومن خلال هذه المكونات، تنتقل مبادرة "عين الصقر" من نموذج فكري ريادي إلى **نظام حوكمي وطني قابل للتوسع، المراجعة، والتكامل عبر الزمن**.

📘 ثالثًا: ارتباط الحوكمة بالأهداف الاستراتيجية

إن الحوكمة الرقمية ليست غاية في حد ذاتها، بل هي وسيلة استراتيجية **تمكّن** المنظومة الوطنية للطيران من تحقيق أهدافها الكبرى ضمن إطار رؤية المملكة 2030، التي تسعى إلى ترسيخ ريادة المملكة في القطاعات الحيوية، بما في ذلك سلامة وأمن الطيران. وفي ضوء تعقيد البيئات التشغيلية المعتمدة على التوأمة الرقمية والذكاء الاصطناعي، يصبح للحوكمة دور محوري في **ترجمة الرؤية إلى ممارسات تشغيلية فعالة**، قائمة على الشفافية والابتكار والاستدامة.

1. تمكين الاستجابة اللحظية للمخاطر

تعتمد بيئة الطيران الحديثة على أنظمة معقدة مترابطة تتفاعل مع تغيّرات لحظية في الزمن الحقيقي. ومن خلال حوكمة ذكية تعتمد على البيانات:

- يتم **تحديد المخاطر المحتملة قبل وقوعها** عبر تحليل استباقي داخل التوأم الرقمي.
- تُفعّل سيناريوهات جاهزة للاستجابة في حال وقوع أحداث حرجة مثل أعطال فنية، ازدحام عملياتي، أو تهديدات أمنية.
- تُقلل أوقات اتخاذ القرار من ساعات إلى ثوانٍ معدودة، ما يرفع من **جاهزية المنظومة ويقلص الهدر التشغيلي والخسائر البشرية**.

2. تعزيز الامتثال الكامل للمعايير الدولية

تُعد الحوكمة الوسيلة الأكثر موثوقية لضمان **الاتساق التنظيمي والتشغيلي** مع المعايير الدولية، مما يعزز مكانة المملكة كمركز طيران إقليمي وعالمي:

- تكفل الحوكمة الالتزام المستمر بإرشادات ICAO، وتطبيق معايير ISO/NIST وIATA، بطريقة مدمجة داخل الأنظمة الرقمية نفسها.
- توفر تقارير ذكية وآلية توثق الامتثال، وتتيح لفرق التدقيق الداخلي والخارجي متابعة الأداء اللحظي والانحرافات في الزمن الحقيقي.
- تعزز قدرة المملكة على **اجتياز تقييمات الامتثال الدولية** بسهولة، بما يفتح الأبواب أمام مزيد من الشراكات والتحالفات الجوية.

3. بناء الثقة في تجربة المسافر

في قطاع يواجه تحديات يومية تتعلق بالسلامة، السرعة، والراحة، تصبح الحوكمة عاملاً حاسمًا في تعزيز ثقة المسافر:

- تضمن **شفافية الإجراءات وتناسقها**، ما ينعكس في تجربة سلسة ومنظمة داخل المطار.
- تفعّل تقنيات الاستشعار والذكاء الاصطناعي بطريقة لا تنتهك الخصوصية، من خلال ضوابط حوكمة دقيقة وواضحة.
- تعزز مصداقية التعامل مع شكاوى الركاب والبلاغات الأمنية عبر منصات رقمية متصلة بحوكمة مركزية، ما يولد شعورًا بالاطمئنان لدى المستخدم النهائي.

4. تسريع الابتكار المستدام في بيئة عالية التعقيد

البيئات المعتمدة على التوأم الرقمي والذكاء الاصطناعي تتطلب مساحات آمنة للاختبار والابتكار، دون المساس بالسلامة أو الامتثال:

- تخلق الحوكمة إطارًا حامياً يسمح بالتجريب والابتكار **ضمن حدود واضحة ومعايير شفافة**.
- تُفعّل مبادرات الابتكار المفتوح (Open Innovation) وربطها مباشرة بالمجال التشغيلي، مما يسمح بتحقيق مكاسب حقيقية بدلًا من أفكار نظرية.
- تُدمج الحوكمة بمنهجيات الابتكار الرشيق (Agile Innovation) والتصميم المرتكز على المستخدم (Human-Centered Design)، بما يضمن تحوّلاً رقميًا مستدامًا لا عشوائيًا.

