ايكاو

Doc 10213 ـ غير مقيَّدة التوزيع

اعتبارات المخاطر الإلكترونية العالمية

الطبعة الأولى - ٢٠٢٥

اعتمدها الأمين العام ونُشرت بموجب سلطته

منظمة الطيران المدني الدولي

ايكاو

Doc 10213 ـ غير مقيَّدة التوزيع

اعتبارات المخاطر الإلكترونية العالمية

الطبعة الأولى - ٢٠٢٥

اعتمدها الأمين العام ونُشرت بموجب سلطته

منظمة الطيران المدني الدولي

تُنشر هذه الوثيقة في طبعات مستقلة باللغات العربية والإسبانية والإنجليزية
والروسية والصينية والفرنسية
منظمة الطيران المدني الدولي
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

للحصول على المعلومات المتعلقة بتقديم طلبات الشراء، والاطلاع على قائمة بأسماء
جميع وكلاء البيع وبائعي الكتب، يرجى زيارة موقع الإيكاوالإيكاو على الرابط: www.icao.int

الطبعة الأولي – ٢٠٢٥

الوثيقة Doc 10213 – "اعتبارات المخاطر الإلكترونية العالمية"
Order Number: 10213-U
ISBN 978-92-9275-999-5-O

التعديلات

تُعلن التعديلات في ملاحق كتالوج المنتجات والخدمات، ويمكن الاطلاع على الكتالوج وملاحقه على موقع الإيكاو على الإنترنت عبر الرابط www.icao.int. والجدول أدناه مخصّص لتسجيل مثل هذه التعديلات.

سجل التعديلات والتصويبات

التعديلات		
رقم	التاريخ	أُدخل بواسطة

التصويبات			
رقم	اللغة	التاريخ	أُدخل بواسطة

تحتوي وثيقة الإيكاو "اعتبارات المخاطر الإلكترونية العالمية" (الوثيقة Doc 10213 – مقيَّدة التوزيع) على معلومات مقيَّدة التوزيع ويقتصر استخدامها على الجهات الحكومية ومؤسسات الصناعة وسائر جهات قطاع الطيران المعنية بالأمن الإلكتروني لأغراض تقييم المخاطر. أما هذه النسخة من الوثيقة Doc 10213 فهي تتضمَّن مقتطفات غير مقيَّدة التوزيع ويمكن توزيعها على الجمهور العام.

تمهيد

شهد العقدان الماضيان تطورات متسارعة في استخدام المعلومات والتقنيات الجديدة في قطاع الطيران المدني لدعم أهداف التشغيل الآلي والترابط والتشغيل البيني. وقد تسارعت وتيرة هذا الاتجاه في الآونة الأخيرة، لا سيما في المجالات التشغيلية، بغرض الاستفادة من آخر المستجدات التكنولوجية، مثل التعلم الآلي وتحليل البيانات الضخمة. وستؤدي هذه الرقمنة إلى التعجيل بنشر مفاهيم تشغيلية جديدة على الأرض وفي الجو ودمج الوافدين الجدد، مثل أنظمة الطائرات غير المأهولة، في منظومة النقل الجوي. ويكمن الهدف النهائي من هذه التطورات في تحقيق نمو قطاع الطيران المدني وضمان سلامته وأمنه وكفاءته وسعته واستدامته في الوقت نفسه.

إلا إن هذا الاتجاه أدى إلى توسيع نطاق التهديدات الإلكترونية لتشمل الأنظمة التشغيلية والمعلومات، مع احتمال حدوث آثار سلبية على سلامة الطيران المدني وأمنه وسعته و/أو كفاءته. ومن ثم لم يجد قطاع الطيران مفراً من التصدي للتهديدات والمخاطر الإلكترونية التي يتعرض لها الطيران المدني خارج السياق التقليدي لأمن تكنولوجيا المعلومات/التكنولوجيا التشغيلية (IT/OT) بحيث يجري دمج إدارة المخاطر الإلكترونية في مجال الطيران في العمليات المتعلقة بإدارة مخاطر الطيران في كافة تخصّصات الطيران المدني. ويأتي ذلك دعماً لحماية منظومة النقل الجوي وتحصينها من خلال أُطر فعالة وقوية لإدارة المخاطر.

وقد أعدت الإيكاو وثيقة "اعتبارات المخاطر الإلكترونية العالمية" لمساعدة الدول الأعضاء والجهات المعنية في دمج إدارة المخاطر الإلكترونية في عملياتها لإدارة مخاطر الطيران. كما ترسم الوثيقة أيضاً مشهداً عالمياً عالي التنوع للتهديدات الإلكترونية بغرض التأكيد على أهمية التصدي للتهديدات والمخاطر الإلكترونية التي يتعرض لها الطيران المدني، للمساعدة في تحصين القطاع وحمايته.

وتدعم الوثيقة الدول والجهات المعنية في الوفاء بالتزاماتها المتعلقة بتقييم المخاطر على النحو المنصوص عليه في الملاحق باتفاقية الطيران المدني الدولي (اتفاقية شيكاغو)، ولا سيما التزاماتها بموجب القاعدة القياسية ٤-٩-١ في الملحق السابع عشر — "أمن الطيران". كما تدعم الوثيقة أيضا تنفيذ استراتيجية[١] الإيكاو للأمن الإلكتروني في مجال الطيران وخطة عمل الأمن الإلكتروني المرتبطة بها.[٢]

وتتماشى المعلومات الواردة في هذه الوثيقة مع المبادئ العامة لتوجيهات الإيكاو بشأن السلامة الجوية وأمن الطيران، كما ترد في "بيان سياق المخاطر العالمية في مجال أمن الطيران" (Doc 10108 وثيقة مقيَّدة التوزيع) ووثيقتيْ "دليل أمن الطيران" (Doc 8973 – وثيقة مقيّدة التوزيع) و"دليل إدارة السلامة" (Doc 9859).

وتتضمَّن هذه الوثيقة أيضاً مرفقات تحتوي على أمثلة لتطبيق منهجية إدارة المخاطر الإلكترونية في تقييمات مخاطر أمن وسلامة الطيران. كما تتضمن المرفقات أيضاً إرشادات بشأن تصنيف التهديدات الإلكترونية، وهي إرشادات مصمّمة لمساعدة الدول والجهات المعنية على تحديد الصلات المتبادلة والروابط بين مختلف تخصّصات الطيران. ويهدف ذلك إلى دعم مساعي استحداث ورعاية إطار قوي لإدارة المخاطر في مجال الطيران المدني.

ونود أن نعرب هنا عن تقديرنا للخبراء العاملين في فريق خبراء الأمن الإلكتروني ومجموعة عمل التهديدات والمخاطر الإلكترونية التابعة له على مساهماتهم القيّمة من حيث الوقت والمعرفة لدعم تطوير هذه الوثيقة.

---

[١] انظر https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx

[٢] انظر https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx

المحتويات

الصفحة

الأسماء الموجزة والمختصرات

ANSP	مقدّم خدمات ملاحة جوية
APT	التهديد المستمر المتطور
ATC	مراقبة الحركة الجوية
AVSEC	أمن الطيران
CPDLC	الاتصال بين المراقب والطيار عبر وصلة البيانات
CRC	التحقق الدوري للتكرارية
DDoS	حجب الخدمة الموزّع
EATM-CERT	فريق الاستجابة للطوارئ الحاسوبية التابع لإدارة الحركة الجوية الأوروبية
EFB	الحقيبة الإلكترونية للرحلات الجوية
FTA	تحليل شجرة الأعطال
GNSS	النظام العالمي للملاحة بالأقمار الصناعية
HVAC	التدفئة والتهوية وتكييف الهواء
IP	بروتوكول الإنترنت
IPR	حق الملكية الفكرية
IT/OT	تكنولوجيا المعلومات/التكنولوجيا التشغيلية
MET	الأرصاد الجوية
NEASCOG	فريق التنسيق المشترك بين الناتو ويوروكنترول المعني بأمن إدارة الحركة الجوية
PBIED	الجهاز المتفجّر الارتجالي المحمول
PII	معلومات محدِّدة لهوية الأشخاص
UAS	نظام (نُظُم) الطائرة غير المأهولة

الفصل الأول

التعاريف

مراقبة الدخول. تدابير لحظر الوصول إلى الأصول المادية والإلكترونية إلا على أولئك المصرّح لهم.

وسيلة إيصال الهجوم. وسيلة الوصول التي يستخدمها المهاجم لبدء الهجوم.

التوافر. إتاحة للوصول أو الاستخدام عند الطلب من قبل فرد مأذون له أو مستخدم أو برنامج أو عملية أو نظام أو جهاز.

الأمن الإلكتروني في مجال الطيران. مجموعة التقنيات والضوابط والتدابير والعمليات والإجراءات والممارسات المصمّمة لضمان السرية والسلامة والتوافر والحماية الشاملة وقدرة الأصول الإلكترونية على التصدي للهجوم و/أو التلف و/أو التدمير و/أو التعطيل و/أو الوصول غير المأذون به و/أو الاستغلال.

السرية. خاصية عدم إتاحة سُبل الوصول إلى أي أصل من الأصول أو الكشف عنه لفرد أو مستخدم أو برنامج أو عملية أو نظام أو جهاز غير مأذون له.

البينة التحتية الحرجة للطيران المدني. الأصول التي تعتبر حيوية لدرجة أن إصابتها بالعجز أو تعريضها للخطر أو تدميرها من شأنه أن يُحدث تأثيراً موهناً على سلامة الطيران وأمن الطيران وكفاءته و/أو سعته.

أصل إلكتروني. البنود الرقمية والمادية التي لها قيمة من حيث الأعمال والعمليات والسلامة الجوية وأمن الطيران والكفاءة و/أو السعة، مثل الأنظمة والمعلومات والبيانات والشبكات والأجهزة والبرامج والمعدات والعمليات والبرامج الثابتة والموظفين المختصين/ المعتمدين والموارد الإلكترونية الأخرى.

هجوم إلكتروني. الاستخدام المتعمد للوسائل الإلكترونية لتعطيل أصول إلكترونية، أو تغييرها أو تدميرها أو الوصول إليها دون إذن.

حدث إلكتروني. أي حدث يمكن ملاحظته في شبكةٍ أو نظام.

واقعة إلكترونية. حدث أو سلسلة أحداث إلكترونية تؤثر سلباً على السلامة الجوية وأمن الطيران وكفاءته و/أو سعته.

تخفيف المخاطر الإلكترونية. ضوابط الأمن التي تهدف إلى تقليل المخاطر الإلكترونية المرتبطة بتهديد أو موطن ضعف إلكتروني معين، مع مراعاة تأثيرها على السلامة الجوية وأمن الطيران وكفاءته و/أو سعته.

تحصين الشبكة الإلكترونية. قدرة الأصول الإلكترونية على الحفاظ على الوظائف الحيوية في ظل ظروف معاكسة أو ضغوط، والتعافي من تلك الظروف المعاكسة.

المخاطر في مجال الأمن الإلكتروني. احتمال حدوث نتائج غير مرغوب فيها ناجمة عن وقوع حدث إلكتروني.

تقييم المخاطر الإلكترونية. عملية مستمرة تقوم على تحديد المخاطر الإلكترونية وتحليلها وتقييمها.

إدارة المخاطر الإلكترونية. عملية مستمرة قائمة على تحديد التهديدات والمخاطر الإلكترونية والتخفيف من حدتها ومعالجتها ورصدها، وفقاً لتقييم المخاطر.

مصفوفة المخاطر الإلكترونية. أداة لترتيب عناصر المخاطر وعرضها (احتمالية الحدوث، والتهديد الأثر/ التبعات ومواطن الضعف (الهشاشة) والإشارة في نهاية المطاف إلى المخاطر المتبقية.

التهديد الإلكتروني. أي حدث إلكتروني محتمل من شأنه أن يؤثر سلباً على السلامة الجوية وأمن الطيران وكفاءته و/أو سعته.

اضطراب /تعطيل. حدث إلكتروني، متوقع أو غير متوقع، يتسبب في انحراف سلبي غير مخطط له عن العمليات العادية.

السلامة. اتسام الأصل بالدقة والاستيفاء، بما يؤكد ماهية هذا الأصل.

الموثوقية. قدرة الأصل على أن يؤدي الوظيفة المطلوبة، بالمستوى المتوقع، في ظل ظروف محددة، دون تعطل، وذلك طوال فترة زمنية محددة.

الشدة. مؤشر نوعي لحجم التأثير السلبي الناتج عن تهديد ما.

الجهة القائمة بالتهديد (أو الجهة المهدِّدة). جهة مسؤولة، بشكل جزئي أو كامل، عن واقعة ما تؤثر أو يُحتمل أن تؤثر على مؤسسة ما أو نظام ما.

الفصل الثاني

منهجية إضافة عنصر إدارة المخاطر الإلكترونية
إلى أُطر إدارة مخاطر الطيران

ملاحظة ١ – في هذا الفصل، تشير وظائف الطيران إلى الوظائف في تخصص (تخصصات) الطيران المختلفة حيث تُدرج إدارة المخاطر الإلكترونية في عملياتها الخاصة بإدارة المخاطر، أي سلامة الطيران و/أو أمن الطيران و/أو كفاءة الملاحة الجوية و/أو سعة الملاحة الجوية. وفي السياق نفسه، فإن وظائف الطيران الحرجة هي الوظائف التي تُعتبر حاسمة بالنسبة لتخصص (تخصصات) الطيران المعنية.

ملاحظة ٢ – في هذا الفصل، يُقصد بمهنيي إدارة مخاطر الطيران مهنيي سلامة الطيران وأمن الطيران وكفاءة الملاحة الجوية و/أو مهنيي إدارة مخاطر السعة، وتشير عمليات إدارة مخاطر الطيران إلى عمليات إدارة المخاطر في تخصص (تخصصات) الطيران المعني(ة).

٢–١ الأهداف

٢–١–١ يدعم هذا الفصل الدول والجهات المعنية في عمليات إدارة المخاطر، بدءاً من تحديد المخاطر وحتى معالجة المخاطر ومراجعتها، من خلال التوصية باتباع منهجية عامة لإضافة عنصر تقييم المخاطر الإلكترونية وإدارتها إلى أُطر إدارة المخاطر القائمة بالفعل في مجال سلامة الطيران وأمنه وكفاءة الملاحة الجوية وسعتها.

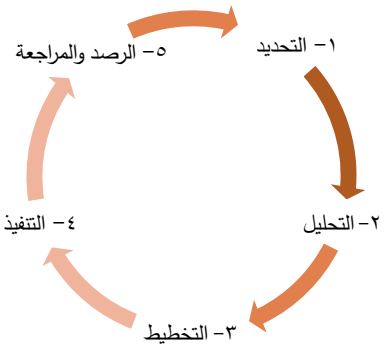
ملاحظة ١ – في حين أن المنهجية تتناول إضافة عنصر إدارة المخاطر الإلكترونية إلى تقييمات سلامة الطيران وأمنه وكفاءة الملاحة الجوية وسعتها، من الممكن تطويع المنهجية بحيث يمكن تطبيقها على أي تخصص آخر في مجال الطيران المدني (مثل إدارة مخاطر الأعمال التجارية).

ملاحظة ٢ – قبل تطبيق المنهجية الواردة في هذا الفصل، قد ترغب الدول والجهات المعنية في النظر في المجالات التي تعترف فيها السلطات المختصة عادةً بمنهجيات تقييم المخاطر القائمة كوسيلة مقبولة للامتثال للاشتراطات التنظيمية في قطاع الطيران لديها، مثل تقييمات المخاطر المتعلقة بترخيص الطائرات.

٢–١–٢ ويتناول هذا الفصل مهنيي سلامة الطيران وأمن الطيران والملاحة الجوية ومهنيي إدارة المخاطر الإلكترونية الذين يجب أن يعملوا بشكل تعاوني لإضافة عنصر إدارة المخاطر الإلكترونية إلى أُطر إدارة مخاطر الطيران الخاصة بكل منهم في مختلف تخصصات الطيران المدني.

٢-٢ لمحة عامة

٢-٢-١ تتبع المنهجية المقدَّمة في هذه الوثيقة المفاهيم العامة لدورة إدارة المخاطر الفعالة على النحو المبين في الشكل ١.



الشكل ١- دورة إدارة المخاطر

٢-٢-٢ تستند المنهجية إلى المواد الإرشادية الحالية عن تقييم المخاطر الصادرة عن الإيكاو، وهي "دليل إدارة السلامة" (Doc 9859) و"بيان سياق المخاطر العالمية لأمن الطيران" (Doc 10108 – وثيقة مقيَّدة التوزيع). كما تراعي المنهجية عمل أفرقة خبراء الإيكاو المختلفة، بالإضافة إلى مساهمات فريق التنسيق المشترك بين الناتو ويوروكنترول المعني بأمن إدارة الحركة الجوية. وتتماشى المنهجية مع القواعد القياسية الدولية لإدارة المخاطر الإلكترونية (ISO/IEC 27001:2022[٣] ، و ISO 31000:2018[٤] ، و EUROCAE/RTCA ED201A/DO-391[٥] و NIST SP 800-30 Rev.1[٦]).

٢-٢-٣ وسوف يُتيح تطبيق المنهجية على تقييمات مخاطر الطيران على وظائف الطيران الحرجة الحصول على النواتج التالية:

- تقييم محدَّث لمخاطر سلامة الطيران يتضمن تقييم المخاطر الإلكترونية ذات الأهمية؛
- تقييم محدَّث لمخاطر أمن الطيران يتضمن تقييم المخاطر الإلكترونية ذات الأهمية؛
- تقييم محدَّث لمخاطر كفاءة الملاحة الجوية يتضمن تقييم المخاطر الإلكترونية ذات الأهمية؛ و/أو
- تقييم محدَّث لمخاطر سعة الملاحة الجوية يتضمن تقييم المخاطر الإلكترونية ذات الأهمية.

٢-٢-٤ قبل تطبيق المنهجية، من الضروري أن يحدّد المتخصصون في مجال الطيران وظائف الطيران الحرجة في المجال الخاضع للتقييم. ويمكن تحقيق ذلك من خلال إجراء مشاورات ودراسات استقصائية وما إلى ذلك، تأخذ في الاعتبار المتطلبات التنظيمية والقانونية المطبَّقة على الطيران وكذلك البنية التحتية الوطنية الحيوية.

ملاحظة – يتيح تحديد وظائف الطيران الحرجة والبيانات والمعلومات والنُظم الداعمة لها، إلى جانب تطبيق المنهجية، دعم الدول في جهودها الرامية إلى الوفاء بالتزاماتها بموجب "القاعدة القياسية ٤-٩-١ في الملحق السابع عشر" — أمن الطيران[٧].

---

[٣] انظر https://www.iso.org/standard/27001https://www.iso.org/standard/27001

[٤] انظر https://www.iso.org/standard/65694.html https://www.iso.org/standard/65694.html

[٥] انظر https://www.eurocae.net/product/ed-201a-aeronautical-information-system-security-aiss-framework-guidance/ أو https://www.rtca.org/security/https://www.eurocae.net/product/ed-201a-aeronautical-information-system-security-aiss-framework-guidance/https://www.rtca.org/security/

[٦] انظر https://csrc.nist.gov/pubs/sp/800/30/r1/finalhttps://csrc.nist.gov/pubs/sp/800/30/r1/final

[٧] تنطبق ملاحق اتفاقية شيكاغو، بما في ذلك الملحق السابع عشر وقاعدته القياسية ٤-٩-١، على الدول وليس على فرادى تخصصات الطيران، ما

٢-٢-٥ وكما هو مبين في الشكل ٢ أدناه، يجب أن تتضمن المنهجية الخطوات التالية.

➢ **الخطوة ١** – يتم تنفيذ هذه الخطوة من قِبل المتخصصين المعنيين بمخاطر الطيران بالتعاون مع المتخصصين في مجال الإنترنت.

⇦ ابدأ بتقييم مخاطر الطيران الحالية لوظيفة من وظائف الطيران الحرجة.

⇦ سيوفر تقييم مخاطر الطيران ما يلي:

- الحد الأدنى المقبول لمستوى السلامة، ويسمى "مستوى السلامة المستهدف"؛
- مخاطر أمن الطيران المتبقية؛
- الحد الأدنى لمستوى السعة المستهدف؛ و/أو
- الحد الأدنى لمستوى الكفاءة المستهدف.

⇦ حدِّد البيانات والمعلومات والأنظمة التي تدعم وظيفة الطيران الحرجة والتي يمكن لأي تلاعب يحدث فيها أن يؤثر على سلامة الطيران المدني و/أو أمنه و/أو كفاءته و/أو سعته.

ملاحظة:- في حالة تحديد وظيفة طيران حرجة لا ترِد في التقييم الحالي لمخاطر الطيران، ينبغي إجراء تقييم المخاطر المعني واستخدامه في الخطوة (١) في غضون ذلك، يمكن إجراء الخطوة ٢ أدناه لتقييم مخاطر البيانات والمعلومات والأنظمة الداعمة لتلك الوظيفة.

➢ **الخطوة ٢**- يتم تنفيذ هذه الخطوة من قِبل المتخصصين في مجال الإنترنت بالتعاون مع المتخصصين في مخاطر الطيران المعنية.

⇦ تحديد سيناريوهات التهديدات الإلكترونية التي قد تؤثر على البيانات والمعلومات والأنظمة المذكورة أعلاه، وإجراء تقييم للمخاطر الإلكترونية لتلك السيناريوهات.

- وصف سيناريو التهديد، بما في ذلك وسائل وأساليب الهجوم الإلكتروني ونوع الجهة القائمة بالتهديد.
- يجب تقييم الاحتمالية أولاً دون أن تؤخذ في الاعتبار التدابير الاحترازية الحالية. وبهذا الشكل يتم تقييم نوايا الجهة القائمة بالتهديد وقدرتها على تنفيذ سيناريو التهديد. وقد تتضمن هذه الخطوة وصفاً لملف تعريف جهة التهديد وأدواتها وما إلى ذلك، قدر الإمكان.

ملاحظة – ينبغي الاستمرار في رصد التهديدات الإلكترونية التي تم تحديدها، للوقوف على التغيرات في نوايا و/أو قدرات الجهات القائمة بالتهديد.

- يجري تقييم الأثر/التبعات/التأثير من حيث طبيعة ونطاق الهجوم المعني، فيما يتعلق بسلامة الطيران وأمنه وسعة الملاحة الجوية و/أو كفاءة الملاحة الجوية، في ظل أسوأ سيناريو معقول، أو أسوأ السيناريوهات يمكن تصديقه[٨].
- تقييم نقاط الضعف المتبقية في النظام يأخذ في الاعتبار تنفيذ التدابير الاحترازية الحالية.
- الناتج من التقييم أعلاه هو المخاطر الإلكترونية المتبقية. وهو الخطر الإجمالي المتبقي بعد النظر في التدابير الاحترازية الحالية وأخذ احتمالية التهديد وتبعاته في الاعتبار.

ملاحظة ١ – يرد وصف لجداول ترتيب الاحتمالية والتأثير وجداول ترتيب نقاط الضعف المتبقية في القسم التالي.

لم تُخص بالذكر. وتشير القاعدة القياسية ٤-٩-١ إلى "المشغلين أو الهيئات المُشار إليها في البرنامج الوطني لأمن الطيران المدني أو غيره من الوثائق الوطنية في هذا الشأن". وهذه الصيغة تجعل البند ينطبق على جميع تخصّصات الطيران على النحو المحدّد على المستوى الوطني من قِبل كل دولة.

[٨] تستخدم المفردات "الأثر والتأثير والتبعات" دون اختلاف في المعنى في هذه الوثيقة.

ملاحظة ٢– يجب على كل مؤسسة تحديد أهدافها الخاصة بالأمن الإلكتروني ومعايير قبول المخاطر الإلكترونية بناءً على الأُطر التنظيمية والقانونية المعمول بها في مجال الطيران وغير الطيران (مثل السلطة الوطنية للأمن الإلكتروني) والأطر التنظيمية والقانونية، بالإضافة إلى مستويات تحمل المخاطر لديها في وحدها.

➢ **الخطوة ٣** – يجري تنفيذ هذه الخطوة بواسطة متخصصين في مخاطر الطيران.

⇦ قم بتحديث تقييم مخاطر الطيران التي جري تحديدها في الخطوة ١. ستفضي هذه الخطوة إلى النواتج التالية:

- مستوى السلامة المحدّث؛
- مخاطر أمن الطيران المتبقية؛
- مستوى السعة المحدّث؛ و/أو
- مستوى الكفاءة المحدّث.

➢ **الخطوة ٤** – يجري تنفيذ هذه الخطوة من قِبل المتخصصين المعنيين بمخاطر الطيران بالتعاون مع متخصصين في مجال الإنترنت.