5. دعم استدامة التشغيل والموارد البيئية

الاستدامة لم تعد خيارًا ثانويًا، بل أصبحت **شرطًا وجوديًا** للمطارات الحديثة ضمن التصنيفات البيئية العالمية مثل ACI وLEED:

- تتيح الحوكمة تتبع البصمة الكربونية لكل عملية تشغيلية عبر التوأم الرقمي، بما يمكّن من **ضبط الاستهلاك في الزمن الحقيقي**.
- تُوظف أدوات تحليل متقدمة لتحديد الفرص الخفية في توفير الطاقة، تحسين التبريد، تقليل استهلاك الوقود، وتحسين إدارة النفايات.
- تُربط مؤشرات الأداء البيئي بنموذج الحوكمة الشامل، ما يحفز التحسين المستمر ويضمن المراجعة البيئية الدورية.

✅ خلاصة المحور

ترتبط الحوكمة الرقمية في قطاع الطيران بمبادرة "عين الصقر" **ارتباطًا وظيفيًا واستراتيجيًا مباشرًا** بتحقيق رؤية وطنية طموحة نحو مستقبل آمن، ذكي، مستدام، ومبني على الثقة. إنها الأداة الحقيقية التي تحوّل الطموحات الكبرى إلى نتائج قابلة للقياس، و**تُحدث نقلة نوعية من الفوضى الرقمية إلى القيادة المؤسسية الذكية**.

📎 الملحقات

📎 الملحق (أ): الإطار القانوني والتنظيمي المرجعي

يشكل الإطار القانوني والتنظيمي حجر الزاوية في أي نظام حوكمة ناجح، خصوصًا في بيئات عالية الحساسية والتعقيد مثل قطاع الطيران المدني. وفي مبادرة "عين الصقر"، تم تصميم نظام الحوكمة الرقمية للتوأمة الرقمية بالاستناد إلى مرجعيات تنظيمية وتشريعية محلية وإقليمية ودولية تُرسّخ الامتثال، وتضمن التكامل، وتعزز الموثوقية والسيادة الرقمية.

أولاً: السياسات الوطنية للجهات التنظيمية ذات العلاقة

- **سياسات الهيئة العامة للطيران المدني (GACA)**

تُمثل GACA السلطة التنظيمية العليا لقطاع الطيران المدني في المملكة، وتشمل مسؤولياتها:

- وضع الأطر الناظمة لسلامة الطيران وأمنه، بما في ذلك أمن المطارات، الركاب، الأمتعة، وأنظمة المعلومات.
- إصدار لوائح تشغيلية دقيقة تضمن سلامة البيانات في الأنظمة الرقمية المستخدمة داخل المطارات.
- تحديد متطلبات الامتثال والاعتماد الرقمي لأنظمة الذكاء الاصطناعي والتوأمة الرقمية.

تُعد السياسات الصادرة عن GACA أساسًا إلزاميًا ضمن دليل الحوكمة، وتُدمج رقميًا داخل التوأم الرقمي لضمان الرصد اللحظي لحالة الامتثال.

- **أنظمة الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA)**

بصفتها الجهة المعنية بحوكمة البيانات والسيادة الرقمية، تُصدر SDAIA مجموعة من السياسات واللوائح التي تؤطر:

- تصنيف البيانات الحساسة ومواقع تخزينها.
- آليات حمايتها من الوصول غير المشروع.
- حوكمة نماذج الذكاء الاصطناعي وتفسير قراراتها.

ترتبط هذه الأنظمة عضوياً بمنصة "عين الصقر" لضمان الالتزام بمعايير السيادة الوطنية والامتثال الرقمي عند التعامل مع البيانات البيومترية والتشغيلية.