⇦ قم بتقييم نواتج تقييم مخاطر الطيران المحدّثة مقابل مستويات المخاطر الأصلية التي تم الحصول عليها في الخطوة ١.

⇦ يجب أن تكون معايير قبول المخاطر محددة مسبقاً من قبل المؤسسة ويجب أن تكون شاملة، بحيث تغطي كحد أدنى تخصصات الطيران المراد تقييمها (سلامة الطيران وأمنه وسعته و/أو كفاءته) وأهداف وغايات الأمن الإلكتروني.

ملاحظة – يجب على كل مؤسسة تحديد معاييرها الخاصة بقبول المخاطر الإلكترونية بناءً على الأُطر التنظيمية والقانونية المعمول بها في مجال الطيران (وأحياناً في غير الطيران)، بالإضافة إلى مستويات تحمل المخاطر لديها هي وحدها.

⇦ عند تقييم النواتج المحدّثة مقابل النواتج الأصلية التي تم الحصول عليها في الخطوة ١، ينبغي أن تُعتَبر المخاطر المحدّثة لتقييم مخاطر الطيران غير مقبولة إذا:

- كان التقييم المحدّث لمخاطر الطيران لا يلبي الأهداف المقبولة (مستويات المخاطر الأصلية) التي تم الحصول عليها في الخطوة ١؛ أو
- كانت المخاطر الإلكترونية المتبقية لا تفي بأهداف الأمن الإلكتروني على صعيد المؤسسة.

⇦ إذا كانت المخاطر المحدّثة غير مقبولة، يجب على المؤسسة التخفيف من المخاطر من خلال إضافة إجراءات احترازية محددة للأمن الإلكتروني حيثما أمكن ومن ثم إعادة تقييم قبول المخاطر.

⇦ وإذا كانت المخاطر لا تزال غير مقبولة حتى بعد تنفيذ التدابير الاحترازية من المخاطر في مجال الأمن الإلكتروني، فيجب على المؤسسة تحديد تدابير احترازية أخرى جديدة وفعّالة وناجعة لتخفيف المخاطر إلى المستويات المقبولة.

ملاحظة.– في حالة وجود تعارض فيما يتعلق بمقبولية المخاطر بين المتخصصين في مجال الطيران وخبراء الانترنت، ينبغي تصعيد القرار إلى المستوى التنفيذي للمؤسسة.

⇦ وفي حال تم التخطيط لاتخاذ تدابير احترازية للتصدي لمخاطر الأمن الإلكتروني، ارجع إلى الخطوة ٣.

⇦ تأكد من أن التدابير الاحترازية الجديدة للأمن الإلكتروني ليس لها أثر سلبي على تقييم مخاطر الطيران. إذا دعا الأمر، اتخذ تدابير على مستوى الطيران أو راجع تدابير الأمن الإلكتروني لمعالجة أي أثر سلبي[٩].

[٩] تشير "تدابير الطيران" إلى تدابير تعالج مسائل سلامة وأمن الطيران، وكفاءة الملاحة الجوية و/أو التدابير التشغيلية المتعلقة بالسعة.

ملاحظة:- من المهم النظر في التأثير المحتمل للتدابير الاحترازية من مخاطر الأمن الإلكتروني على البيانات و/أو المعلومات و/أو الأنظمة الهامة لوظائف الطيران الحرجة الأخرى، إذ إن هذه التدابير قد تؤثر على تلك الوظائف. وإذا تم الكشف عن وجود هذه التأثيرات، فينبغي إجراء تقييم مشترك لمخاطر الطيران والمخاطر الإلكترونية المرتبطة بتلك الوظائف الحرجة.

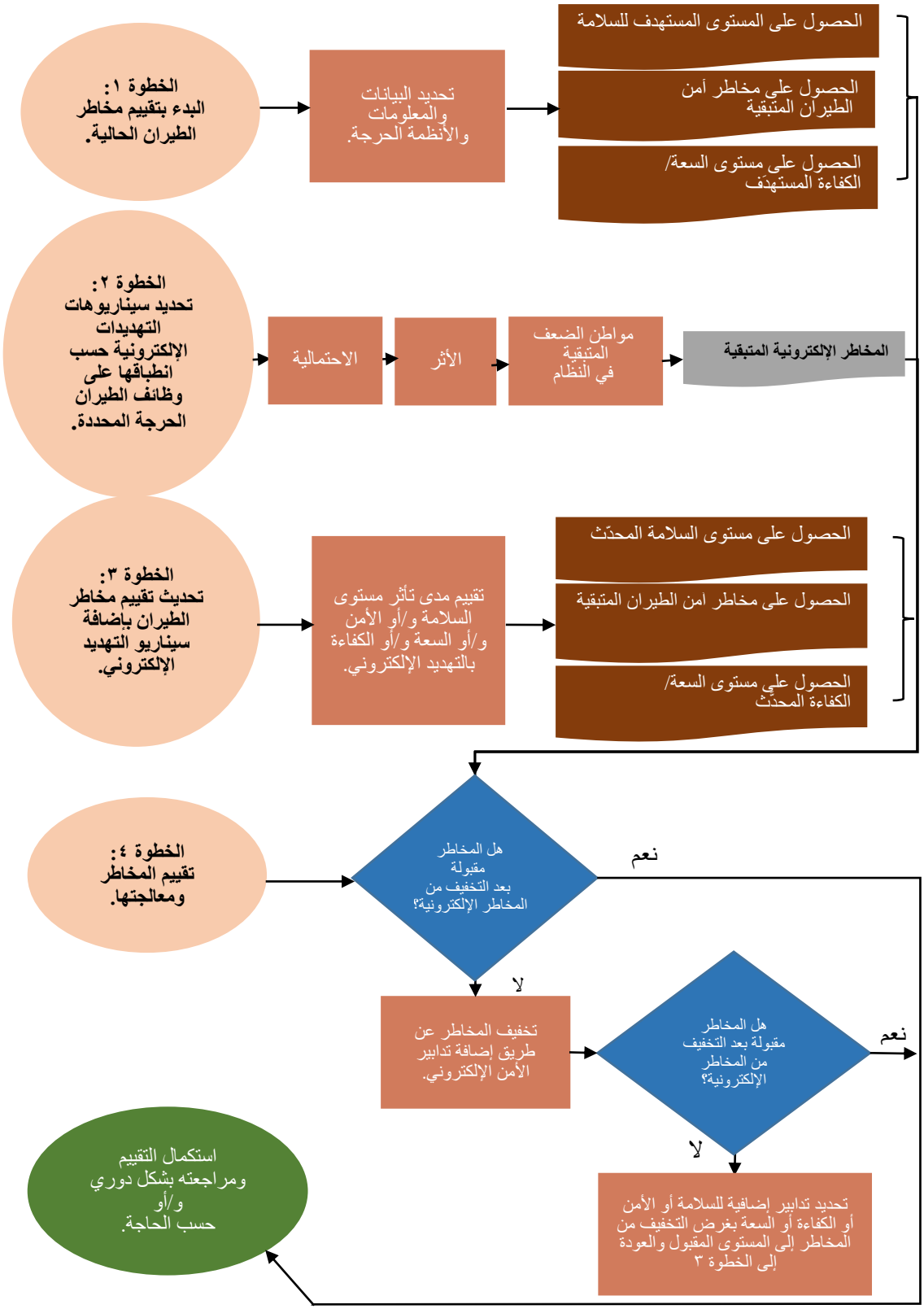
⇦ وينبغي تكرار التقييم للأسباب التالية:

- تطور التهديدات الإلكترونية، مثل سيناريوهات التهديدات الإلكترونية الحالية أو الجديدة التي قد تصبح مع مرور الوقت معقولة، والتغيرات في المعلومات أو المعرفة المستخدمة في التعرف على المخاطر وتحليلها وتصنيفها؛
- التغييرات التي تطرأ على المتطلبات المتعلقة بتقييم المخاطر في المجال (المجالات) التي يجري فيها دمج المخاطر الإلكترونية؛
- التغييرات الوظيفية في وظائف الطيران التي يتم تقييمها؛ و/أو
- التغييرات في تقبّل المخاطر المؤسسية والسياسة التنظيمية المتعلقة بالرقابة والتقييم المستمرّين و/أو تكرار تقييم المخاطر.

٢-٢-٦ ويرِد في المرفقيْن (ألف) و(باء) مثالان لكيفية تطبيق المنهجية. يوضح المثال الأول في **المرفق (ألف)** كيفية إدراج التهديدات الإلكترونية في تقييم مخاطر السلامة الجوية. ويوضح المثال الثاني في **المرفق (باء)** كيف يمكن إدراج التهديدات الإلكترونية في تقييم مخاطر أمن الطيران.

٢-٢-٧ والهدف من هذه الأمثلة هو توضيح أن تقييمات مخاطر الطيران وتقييمات المخاطر الإلكترونية لا يمكن إجراؤها بمعزل عن التهديدات الإلكترونية لعمليات الطيران. **ومن الضروري أن يتفاعل كلا النوعيْن من التقييمات وأن يجري التنسيق والتعاون فيما بينهما من أجل توفير الحماية والمناعة الشاملتيْن للطيران المدني ضد التهديدات والمخاطر الإلكترونية.**

٢-٣ تسلسل خطوات المنهجية وجداول تصنيف مستويات_المخاطر الإلكترونية



الشكل ٢- خريطة تسلسل خطوات منهجية إدارة المخاطر

جداول تصنيف مستويات المخاطر الإلكترونية

٢-٣-١ ترِد جداول تصنيف المستويات المختلفة في هذا القسم باعتبارها إحدى أفضل الممارسات والإرشادات بشأن كيفية بناء مصفوفات تقييم المخاطر الإلكترونية. رغم أنه يُوصى باستخدام هذه الجداول للفهم المتبادل للتهديدات والمخاطر الإلكترونية في سياق تقاسم المعلومات، إلا أن الجداول يمكن تطويعها بما يتماشى مع استراتيجيات إدارة المخاطر الخاصة بالمؤسسات المعنية[١٠].

٢-٣-٢ تُستخدم التصنيفات في هذا القسم لإنتاج تقييمات الفصل الثالث من النسخة مقيَّدة التوزيع من هذه الوثيقة.

٢-٣-٣ وفقاً لهذه المنهجية، هناك خمس مستويات لتصنيف الاحتمالية والأثر ومواطن الضعف **(مرتفع، متوسط مرتفع، متوسط، متوسط منخفض، منخفض)**. ويرتبط كل مستوى بتصنيف وتعريف.

الاحتمالية

٢-٣-٤ والاحتمالية هي إمكانية تحقق التهديد الإلكتروني، مع مراعاة قدرة ونية الجهة الفاعلة المهددة على تنفيذ مثل هذا الهجوم الإلكتروني.

٢-٣-٥ ويجب إجراء تقييم الاحتمالية من قِبل خبراء في الإنترنت، أو على الأقل من قِبل خبراء في مخاطر الطيران ممَّن بمقدورهم الوصول إلى تقارير تحليلات التهديدات الإلكترونية.

الجدول ١ – ترتيب مستويات احتمالية التهديد الإلكتروني

تصنيف الاحتمالية		
مرتفعة	٥	سيناريو معقول جداً، بالنظر إلى حدوث هجوم فعلي من هذا النوع في السنوات القليلة الماضية، أو وجود دليل قوي على توفّر القدرة والقصد.
متوسطة – مرتفعة	٤	سيناريو معقول بوضوح بالنظر إلى وجود أمثلة حديثة نسبياً أو دليل على تخطيط سابق لتنفيذ هجوم أو عمليات استطلاع مُعادية.
متوسّطة	٣	سيناريو معقول في الأساس، بالنظر إلى وجود بعض الأدلة على توفر القصد والقدرة، وربما وجود بعض الأمثلة.
متوسّطة-منخفضة	٢	سيناريو لا توجد له أمثلة حديثة العهد أو أي أمثلة على الإطلاق، مع بعض الأدلة على وجود القصد، ولكن بمنهجية غير متطورة ظاهرياً بما فيه الكفاية لتنفيذ سيناريو هجوم ناجح أو قد يُستبدل السيناريو بأشكال هجومية أُخرى.
منخفضة	١	سيناريو معقول نظرياً ولكن دون وجود أمثلة، ومع وجود نية نظرية ولكن دون توفر قدرة ظاهرية.