ثانيًا: المعايير الدولية المعتمدة في الإطار التنظيمي

✈️ ICAO – Annex 17

أحد أهم الملاحق الصادرة عن منظمة الطيران المدني الدولي، ويُعنى بأمن الطيران ضد الأعمال غير المشروعة. يشكل هذا الملحق مرجعًا عالميًا يُستخدم لضمان:

- سلامة الأنظمة الرقمية المستخدمة في التوأمة.
- منع أي اختراق إلكتروني قد يُستغل لتنفيذ تهديدات مادية أو رقمية داخل المطارات.

🔐 ISO/IEC 27001 – معيار إدارة أمن المعلومات

يُعتبر معيار ISO 27001 إطارًا صارمًا لإدارة أمن المعلومات الرقمية، ويُلزم المؤسسات بما يلي:

- تحديد أصول المعلومات الحساسة.
- تقييم المخاطر الرقمية.
- تنفيذ ضوابط وقائية (Controls) لحماية الأنظمة.

تقوم مبادرة "عين الصقر" بتطبيق هذا المعيار على البنية التحتية الرقمية الخاصة بها، ويجري ربط مؤشرات الامتثال بهذا المعيار عبر لوحات التحكم القيادية.

🛡️ ISO 45001 – معيار السلامة والصحة المهنية

لا تقتصر التوأمة الرقمية على الأنظمة التقنية فقط، بل تمتد لتشمل البيئة التشغيلية والبشرية. لذا فإن دمج معيار ISO 45001 في الحوكمة الرقمية يضمن:

- مراقبة سلوكيات الأفراد عبر التوأم الرقمي.
- الكشف عن الممارسات التشغيلية التي قد تؤدي إلى حوادث.
- تعزيز بيئة عمل آمنة واستباقية.

🔒 NIST Cybersecurity Framework

تم تطوير هذا الإطار من قِبل المعهد الوطني الأمريكي للمعايير والتقنية، ويُعد مرجعًا عالميًا في حوكمة الأمن السيبراني. يشمل:

- تحديد الأصول الرقمية الحرجة.
- حماية الشبكات من الهجمات المستهدفة.
- كشف التهديدات والرد عليها واستعادة الخدمة بعد الحوادث.

يُطبّق هذا الإطار داخل مكونات التوأم الرقمي لضمان التفاعل الديناميكي بين الاستشعار والتحليل والاستجابة السيبرانية.

🌐 IATA Guidelines

توفر إرشادات الاتحاد الدولي للنقل الجوي توجيهات تشغيلية وأمنية لجميع جوانب النقل الجوي، بما يشمل:

- إدارة العمليات الأرضية.
- تسهيل حركة الركاب.
- سلامة أنظمة التشغيل الإلكتروني والحوسبة الطرفية داخل المطارات.

✅ **خلاصة الملحق**

إن التكامل بين السياسات الوطنية والمعايير الدولية ضمن الإطار المرجعي المنظم لمبادرة "عين الصقر"، ليس مجرد توافق تنظيمي، بل **ركيزة استراتيجية تضمن الاستقرار، الموثوقية، والقبول الدولي**. ويُعد هذا الملحق الوثيقة القانونية والفنية التي تبرر وتُشرعن جميع قرارات وتصميمات الحوكمة الرقمية للتوأمة في القطاع، وتجعل من التجربة السعودية في هذا المجال نموذجًا مرجعيًا يُحتذى به عالميًا.

📎 الملحق (ب): مصفوفة الأدوار والمسؤوليات (نموذج RACI)

تشكل مصفوفة **RACI** (اختصارًا لـ: Responsible, Accountable, Consulted, Informed) أحد أهم الأدوات المنهجية لضمان وضوح الأدوار، ومنع التداخل المؤسسي، وتعزيز كفاءة اتخاذ القرار داخل منظومة الحوكمة الرقمية، وخاصةً في بيئة حيوية ومعقدة كتلك الخاصة بالتوأمة الرقمية في قطاع الطيران.

تم إعداد هذا النموذج بما يتماشى مع المتطلبات الوطنية السعودية (بقيادة الهيئة العامة للطيران المدني GACA والهيئة السعودية للبيانات والذكاء الاصطناعي SDAIA)، ومع الممارسات الإقليمية والدولية المثلى لضمان الاستجابة الفورية، ودقة التنفيذ، وجودة الامتثال.

🔹 اعتماد السياسات

- **مسؤول التنفيذ:** الوحدة الوطنية للحوكمة الرقمية
  تُكلّف بإعداد السياسات والإجراءات التفصيلية بالتنسيق مع الجهات التنظيمية والتشغيلية، مع مواءمتها للأطر الوطنية والدولية.
- **صاحب الصلاحية:** مجلس إدارة الهيئة العامة للطيران المدني (GACA)
  الجهة الوحيدة المخوّلة باعتماد السياسات وتفويضها، مما يعزز الموثوقية والسيادة التنظيمية.
- **يُستشار:** SDAIA، الجهات الأمنية
  تُشارك في تقديم الرأي التنظيمي والتقني فيما يخص السيادة الرقمية، أمن البيانات، وحماية البنى التحتية الحساسة.

- **يُبلَّغ:** شركات المطارات
يتم إشعارها رسميًا بالتحديثات والسياسات الجديدة لضمان تنفيذها الفعلي داخل المنشآت.

- تصنيف البيانات

- **مسؤول التنفيذ:** مدير بيانات التوأم الرقمي
يقود عملية تصنيف البيانات (بيومترية، تشغيلية، أمنية، إلخ) وفق معايير SDAIA وISO، ويضمن تطبيق سياسات تصنيف محكمة ومرنة.
- **صاحب الصلاحية:** الوحدة الوطنية
تعتمد نتائج التصنيف النهائي وتربطها بالأدوار التشغيلية والصلاحيات المؤسسية.
- **يُستشار:** الإدارات التشغيلية
تُستشار لتحديد حساسية البيانات حسب استخدامها الفعلي في العمليات.
- **يُبلَّغ:** كافة المستخدمين
يتم توعيتهم بمستوى سرية البيانات التي يتعاملون معها والإجراءات المصاحبة لكل تصنيف.

- **إدارة الوصول**

- **مسؤول التنفيذ:** فريق أمن المعلومات
يضطلع بمهمة ضبط سياسات التحكم في الوصول للأنظمة والمنصات الرقمية، وتنفيذ آليات التوثيق المتقدم (مثل MFA، Zero Trust).
- **صاحب الصلاحية:** مدير أمن التوأم الرقمي
يمتلك صلاحية منح أو إلغاء الوصول للبيانات أو الأنظمة الحيوية وفقًا لمستوى الحساسية والتصنيف.
- **يُستشار:** رؤساء الأقسام
يُطلب منهم تحديد متطلبات الوصول ضمن فرقهم، وتقييم الحاجة الفعلية للموارد.
- **يُبلَّغ:** مدقق الامتثال
يحصل على نسخة من سجل الوصول والتحديثات الدورية للتحقق من مدى التزام السياسات.

🔹 **الاستجابة للحوادث**

- **مسؤول التنفيذ:** فريق الطوارئ السيبراني (CERT)
  يتولى قيادة العمليات الفنية والاستجابة السريعة للحوادث السيبرانية أو الانقطاعات الرقمية، بما يشمل التفاعل مع التوأم الرقمي.
- **صاحب الصلاحية:** رئيس أمن المعلومات
  يتخذ القرارات النهائية حول رفع مستوى الطوارئ، تصعيد الحالات، أو تعطيل الأنظمة كإجراء وقائي.
- **يُستشار:** الوحدة الوطنية للحوكمة لتقييم تأثير الحادث على الامتثال العام ومصداقية المنظومة الرقمية، وتحديد الإجراءات التصحيحية طويلة المدى.
- **يُبلَّغ:** القيادة التنفيذية
  تُخطر فوريًا بحالة الطوارئ لتنسيق الاستجابة المؤسسية والإعلامية واتخاذ التدابير الاستراتيجية المصاحبة.