[١٠] للحصول على معلومات إضافية عن تقاسم المعلومات الإلكترونية. انظر المواد الإرشادية المتعلقة بتبادل المعلومات الإلكترونية على الرابط التالي: https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspxhttps://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx

الأثر/التبعات/التأثير

٢-٦-٣ الأثر هو ناتج قياس تبعات الحادث الإلكتروني، بعبارات نوعية، على الأصول المذكورة في وصف سيناريو التهديد.

٢-٧-٣ ويجب إجراء تقييم الأثر من قِبل خبراء طيران مختصين بوظيفة الطيران محل التحليل.

٢-٨-٣ الآثار المترتبة على سلامة الطيران وأمن الطيران مستقاة من مواد الإيكاو الإرشادية بشأن تقييم مخاطر سلامة وأمن الطيران وتقييم مخاطر أمن الطيران، على التوالي، في "دليل إدارة السلامة" (Doc 9859) و"بيان سياق المخاطر العالمية لأمن الطيران" (Doc 10108– وثيقة مقيّدة التوزيع). الآثار المترتبة على سعة الملاحة الجوية وكفاءتها تم إعدادها لهذه الوثيقة.

الجدول ٢- ترتيب مستويات آثر التهديد الإلكتروني

تصنيف الاثر/التبعات/التأثير[١١]			
	سلامة الطيران[١٢]	**أمن الطيران[١٣]**	**سعة و/أو كفاءة الملاحة الجوية**
مرتفعة = ٥	**كارثية:** - تحطم الطائرة	- مئات الوفيات - مليارات الدولارات الأمريكية - اضطراب حاد في الخدمات وانهيار الثقة في منظومة الطيران	- اضطراب خطير في سعة و/أو كفاءة الملاحة الجوية. - انقطاع واسع النطاق أو تعطل كامل للأنظمة التشغيلية الرئيسية، يؤثر بشدة على إدارة الحركة الجوية أو عمليات المطارات[١٤] أو عمليات شركات الطيران.[١٥] - تزايد كبير في حالات تأخير أو إلغاء الرحلات الجوية، على نحو يشكل مخاطر تشغيلية كبيرة على منظومة الطيران والقدرة على تشغيل الطائرات.
متوسطة- مرتفعة = ٤	**جسيمة:** - إصابات خطيرة - أضرار رئيسية	- بعض آثار التبعات المرتفعة، ولكن ليس كلها	- اضطراب خطير في سعة و/أو كفاءة الملاحة الجوية.

[١١] جدول تصنيف الأثر/التبعات/التأثير يصف الآثار فيما يتعلق بكل تخصص من تخصصات الطيران التي تُستخدم فيها المنهجية. الأعمدة مستقلة عن بعضها البعض بناءً على كل تخصص من تخصصات الطيران، وينبغي قراءة المعدلات المذكورة في العمود الأول مع العمود الخاص بتخصص الطيران الذي يُدرج فيه تقييم المخاطر الإلكترونية.

[١٢] أثر/تبعات/تأثير سلامة الطيران مأخوذة من الطبعة الرابعة من "دليل إدارة السلامة" (Doc 9859).

[١٣] تم استخلاص أثر/تبعات/تأثير أمن الطيران من الطبعة الثالثة من "بيان سياق المخاطر العالمية لأمن الطيران" (Doc 10108 – وثيقة مقيّدة التوزيع).

[١٤] تشمل عمليات المطارات في هذا السياق جميع خدمات المطار الضرورية لوصول الطائرات ومغادرتها وسيرها في الممرات، بالإضافة إلى إدارة الركّاب، بما في ذلك على سبيل المثال لا الحصر الوصول إلى البوابات، وتوافر الخدمات الأمنية، وتفتيش المدرج، ومناولة الأمتعة، والوقود، وإزالة الجليد، وخدمات التموين، وإضاءة المطار، والخدمات الأخرى اللازمة.

[١٥] تشمل عمليات الطيران في هذا السياق جميع الجوانب التي تؤثّر على القدرة على تشغيل الطائرات بطريقة فعّالة، بما في ذلك المعلومات المقدمة لأطقم القيادة، وصيانة الطائرات، وعمليات الطيران، والأرصاد الجوية، وتوافر النُظم العالمية للملاحة بالأقمار الصناعية مقابل الملاحة غير الدقيقة والاقتراب غير الدقيق، ومعلومات الطيران، وما إلى ذلك.

	- انكماش كبير في هوامش السلامة لدرجة تتعذر معها الثقة في أن ينجز المشغِّلون مهامهم بدقة وبصورة تامة.		- انقطاعات أو أعطال ممتدة في الأنظمة التشغيلية الرئيسية، على نحو يؤثر على الخدمات الأساسية والقدرة على تشغيل الطائرات. - تزايد كبير في حالات تأخير تدفقات الحركة الجوية أو عمليات المطار أو عمليات شركات الطيران، بما يؤدي إلى الاكتظاظ.
متوسّطة = ٣	**كبيرة:** - أشخاص لحقت بهم إصابات - واقعة خطيرة - انخفاض كبير في هوامش السلامة، وانخفاض في قدرة العاملين على التعامل مع ظروف التشغيل العسيرة نتيجة زيادة عبء العمل أو نتيجة لظروف تحد من كفاءتهم؛	- عشرات الوفيات - مئات ملايين الدولارات الأمريكية - اضطراب حاد في الخدمات وانهيار الثقة في منظومة الطيران	- اضطراب ملحوظ في سعة و/أو كفاءة الملاحة الجوية. - انقطاع جزئي أو أعطال في الأنظمة التشغيلية الرئيسية، بما يؤثر على خدمات متعددة. - حالات تأخير متوسطة الشدة في تدفقات الحركة الجوية أو تأثير معتدل على عمليات المطار أو عمليات شركات الطيران، مما يتطلب تنسيقاً وموارد إضافية لإدارتها.
متوسّطة–منخفضة = ٢	**محدودة:** - إزعاج وقيود تشغيلية - استخدام إجراءات الطوارئ - واقعة صغيرة.	- بعض آثار التبعات المتوسطة، ولكن ليس كلها	- اضطراب محدود في سعة و/أو كفاءة الملاحة الجوية. - حادثة محدودة لا تؤثر إلا على أنظمة أو خدمات محددة. - حالات تأخير طفيفة أو أوجه قصور صغيرة في تدفقات الحركة الجوية أو في عمليات المطار أو عمليات شركات الطيران، يمكن التعامل معها في إطار الإجراءات التشغيلية العادية.
منخفضة = ١	**ضئيلة:** - احتمال وقوع بعض الإصابات - تبعات محدودة	- احتمال وقوع بعض الوفيات والإصابات - بعض الآثار الاقتصادية - بعض الاضطراب في الخدمات وفي الثقة في منظومة الطيران	- اضطراب محدود في سعة و/أو كفاءة الملاحة الجوية. - حادثة معزولة ذات تأثير محدود للغاية على العمليات بشكل عام. - تأخير أو تعطيل محدود للغاية في تدفق الحركة الجوية، وتأثير محدود للغاية على عمليات المطار أو عمليات شركات الطيران.

مواطن الضعف (الهشاشة)

٢-٣-٩ تُقاس مواطن الضعف من حيث الكيف. وهي تصف فعالية التدابير الحالية في التخفيف من تبعات سيناريو التهديد الإلكتروني على الأصول المعنية.

٢-٣-١٠ ينبغي إجراء تقييم الثغرات الأمنية بالتعاون بين خبراء الطيران وخبراء الإنترنت الذين يمكنهم تحليل وظيفة الطيران الحرجة المعنية وتقييم كيفية استغلال الجهات القائمة بالتهديد لنقاط الضعف الإلكترونية.

الجدول ٣ – ترتيب درجات مواطن الضعف إزاء التهديد الإلكتروني

ترتيب درجات مواطن الضعف		
مرتفعة	١	لا توجد تدابير احترازية نافذة وذلك إما بسبب عدم وجود شروط أو لعدم وجود إجراءات فعّالة واقعية.
متوسطة – مرتفعة	٠,٨	نطاق التدابير الاحترازية محدود والمجالات وبعض الجوانب الهامة للمخاطر ليست مشمولة بأحكام الملحق السابع عشر أو بتدابير نافذة.
متوسّطة	٠,٦	هناك خصائص لكل من المستوى **متوسط– مرتفع** والمستوى **متوسط–منخفض**.
متوسّطة–منخفضة	٠,٤	متوسّطة – منخفضة أي أن التدابير الاحترازية مطبقة عموماً، ولكنها قد تكون غير مكتملة النضج أو محدودة الفعالية. على سبيل المثال، قد تكون هناك أدلة خاصة بأمن المعلومات وضعتها الإيكاو في جميع المجالات والجوانب، ولكن من الناحية العملية يمكن تطوير هذه الأدلة أو تنفيذها بشكل أفضل.
منخفضة	٠,٢	توجد متطلبات واضحة، ويجري على نطاق واسع استخدام تدابير احترازية تعتبر فعّالة بشكل عام.

مثال لعملية تقييم المخاطر الإلكترونية

الجدول ٤ – مصفوفات ترتيب مستويات المخاطر الإلكترونية وتقييمها

مصفوفة تقييم المخاطر الإلكترونية				
سيناريو التهديد الإلكتروني	الاحتمالية X	الأثر X	مواطن الضعف	= المخاطر المتبقية
الجهة القائمة بالتهديد تستخدم هجوماً إلكترونياً للتأثير على أحد أصول الطيران التي تديرها إحدى الجهات المعنية في مجال الطيران من خلال استغلال ثغرة أمنية.	متوسّطة ٣	متوسط–مرتفع ٤	متوسط – مرتفع ٠,٨	٩,٦

مصفوفة تقييم المخاطر الإلكترونية	
معدلات المخاطر	مستويات المخاطر
٢٥–٢٠	مرتفعة
٢٠–١٥	متوسطة – مرتفعة
١٥–١٠	متوسّطة
١٠–٥	متوسّطة–منخفضة
٥–٠	منخفضة

المرفقات

المرفق (ألف)

مثالٌ لتطبيق المنهجية
في إدارة مخاطر سلامة الطيران

افتراضات ولمحة عامة

يوضّح هذا المثال إدراج تقييم المخاطر الإلكترونية في تقييم مخاطر سلامة الطيران، باستخدام سيناريو تهديد افتراضي يجري تقييمه من قِبل أحد مزودي خدمات الملاحة الجوية.

الافتراضات:

- قام مقدم خدمة الملاحة الجوية بالفعل بتقدير مخاطر السلامة في السياق المعني وتقييمها والتخفيف من حدتها باستخدام تحليل شجرة الأعطال (FTA)[١٦].
- وقد حدد خبراء سلامة الطيران الاتصالات الجوية–الأرضية كإحدى وظائف الطيران الحرجة.
- ولأغراض التبسيط، يُفترض أن التهديد الإلكتروني الخاضع للتقييم يؤثر فقط على السلامة (لا تأثير على كفاءة الملاحة الجوية وسعتها).
- ويستخدم مقدم خدمات الملاحة الجوية نفس جداول ترتيب المستويات الخاصة بالاحتمالية والأثر ومواطن الضعف المستخدمة في هذه الوثيقة.
- لكن نظام تقدير مستويات التصنيف المستعمل لتقييم المخاطر الإلكترونية يستخدم قيماً مختلفة عن تلك الواردة في الفقرة ٣–٣–١٧ حيث يقتصر نطاق التقييم في المثال الذي بين أيدينا على الأنظمة الأرضية والبيانات المتعلقة بالاتصال بين المراقب والطيار عبر وصلة البيانات.
- ولأغراض التبسيط، يُفترض في سيناريو التهديد الإلكتروني أدناه، كما هو موضح في الشكل ٣، أن تأثير التهديد الإلكتروني يقتصر على رسائل الاتصال بين المراقب والطيار عبر وصلة البيانات المتعلقة بتصريح مستوى الطيران.