✅ **خلاصة الملحق**

تُعد مصفوفة RACI في هذا الدليل ليس فقط أداة تنظيمية، بل **ركيزة تشغيلية لتوزيع المسؤوليات بشكل ذكي ومرن**، تتكامل مع حوكمة الذكاء الاصطناعي، وإدارة البيانات، والاستجابة السيبرانية، لتصنع منظومة متماسكة وقابلة للتوسع. ومن خلال هذا التوزيع المحكم، تصبح المنظومة الرقمية قادرة على الاستجابة بسرعة، والتعلم من الأخطاء، ومواصلة التطور ضمن أعلى معايير السلامة، السيادة، والابتكار.

📎 ملحق (ج): قنوات التواصل

في أي منظومة حوكمة رقمية متكاملة، تُعد قنوات التواصل أحد الأعمدة الأساسية التي تضمن التفاعل الفعّال بين الجهات المسؤولة والمستفيدين الداخليين والخارجيين، وتسهم في ترسيخ ثقافة الشفافية والمساءلة، كما تُمكِّن من رصد التحديات والملاحظات والتحسينات في الزمن الحقيقي. وضمن إطار مبادرة "عين الصقر"، تم تخصيص قنوات تواصل احترافية ومتنوعة تواكب حساسية البيئة التشغيلية وأهمية انسيابية المعلومة.

🔹 **الاستفسارات العامة**

البريد الإلكتروني للوحدة الوطنية للحوكمة الرقمية
تم تخصيص عنوان تواصلي موحد لاستقبال كافة الأسئلة والاستفسارات ذات العلاقة بالدليل، أو السياسات المعتمدة، أو أي جوانب تنظيمية أو تقنية تتعلق بتطبيقات التوأمة الرقمية في قطاع الطيران.

هذه القناة تتيح للجهات التشغيلية، ومقدمي الخدمات، والمطورين، والمهتمين من القطاعين العام والخاص الحصول على إجابات رسمية ومعتمدة، مما يسهم في تقليل الاجتهادات الفردية وضمان تفسير موحد للسياسات والمعايير.

- **الإبلاغ عن مخالفات الامتثال**

الخط الساخن أو البوابة الإلكترونية الخاصة بوحدة التدقيق
في بيئة رقمية معقدة كبيئة التوأم الرقمي، يصبح الامتثال أداة حيوية للسلامة، وليس مجرد التزام إداري. لذا تم توفير قناة مخصصة وآمنة تسمح بالإبلاغ الفوري عن أي مخالفات تنظيمية، تشغيلية، أو سيبرانية.
وتُدار هذه القناة من قبل وحدة مستقلة لضمان النزاهة والخصوصية، وتخضع آليتها لإطار زمني واضح لمعالجة البلاغات، بما يضمن الاستجابة العادلة والفعالة.

- **مقترحات تحسين (Kaizen)**

منصة "عين الصقر" للابتكار والتطوير
تماشيًا مع فلسفة "التحسين المستمر" (Kaizen)، تُعد هذه المنصة مساحة رقمية مفتوحة تسمح للمستخدمين — من مشغلي الأنظمة، وفنيي الصيانة، وحتى المسافرين — بتقديم أفكارهم وملاحظاتهم ومقترحاتهم التطويرية على مدار الساعة.

ويُعد ربط هذه المنصة مباشرة بالنظام التشغيلي للتوأم الرقمي خطوة استراتيجية، حيث تُحوَّل المقترحات تلقائيًا إلى وحدات التحليل، ويتم تقييمها باستخدام مؤشرات القيمة المضافة، ومن ثم اتخاذ القرار بشأن تنفيذها وفق أولويات واضحة.