[١٦] تحليل شجرة الأعطال: هو أداة تدعم تحديد وتحليل الظروف والعوامل التي تسبّب أو تساهم في وقوع حدث محدد غير مرغوب فيه، وهو حدث عادةً ما يؤثر بشكل كبير على سلامة النظام أو أدائه أو اقتصادياته أو غير ذلك من الخصائص الضرورية. ويجري تطبيق تحليل شجرة الأعطال بشكل مكثّف على تقييم سلامة الأنظمة.
ويمكن العثور على إرشادات بشأن استخدام تحليل شجرة الأعطال في الجزء الرابع من أداة منهجية تقييم السلامة الإلكترونية (eSAM) الخاصة بيوروكونترول https://www.eurocontrol.int/tool/safety-assessment-methodology ، ضمن محتويات الجزء الرابع، المرفق (كاف): "مواد إرشادية لتحليل شجرة الأعطال" Fault Tree Analysis Guidance Material. https://www.eurocontrol.int/tool/safety-assessment-methodology

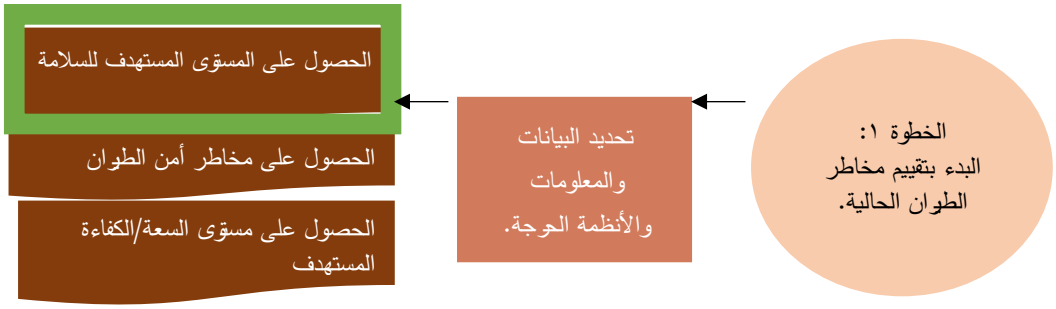
سيناريو التهديد الإلكتروني:

- تعاون خبراء سلامة الطيران مع خبراء في مجال الإنترنت لمراجعة تقييمات مخاطر السلامة الحالية لوظيفة الاتصالات الجوية–الأرضية واختاروا نظام وصلة البيانات كنظام وكمعلومات تدعم الوظيفة الحرجة التي ينبغي تقييمها لغرض الوقوف على المخاطر الإلكترونية.
- وقد أنتج خبراء سلامة الطيران تقييماً لمخاطر السلامة الحالية لحدث من أحداث السلامة البارزة يتعلق "بتسليمٍ زائف غير مكتشف لرسالة واحدة أو عدة رسائل مستخدَمة لإصدار التصاريح (مستوى الطيران المسموح به والاتجاه والسرعة) إلى طائرة واحدة أو عدة طائرات".
- وتوصّل خبراء الإنترنت، من خلال المناقشات مع خبراء سلامة الطيران، إلى أن "العبث بالبيانات في رسالة وصلة البيانات المرسلة من مراقب الحركة الجوية إلى الطيار" يُعد سيناريو لتهديد إلكتروني يجب تقييمه وإدراجه في تقييم مخاطر سلامة الطيران المذكور أعلاه.
- ويغطي السيناريو الذي يجري تقييمه في هذا المثال التلاعب المتعمد بالبيانات في رسالة وصلة البيانات، حيث تم التلاعب بالرسالة الأصلية (المتعلقة بتصريح مستوى الطيران) المرسَلة من مراقب الحركة الجوية إلى الطيار (تضمّنت الرسالة مستوى طيران خاطئ عمداً) من قِبل جهة خبيثة قبل إرسالها إلى الطائرة.
- وللتبسيط، فإن وسيلة الهجوم قيد النظر موجودة فقط على الجزء الأرضي من البنية التحتية لمحطة وصلة البيانات: المرافق الأرضية لمقدمي خدمة الملاحة الجوي (الشبكة الداخلية أو الخوادم)، أو صادر عن الشبكة الأرضية لمزود خدمة الاتصال، أو من الشبكة المحلية والخوادم الخاصة بمحطة الاتصال الجوي – الأرضي، أي أن المثال يستثني سُبل الهجوم الأخرى مثل الاتصال الجوي الأرضي لرسائل وصلة البيانات. ومن خلال الاستعانة بمثال تصنيف التهديدات الإلكترونية في المرفق (جيم) (يُرجى الرجوع إلى النسخة مقيَّدة التوزيع من هذه الوثيقة). يمكن تصنيف هذا التهديد الإلكتروني على النحو التالي:
  - المجال: مقدم خدمات ملاحة جوية.
  - الوظيفة: الاتصالات، والملاحة والاستطلاع.
  - الوظيفة الفرعية: الاتصالات.
  - التهديد الإلكتروني: التحريف (تعديل محتوى الرسالة).

الشكل ٣ – التهديد: العبث بالبيانات

(ملاحظة — الشكل ٤ في النسخة مقيَّدة التوزيع)

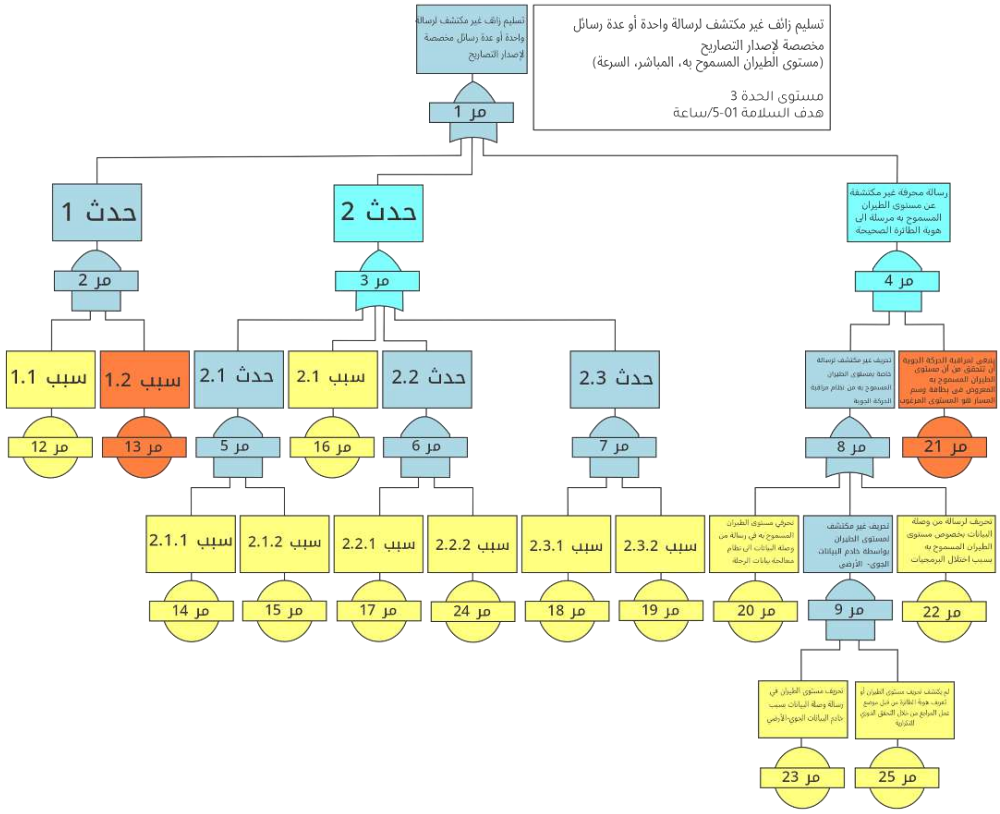
تطبيق المنهجية خطوة بخطوة:



- تعاون خبراء سلامة الطيران مع خبراء إلكترونيين لمراجعة تقييمات مخاطر السلامة الحالية لوظيفة الاتصالات الجوية–الأرضية وحددوا نظام وصلة البيانات كنظام وكمعلومات تدعم الوظيفة الحرجة التي ينبغي تقييمها في إطار المخاطر الإلكترونية.
- وأنتج خبراء سلامة الطيران مخطط شجرة أعطال السلامة الأصلي، بدون الأسباب الإلكترونية[١٧]. الحدث البارز المتعلق بسيناريو التهديد الإلكتروني لوصلة البيانات قيد النظر هو "تسليم زائف غير مكتشَف لرسالة واحدة أو عدة رسائل تُستخدم لإصدار التصاريح لطائرة أو عدة طائرات".
- **مستوى السلامة المستهدف للحدث البارز "لا يزيد عن (٨١٠–٥) وإقعة في كل ساعة طيران".**

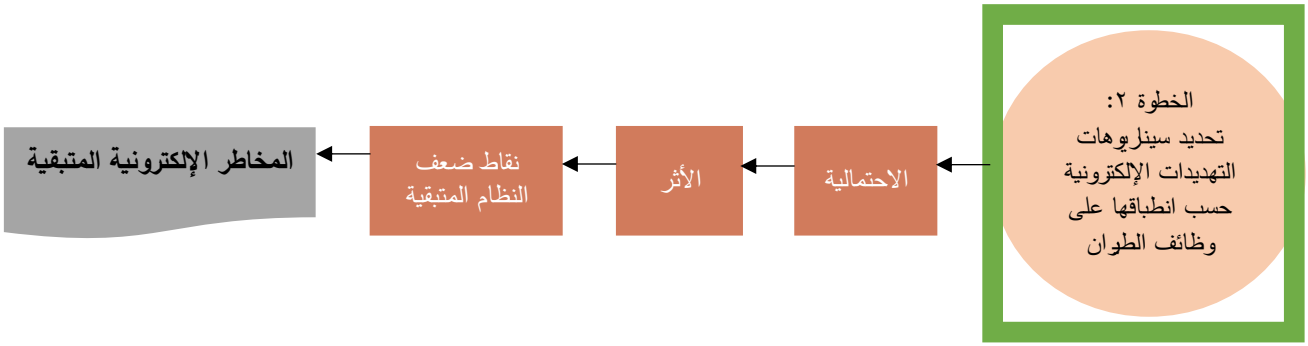
[١٧] المختصرات في مخطط شجرة الأعطال:

- AGDP: معالج رابط البيانات الجوي–الأرضي، خادم البيانات الجوي–الأرضي
- CFL: مستوى الطيران المسموح به
- CWP: موضع عمل المراجع (الواجهة البينية بين الإنسان والآلة)
- FDPS: نظام معالجة بيانات الرحلة



الشكل ٤ – مخطط شجرة الأعطال الأصلية

(ملاحظة — الشكل ٥ في النسخة مقيَّدة التوزيع)



- توصّل خبراء الإنترنت، من خلال المناقشات مع خبراء سلامة الطيران، إلى أن "العبث بالبيانات في رسالة وصلة البيانات المرسلة من مراقب الحركة الجوية إلى الطيار" يُعد سيناريو لتهديد إلكتروني معقول يجب تقييمه وإدماجه في تقييم مخاطر سلامة الطيران المذكور أعلاه.
- وقد تم إجراء تقييم المخاطر الإلكترونية من قِبل خبراء إنترنت تابعين لمقدم خدمات الملاحة الجوية بالتعاون مع خبراء السلامة. ويمتلك خبراء الانترنت معرفة بالأساليب الشائعة ونواقل الهجوم للتهديدات الإلكترونية بينما يمتلك خبراء السلامة معرفة ببنية النظام.