خلاصة الملحق

تمثل قنوات التواصل في هذا الملحق **نقطة التقاء بين الشفافية التشغيلية والتمكين المجتمعي**، حيث تضمن سرعة الاستجابة، وتوسيع دائرة المشاركة، وإغلاق فجوات الصمت المؤسسي. وهي ليست مجرد وسائط نقل معلومات، بل أدوات تمكين تخلق بيئة تشغيلية مرنة، وتزيد من النضج المؤسسي، وتعزز الولاء والثقة على المستويين المحلي والدولي.

🔷 تنويه منهجي

> تم إعداد هذه الدراسة كمقترح علمي/تشغيلي للمشاركة في هاكاثون الطيران المدني، وهي مبنية بالكامل على اجتهادات تحليلية وممارسات مرجعية دولية متاحة للعامة، دون مشاركة أي جهة رسمية أو تكليف من جهة تنظيمية قائمة.

جميع السياسات، الأدوار، الأطر، والأمثلة الواردة تُطرح **كنموذج افتراضي قابل للتبني أو التعديل**، ويُفترض تعيين الجهات المرجعية ذات العلاقة لاحقًا عند اعتماد المبادرة رسميًا.

تهدف هذه الوثيقة إلى تقديم **رؤية ابتكارية ومتكاملة** تسهم في تعزيز سلامة وأمن قطاع الطيران باستخدام منظومة التوأمة الرقمية وحوكمتها الفعالة.

📘 مسرد المصطلحات (Glossary of Terms)

ضمن بيئة تشغيلية رقمية متسارعة كتلك الخاصة بقطاع الطيران، يُعد توحيد المفاهيم والمصطلحات من أهم عوامل نجاح أي مبادرة رقمية. إن وجود مرجعية لغوية دقيقة يسهم في بناء فهم مشترك بين الأطراف التقنية، والإدارية، والتنظيمية، ويضمن تكامل الرؤية عند تصميم السياسات وتنفيذ الحلول. فيما يلي المصطلحات الأساسية التي تشكّل القاموس المفاهيمي لدليل الحوكمة الرقمية لمنظومة التوأمة الرقمية:

- **التوأم الرقمي (Digital Twin)**

هو نموذج رقمي حي ومتزامن يُنشأ ليعكس أصلًا ماديًا فعليًا (كالمطار أو أحد أنظمته الفرعية)، ويُحدث باستمرار بناءً على تدفقات البيانات اللحظية من الحساسات والمصادر المتعددة.
يُستخدم هذا التوأم في مهام المراقبة، التحليل، التشخيص، والتنبؤ بسلوك النظام، مما يتيح اتخاذ قرارات قائمة على الواقع الرقمي قبل أن تتطور التحديات إلى مشكلات فعلية.
يمثّل التوأم الرقمي حجر الأساس في التحول من الصيانة التفاعلية إلى الإدارة الاستباقية.

- **التوأم الإدراكي (Cognitive Twin)**

هو الامتداد التطوري للتوأم الرقمي، حيث لا يقتصر دوره على تمثيل الواقع بل يتجاوزه إلى فهمه وتحليله سياقيًا عبر تقنيات الذكاء الاصطناعي المتقدمة والتعلم العميق.
يمتاز هذا النموذج بقدرته على التعلم التراكمي، وتوليد رؤى تنبؤية معقدة، واقتراح قرارات مدعومة بالأدلة، بل وتفسيرها للمستخدمين المعنيين (XAI).
هذا المفهوم يشكّل ركيزة استراتيجية للانتقال من الأتمتة التقليدية إلى منظومات "تفكر وتفهم".

- **الحوكمة الرقمية (Digital Governance)**

تشير إلى الإطار المؤسسي، التنظيمي، والتشغيلي الذي يضبط بيئة العمل الرقمية من حيث الصلاحيات، صنع القرار، المساءلة، والامتثال.
في سياق التوأمة الرقمية، تُعد الحوكمة الضامن المركزي لجودة البيانات، أمن النماذج، موثوقية الأداء، وشفافية الأثر.