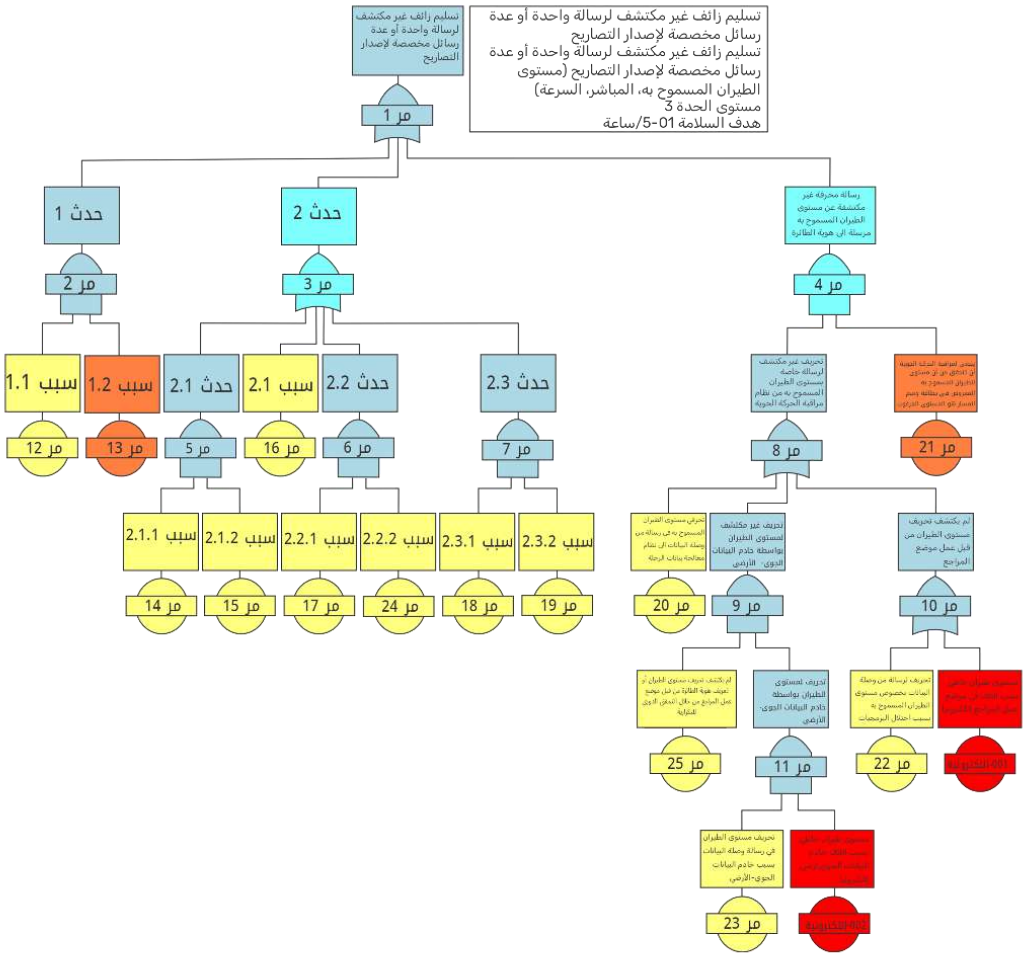
وتم توسيع مكونات تقييم المخاطر الإلكترونية في الخطوة ٢ لتشمل الخطوات التالية:

وتم اتخاذ الخطوات التالية لإجراء تقييم المخاطر الإلكترونية توطئة لبناء مصفوفة المخاطر الإلكترونية.

⇦ **الاحتمالية:**

- بالنسبة للاحتمالية غالباً ما يستخدم خبراء السلامة إمكانية الحدوث (مثل عدد الحوادث لكل ساعة طيران). أيضاً، عند استخدام أشجار الأعطال، يستخدم بعض الخبراء "المسافة" من الحدث البارز في شجرة الأعطال لتقدير الاحتمالية (مثلاً كلما ابتعد عن الحدث البارز، قلَّ احتمال تأثيره على الحدث البارز من حيث تغيير مستوى السلامة المستهدف). ومن ناحية أخرى، غالباً ما يستخدم خبراء الإنترنت جداول احتمالات ذات قيم متفرِّدة (مثل الجدول ١ في الفصل الثاني). والهدف من هذا العمل المشترك بين الخبراء هو مواءمة فهم مكونات المخاطر المختلفة.
- وعلى هذا النحو، في هذا المثال، فإن إدراج التهديد الإلكتروني في شجرة الأعطال (العناصر الحمراء) يسهّل تقدير احتمالية تحقق التهديد الإلكتروني من حيث القدرة والقصد من وضع التهديد الإلكتروني موضع التنفيذ والقصد من التهديد الإلكتروني[١٨].

[١٨] في التقييم الكامل للمخاطر الإلكترونية، يمكن إضافة العديد من نواقل الهجوم إلى المخطط الأصلي، حيث لا يتضمن المثال المذكور سوى وسيلتي هجوم محتملتيْن فقط، وذلك لأغراض التبسيط.



الشكل ٥ – مخطط شجرة الأعطال المحدَّثة

(ملاحظة — الشكل ٦ في النسخة مقيَّدة التوزيع)

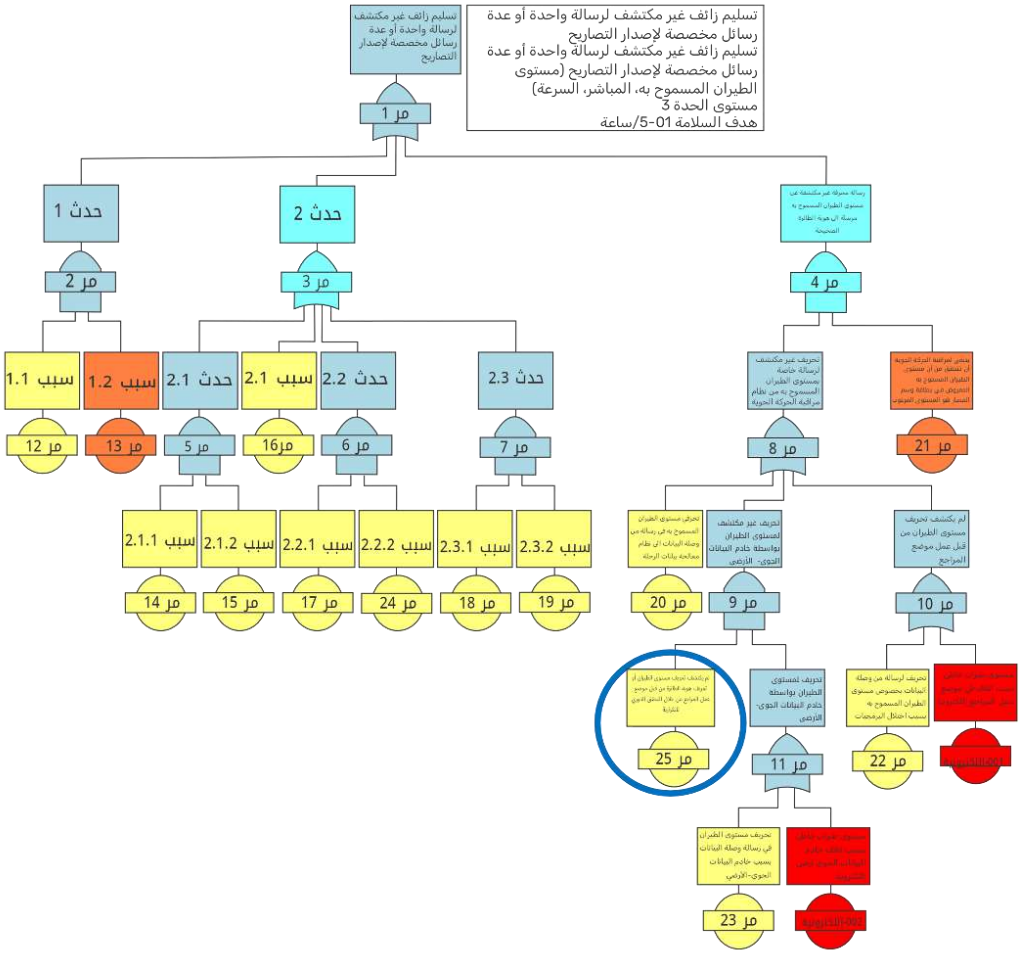
- تم تحديد احتمالية التهديد الإلكتروني عند الدرجة ٢ التي تعني مستوى **متوسط – منخفض** (أي سيناريو لا توجد له أمثلة حديثة العهد أو أي أمثلة على الإطلاق، مع بعض الأدلة على وجود القصد، ولكن بمنهجية غير متطورة ظاهرياً بما فيه الكفاية لتنفيذ سيناريو هجوم ناجح أو قد يُستبدل السيناريو بأشكال هجومية أُخرى).

⇦ **الأثر/التبعات/التأثير:**

- ينطوي تقدير الأثر على تقييم سيناريو معقول لأسوأ الحالات، وهو ما يعني في هذه الحالة أن الهجوم الإلكتروني كان ناجحاً وأنه لم يتسنَّ منع وقوع الحدث البارز. وبناء عليه، يفترض تقييم الأثر أعلى درجة ممكنة من الشدة للحدث البارز قبل إضافة التهديد الإلكتروني، وهو ما يعني أثراً بمستوىً **متوسط** (آثار جسيمة على السلامة: "حادث خطير يصحبه انخفاض في قدرة الموظفين التشغيليين على التعامل مع ظروف التشغيل المعاكسة نتيجة لزيادة عبء العمل أو نتيجة لظروف تضعف كفاءتهم").

⇦ **مواطن الضعف:**

- يُجرى تقييم مواطن الضعف مع مراعاة التدابير الاحترازية الحالية.
- وفي هذا الصدد، يشير تحليل شجرة الأعطال إلى أنه تم إجراء التحقق الدوري للتكرارية (CRC) لرسالة وصلة البيانات بين المراقب والطيار[١٩]. وبناء عليه، يُؤخذ ذلك في الاعتبار بالإضافة إلى التدابير المتعلقة بأمن تكنولوجيا المعلومات (حماية الأنظمة والخوادم) وأمن الطيران (التحريات الشخصية ومراقبة الدخول).



الشكل ٦ – مخطط شجرة الأعطال المحَّدثة (مع الدائرة)

(ملاحظة — الشكل ٧ في النسخة مقيَّدة التوزيع)

- يدرك خبراء الإنترنت أن التحقق الدوري للتكرارية يستخدم بشكل أساسي للكشف عن الأخطاء غير المقصودة في البيانات. ولا يُعتبر التحقق الدوري للتكرارية فعالا ضد التداخلات المتعمدة لأن المهاجم قادر على تغيير البصمة الرقمية للتحقق الدوري للتكرارية بموازاة التغيير في الرسالة، وبالتالي، فإن استنتاج خبراء الإنترنت هو أن الضوابط الإلكترونية الحالية قد لا تكون كافية للتخفيف من المخاطر.

[١٩] يُعرّف التحقق الدوري للتكرارية بأنه "طريقة لضمان عدم تغيير البيانات بعد إرسالها عبر اتصال ما". المصدر: NIST SP800-72

- إلى جانب ذلك، أدى تقييم مواطن الضعف إلى استنتاج مفاده أن أي هجوم إلكتروني خارجي سيكون من الصعب إلى حد ما إعداده وتنفيذه. وتتمتع شبكات وأنظمة الاتصالات الخاصة بمقدم خدمات الملاحة الجوية بالحماية الكافية ضد الهجمات الخارجية، وقد طبقت المؤسسة قدرات كافية للمراقبة والكشف. وقد يكون تنظيم الهجوم الداخلي (التهديد الداخلي) أسهل نسبياً نظراً لأن تدابير الأمن المادي المطبقة كافية أيضاً (مراقبة الدخول إلى الغرف المقيدة والتحريات الشخصية بشأن الموظفين الذين يمكنهم الوصول إلى تلك المناطق).
- وبناءً على ذلك، تُمنح مواطن الضعف تقييماً بمستوى **متوسط–مرتفع** (٠,٨).

⇦ **المخاطر الإلكترونية المتبقية:**

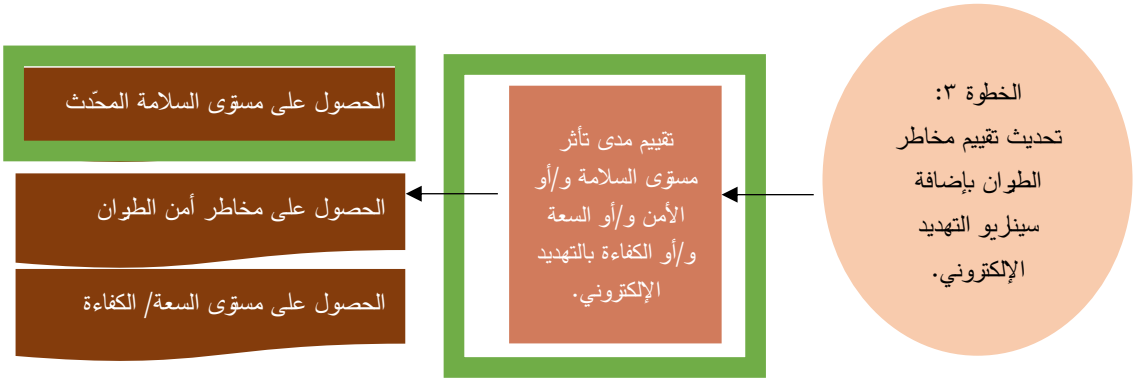
- يمكن الآن حساب المخاطر الإلكترونية المتبقية من خلال ضرب العلامات المحرزة على صعيد الاحتمالية والتأثير ومواطن الضعف: ٢ × ٣ × ٠,٨ = ٤,٨.

⇦ وقد تم تقريب العلامة المحرزة للمخاطر الإلكترونية المتبقية البالغة ٤,٨ إلى ٥ حيث اعتبرها الخبراء أقرب إلى المستوى **المتوسط–منخفض** منها إلى المستوى **المنخفض**.