تشمل هذه الحوكمة السياسات، الأدوار، أدوات التدقيق، وآليات التحسين المستمر، وهي التي تحول التكنولوجيا من أدوات منفصلة إلى منظومة متماسكة ذات موثوقية تشغيلية.

- **السيناريوهات الاستباقية (Proactive Scenarios)**

هي نماذج محاكاة مخططة مسبقًا لأحداث محتملة، تُستخدم لاختبار الجاهزية التشغيلية والمرونة السيبرانية والفيزيائية.
تشمل هذه السيناريوهات حالات مثل تعطّل أحد أنظمة المراقبة، أو اختراق أمني لحساسات حيوية، أو تكدس مفاجئ في تدفقات المسافرين.
يسهم تفعيل هذه السيناريوهات داخل بيئة التوأم الرقمي في تطوير خطط الاستجابة وتدريب الكوادر على إدارة الأزمات.

- **الوضع الآمن (Fail-Safe)**

هو وضع تشغيل احتياطي آمن يُفعّل تلقائيًا عند حدوث انقطاع في الاتصال، أو تعطل في النظام الرقمي، أو عند الكشف عن بيانات غير موثوقة.
يهدف هذا النمط إلى ضمان الحد الأدنى من الاستمرارية التشغيلية والأمان، مع تعطيل مؤقت لبعض الوظائف غير الحيوية.
يتطلب تصميم هذا الوضع مراجعة دقيقة لأولوية العمليات، وتحديد المسارات الحرجة التي يجب أن تظل نشطة حتى أثناء الفشل أو الانفصال الرقمي.

🟦 ملاحظات ختامية

إن مسرد المصطلحات هذا ليس مجرد ملحق لغوي، بل يُعد أداة استراتيجية لضمان وحدة التفسير، وتقليل ازدواجية الفهم، وتعزيز قدرة أصحاب المصلحة على المشاركة الفاعلة في بناء وتشغيل حوكمة التوأمة الرقمية بكفاءة واحترافية.

📘 المراجع

- **International Civil Aviation Organization (ICAO).** (2022). *Annex 17 – Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference*. ICAO Publications.

- **International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC).**
  (2022). *ISO/IEC 27001 – Information Security Management Systems – Requirements*.

- **International Organization for Standardization (ISO).**
  (2018). *ISO 45001 – Occupational Health and Safety Management Systems – Requirements with Guidance for Use*.

- **National Institute of Standards and Technology (NIST).**
  (2018). *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1. U.S. Department of Commerce.

- **International Air Transport Association (IATA).**
  (2021). *Security and Safety Guidelines*. IATA Publications.

📘 شكر وعرفان

تتقدم قيادة فريق إعداد هذه الدراسة بخالص الشكر والتقدير إلى كافة المبادرات، والممارسات الدولية، والمعايير التنظيمية التي أتاحت محتواها عبر المصادر المفتوحة، مما أتاح لنا بناء هذا النموذج المقترح لحوكمة التوأمة الرقمية في قطاع الطيران. لقد كان لتنوع وتكامل هذه المراجع العامة دورٌ محوري في تشكيل رؤية شاملة وعملية تستند إلى أفضل ما توصلت إليه التجارب العالمية.

🔹 **تنويه مهم:**

تم إعداد هذا الدليل ضمن إطار المشاركة في **هاكاثون الطيران المدني**، وهو يعكس اجتهادًا علميًا وتحليليًا قائمًا على معلومات عامة وفرضيات فنية واستراتيجية مستمدة من مصادر مفتوحة، دون أي تدخل أو تكليف من جهات رسمية.

لم يتم الاستعانة بأي جهة حكومية أو خاصة في إعداد هذا العمل، ولم يُقدّم لنا أي دعم مباشر أو غير مباشر من أي جهة كانت.

نأمل أن تسهم هذه الدراسة في إثراء النقاشات الوطنية حول مستقبل سلامة وأمن الطيران، وتعزيز جاهزية المملكة للريادة الرقمية في أحد أكثر القطاعات حساسية وتعقيدًا في العالم.