ومن ثم تصبح مصفوفة المخاطر الإلكترونية بعد ذلك على النحو التالي:

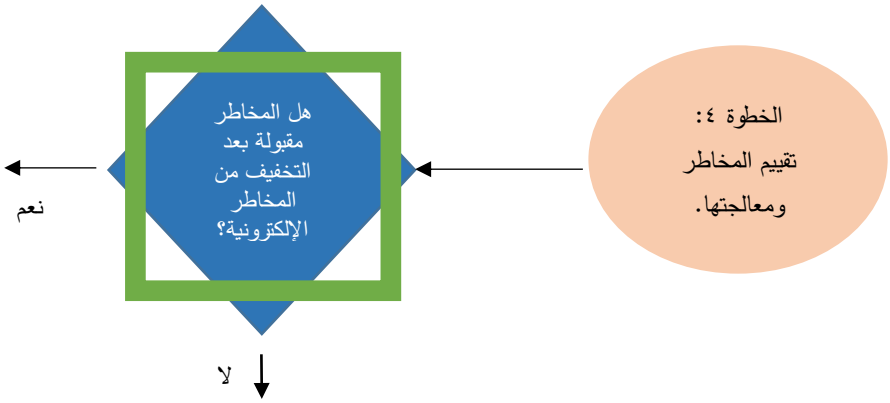
مصفوفة المخاطر الإلكترونية

السيناريو	الاحتمالية	الأثر	التدابير الاحترازية	مواطن الضعف	المخاطر المتبقية
متسلل يعبث بالحمولة الإيرادية للبيانات في رسالة وصلة بيانات مرسلة من مراقب جوي إلى طيار.	٢ **متوسّط–منخفض** سيناريو لا توجد له أمثلة حديثة العهد أو أي أمثلة على الإطلاق، مع بعض الأدلة على وجود القصد، ولكن بمنهجية غير متطورة ظاهرياً بما فيه الكفاية لتنفيذ سيناريو هجوم ناجح أو قد يُستبدل السيناريو بأشكال هجومية أُخرى.	٣ **كبير:** حدث بارز في مجال السلامة: تسليم زائف غير مكتشف لرسالة واحدة أو عدة رسائل مستخدمة لإصدار التصاريح.	**التحقق الدوري للتكرارية** تم بالفعل تنفيذ المراقبة وقدرات اكتشاف المتسللين. اتخاذ تدابير الأمن المتعلقة بتكنولوجيا المعلومات مراقبة الدخول المادي والتحريات الشخصية	٠.٨ **متوسط – مرتفع** لا يُعد التحقق الدوري للتكرارية أداة مناسبة للكشف عن العبث الخبيث بالمعلومات بالنظر إلى أنه يمكن العبث به مع المعلومات.	٤.٨ **(مقرَّب إلى ٥)** **متوسّط–منخفض** ستتم مقارنة هذا المعدل_مع معدلات سيناريوهات التهديدات الأخرى واستخدامه لترتيب مستوى التهديدات.



⇦ الآن وبعد أن تم تحديث الرسم البياني لشجرة الأعطال، وأصبحت المؤسسة تعرف الكثير عن التهديد الإلكتروني بعد ترجمته إلى مخاطر إلكترونية موازية لأهداف السلامة، يمكن تحديث تقييم مخاطر السلامة الأصلي بما في ذلك تقييم التهديد الإلكتروني، مما قد يؤدي إلى أرجحية جديدة بوقوع الحدث البارز المتعلق بالسلامة ("تسليم زائف غير مكتشف لرسالة أو عدة رسائل تُستخدم لإعطاء التصاريح").

⇦ وسيشكل هذا الأساس للخطوات التالية: تقييم المخاطر ومعالجة المخاطر.

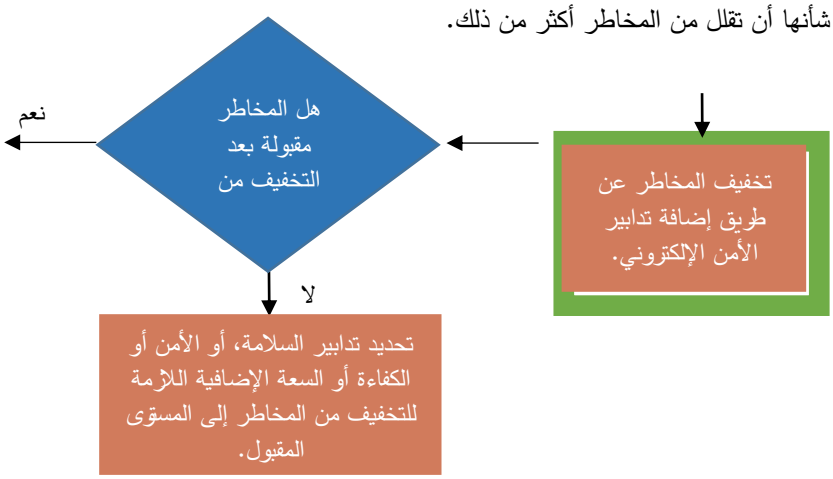


بعد الحصول على التقييمات المحدّثة، يستخدم مقدم خدمات الملاحة الجوية مصفوفة المقبولية الحالية. وقد تحتوي مصفوفة المقبولية هذه على أنواع مختلفة من المعايير مثل:

- المعايير الإلكترونية، والتي يشمل مصدرها لوائح الطيران، ولوائح/قوانين البنية التحتية الحيوية، ومدى تحمّل المخاطر التنظيمية، وما إلى ذلك.
- معايير السلامة، التي تشمل العلاقة بين أثر السلامة واحتمالية السلامة المستهدفة بالإضافة إلى المصادر المتعلقة بلوائح الطيران المعنية.
- معايير السعة والكفاءة في الملاحة الجوية، التي تعتمد على المؤسسة (وتقع خارج نطاق هذا المثال).

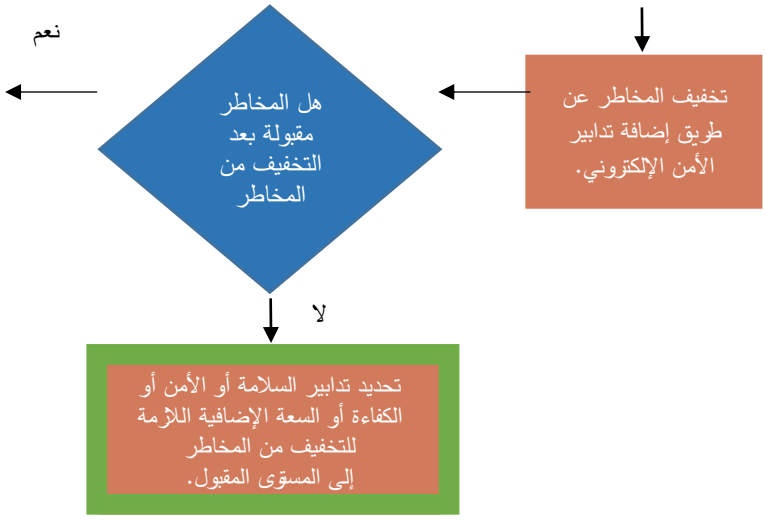
وينبغي أن يفضي هذا التقييم مقابل هذه المعايير التنظيمية إلى اتخاذ قرار :**هل يمكن قبول المخاطر كما هي أم يجب وضع ضوابط إلكترونية مكملة للضوابط الحالية؟**

أدى التقييم إلى اتخاذ قرار بأنه على الرغم من أن المخاطر الإلكترونية المتبقية **متوسطة – منخفضة**، يجب النظر في اتخاذ تدابير تخفيف إضافية من شأنها أن تقلل من المخاطر أكثر من ذلك.



⇦ **التدابير الاحترازية من مخاطر الأمن الإلكتروني:**

- اقترح خبراء الإنترنت أولاً إضافة معدات جديدة لتعزيز حماية النظام من التدخل. ولكن هذه الإضافة رُفضت من قبل خبراء السلامة لأنها ستخلق نقاط أعطال جديدة تتطلب مراجعة تقييم سلامة النظام بأكمله، بالإضافة إلى الأنظمة الأخرى المتأثرة.
- واتفق خبراء السلامة والإنترنت على أن الضوابط الموجودة لحماية النظام من أي هجوم إلكتروني خارجي كافية، وبالتالي قرروا البحث عن تدابير للتخفيف من التهديد الداخلي الذي تم الاتفاق على أنه أكثر معقولية أثناء تقييم المخاطر الإلكترونية.
- واقترح خبراء الإنترنت تدابير لتشديد امتيازات الوصول إلى الحواسيب والخوادم الموجودة، وهو ما تم قبوله.



⇦ **التدابير الاحترازية الإضافية:**

- في وجود هذه التدابير الاحترازية للأمن الإلكتروني، تبيّن أن هناك إمكانية لتقليل المخاطر بشكل أكبر من خلال النظر في أنواع أخرى من التدابير الاحترازية.

- وقد اقترح خبراء أمن الطيران تشديد التحريات الشخصية وتدابير التحكم في وصول الموظفين المصرَّح لهم بالوصول إلى مراقبة الحركة الجوية غرف الخوادم.
- وتم تكرار تقييم المخاطر بعد أن أُخذت في الاعتبار التدابير الجديدة للتخفيف من المخاطر (التدابير الإلكترونية وتدابير الأمن الإلكتروني على حد سواء) وتقرر أن التدابير الجديدة ستقلل من المخاطر إلى مستوى مقبول، لذلك تم قبول تنفيذ التدابير الجديدة.

⇦ **مصفوفة المخاطر الإلكترونية:**

- أدى ذلك إلى استكمال مصفوفة تقييم المخاطر الإلكترونية بعد أن تم تسجيل التدابير الاحترازية الإضافية لكي يجري تنفيذها، وبذلك تتخذ مصفوفة تقييم المخاطر الإلكترونية النهائية الشكل التالي.

مصفوفة المخاطر الإلكترونية

السيناريو	الاحتمالية	الأثر	التدابير الاحترازية	مواطن الضعف	المخاطر المتبقية	التدابير الاحترازية الإضافية
متسلل يعبث بالحمولة الإيرادية للبيانات في رسالة وصلة بيانات مرسلة من مراقب جوي إلى طيار.	**٢** **متوسّط–منخفض** سيناريو لا توجد له أمثلة حديثة العهد أو أي أمثلة على الإطلاق، مع بعض الأدلة على وجود القصد، ولكن بمنهجية غير متطورة ظاهرياً بما فيه الكفاية لتنفيذ سيناريو هجوم ناجح أو قد يُستبدل السيناريو بأشكال هجومية أُخرى؛	**٣** **كبير:** حدث بارز في مجال السلامة: تسليم زائف غير مكتشف لرسالة واحدة أو عدة رسائل مستخدمة لإصدار التصاريح.	**التحقق الدوري للتكرارية** تم بالفعل تنفيذ المراقبة وقدرات اكتشاف المتسللين. تدابير تكنولوجيا المعلومات المتعلقة بالأمن مراقبة الدخول المادي/ التحريات الشخصية	**٠.٨** **متوسط – مرتفع** لا يُعد التحقق الدوري للتكرارية أداة مناسبة للكشف عن العبث الخبيث بالمعلومات بالنظر إلى أنه يمكن العبث به مع المعلومات.	**٤.٨** **(مقرَّب إلى ٥)** **متوسّط–منخفض** ستتم مقارنة هذا المعدل مع معدلات سيناريوهات التهديدات الأخرى واستخدامه لترتيب مستوى التهديدات.	**الإلكترونية:** **تحسين ومراقبة امتيازات الوصول الرقمي إلى أجهزة الكمبيوتر والخوادم ذات الصلة.** **الأخرى:** **تشديد التحريات الشخصية وضبط الوصول المادي للموظفين المخوَّل لهم الوصول إلى مراقبة الحركة الجوية وغرف الخوادم.**

الخلاصة

يرِد النهج التدريجي في هذا المثال لأغراض التوضيح بقصد إظهار الطريقة التي يجب أن تتفاعل بها تقييمات السلامة والمخاطر الإلكترونية للتصدي للتهديدات والمخاطر التي يتعرض لها الطيران المدني. وعلى أرض الواقع، ستجري هذه العملية بطريقة أكثر تكرارية وتكاملاً، اعتماداً على الهيكل المؤسسي للنُظم الإدارية والأُطر التنظيمية أو القانونية المعمول بها.

— — — — — — — —

المرفق (باء)

مثالٌ لتطبيق المنهجية
في إدارة مخاطر سلامة الطيران

افتراضات ولمحة عامة

يوضح المثال أدناه دمج تقييم المخاطر الإلكترونية في تقييم مخاطر أمن الطيران، باستخدام سيناريو تهديد افتراضي يجري تقييمه من قِبل الدولة.

الافتراضات:

- قامت الدولة بالفعل بتقييم مخاطر أمن الطيران ذات الصلة وتقديرها والتخفيف من حدتها باستخدام مصفوفات مخاطر أمن الطيران.
- وقد اختار خبراء أمن الطيران لهذا الغرض فحص الأمتعة اليدوية كوظيفة طيران حرجة.
- ولأغراض التبسيط، يُفترض أن التهديد الإلكتروني الخاضع للتقييم يؤثر فقط على أمن الطيران (لا تأثير على السلامة، أو كفاءة الملاحة الجوية و/أو سعتها).
- وتستخدم الدولة نفس جداول التقييم للاحتمالية والأثر ومواطن الضعف كتلك المستخدمة في هذه الوثيقة.
- ولأغراض الاتساق، يستخدم نظام التقييم المستعمل في تقييم المخاطر الإلكترونية نفس القيم الواردة في الفصل الثالث من النسخة مقيَّدة التوزيع من هذه الوثيقة. ولكن في واقع الأمر، ستختلف معدلات الاحتمالية والأثر ومواطن الضعف لفرادى الدول والمنظمات وفقاً للمتغيرات المختلفة التي تؤثر على هذه التصنيفات (القدرات، القصد، التدابير الاحترازية الحالية، إلخ).
- ونظراً لحساسية تقييمات مخاطر أمن الطيران، لا يشرح هذا الجزء سوى عملية دمج تقييم المخاطر الإلكترونية في تقييم أمن الطيران. بيد أن عملية تقييم المخاطر الإلكترونية سيجري وصفها بالتفصيل.

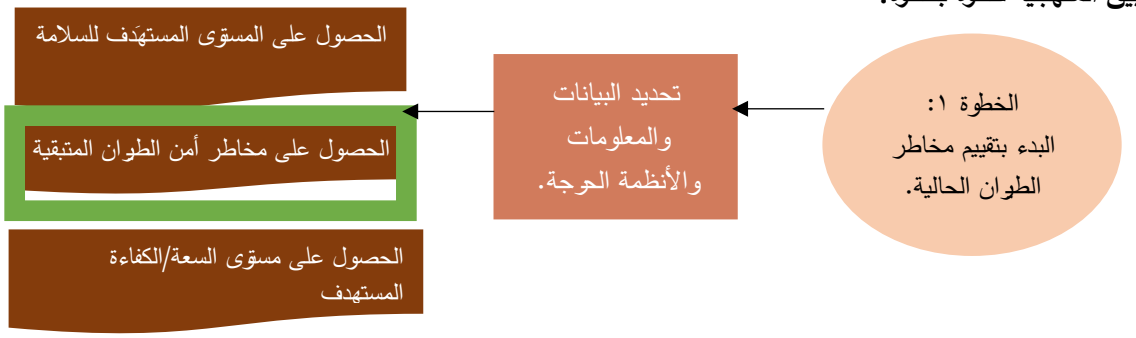
سيناريو التهديد الإلكتروني:

- تُجري الدولة تحليلاً لمختلف الأساليب التي يمكن لخصم أن يستخدمها لاستجلاب أجهزة محمولة متفجرة ارتجالية على متن طائرة في الأمتعة اليدوية بهدف إسقاط الطائرة.
- تعاون خبراء سلامة الطيران مع خبراء إنترنت لمراجعة تقييمات مخاطر السلامة الحالية لوظيفة فحص أمتعة الركاب وحددوا نظام الكشف في جهاز الفحص بوصفه يشكل النظام الحرج والمعلومات (الداعمة لوظيفة الطيران الحرجة) التي ينبغي تقييمها للوقوف على المخاطر الإلكترونية.
- وأعد خبراء أمن الطيران تقييماً للمخاطر الأمنية الحالية للأجهزة المتفجرة الارتجالية (سواء المحمولة على الجسم أو المستجلبة ضمن أمتعة الركاب) وقرروا النظر في الأخيرة فقط في عملية التقييم هذه.
- ومن خلال المناقشات مع خبراء أمن الطيران، توصل خبراء الانترنت إلى أن "العبث بالبيانات في مكون نظام الكشف بهدف تغيير نتائج عملية الفحص الآلي" يشكل سيناريو لتهديد إلكتروني يجب تقييمه ودمجه في تقييم مخاطر أمن الطيران المذكورة أعلاه.
- أسلوب الهجوم: يمكن تنفيذ هذا الهجوم من خلال التدخل في قدرات الكشف عن المعدات إما بالوصول المادي أو عن بعد إلى المعدات المعنية.

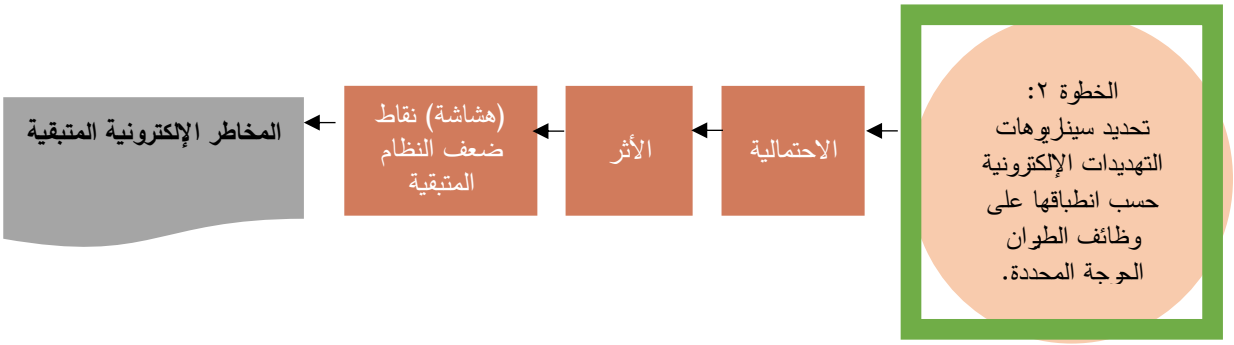
- ومن خلال الاستعانة بمثال تصنيف التهديدات الإلكترونية في المرفق (جيم)، (يُرجى الرجوع إلى النسخة مقيَّدة التوزيع من هذه الوثيقة)، يمكن تصنيف هذا التهديد الإلكتروني على النحو التالي:

  - المجال: المطار.
  - الوظيفة: الأمن.
  - الوظيفة الفرعية: فحص أمتعة الركّاب.
  - التهديد الإلكتروني: التغيير (التدخل في برمجيات/أنظمة الكشف).

تطبيق المنهجية خطوة بخطوة:



- تعاون خبراء سلامة الطيران مع خبراء الإنترنت لمراجعة تقييمات مخاطر السلامة الحالية للأجهزة الارتجالية المتفجرة اليدوية في أمتعة الركاب وحددوا نظام الكشف في وظيفة جهاز الفحص بوصفه نظاماً ومعلومات داعمة للوظيفة الحرجة التي ينبغي تقييمها للوقوف على المخاطر الإلكترونية.
- وأنتج خبراء أمن الطيران التقييم الأولي لمخاطر الأجهزة الارتجالية المتفجرة اليدوية بدون أسباب إلكترونية. سيناريو أمن الطيران المرتبط بسيناريو التهديد الإلكتروني لدينا هو: "مادة محظورة يجلبها الراكب على متن الطائرة بقصد إسقاط الطائرة".
- **نتيجة هذه العملية هي الحصول على المخاطر الأمنية المتبقية للسيناريو أعلاه.**



- ومن خلال المناقشات مع خبراء أمن الطيران، حدد خبراء الإنترنت "العبث بالبيانات في مكون نظام الكشف بهدف تغيير نتائج عملية الفحص الآلي" كسيناريو تهديد إلكتروني يجب تقييمه ودمجه في تقييم مخاطر أمن الطيران المذكورة أعلاه.
- وتم إجراء تقييم المخاطر الإلكترونية من قبل خبراء إنترنت تابعين للدولة بالتعاون مع خبراء في أمن الطيران. حيث يمتلك خبراء الانترنت معرفة بوسائل وأساليب الهجوم الشائعة للتهديدات الإلكترونية بينما يمتلك خبراء أمن الطيران معرفة بالمعدات ومستويات التحمل.

وتم توسيع مكونات تقييم المخاطر الإلكترونية في الخطوة ٢ لتشمل الخطوات التالية:

واتُخذت الخطوات التالية لإجراء تقييم المخاطر الإلكترونية في مجال الأمن الإلكتروني توطئة لبناء مصفوفة المخاطر الأمنية الإلكترونية:

⇦ **الاحتمالية:**

- غالباً ما يستخدم كل من خبراء أمن الطيران وخبراء الإنترنت جداول احتمالات ذات قيم متفردة (مثل الجدول ١ في الفصل الثاني)، تساعد على مواءمة فهم مكونات المخاطر المختلفة.
- وتتطلب القدرة على تنفيذ الهجوم الإلكتروني الذي يجري تقييمه إعداداً دقيقاً.
- من الصعب تنفيذ هجوم خارجي نظراً لأن معدات الفحص إما أن تكون قائمة بذاتها (غير متصلة بشبكة) أو متصلة بشبكة محلية مغلقة، وسيتطلب ذلك الكثير من الجهد والدراية لتغيير نتيجة عملية الفحص.
- التهديد الداخلي ممكن، ولكنه يتطلب الكثير من الجهد والدراية لتغيير نتيجة عملية الفحص، على سبيل المثال:
  - معرفة تفصيلية بالمطار، ونقاط التفتيش، والجداول الزمنية، وما إلى ذلك.
  - مستوى عالٍ من التعاون (لا يمكن تنفيذ الهجوم دون مساعدة).
  - الوصول إلى الأجهزة و/أو الشبكة المحلية.
- هناك أدلة حالية على وجود قصد.
- ونتيجة لذلك، تم تحديد احتمالية التهديد الإلكتروني عند المستوى ٣، وهو مستوى متوسط (أي سيناريو معقول في الأساس، مع بعض الأدلة على القصد والقدرة وربما بعض الأمثلة).

⇦ **الأثر/التبعات/التأثير:**

- ينطوي تقييم الأثر على تقييم سيناريو معقول لأسوأ الحالات، وهو ما يعني في هذه الحالة أن الهجوم الإلكتروني كان ناجحاً.
- قد يتمخض الهجوم الإلكتروني عن استخراج بيانات خاطئة من معدات الفحص، الأمر الذي قد يؤدي إلى تسرب مواد محظورة دون فحص. وقد يسفر ذلك عن تدمير الطائرة وسقوط المئات من القتلى، وربما وقوع بعض الضحايا على الأرض. وتتمثل إحدى العواقب الأخرى في التكاليف الفورية الباهظة للغاية والأضرار الاقتصادية على المدى الطويل. وبالتالي فإن الأثر سيكون **مرتفعاً** (درجة ٥).

⇦ **مواطن الضعف:**

- لإجراء تقييم مواطن الضعف تؤخذ في الاعتبار التدابير الاحترازية المطبّقة.
- فيما يتعلق بالتدابير الاحترازية المطبّقة:
  - فرضت الدولة استخدام القواعد والتوصيات الدولية الواردة في الملحق السابع عشر — "أمن الطيران" فيما يتعلق بفحص الركاب باستخدام أنظمة الكشف التي يطبقها المطار.
  - كما تشترط الدولة على مشغليها تنفيذ القاعدة القياسية ٤-٩-١ والتوصية الدولية ٤-٩-٢ المتعلقتيْن بالتصدي للتهديدات الإلكترونية، ولذلك يقوم المطار بتنفيذ التدابير التالية:

- هناك فصل منطقي أو مادي في شبكات تكنولوجيا المعلومات عن البنية التحتية التجارية والتشغيلية[٢٠].
- ويجري تطبيق إجراءات التحريات الشخصية عن الموظفين بالإضافة إلى وجود تدابير خاصة بأمن الطيران لحماية الوصول إلى المعدات.

- أكد خبراء الإنترنت أن الضوابط الموجودة حالياً مُرضية للتخفيف من المخاطر الإلكترونية. ومع ذلك، نظراً لأن خبراء أمن الطيران يدركون أن المتطلبات التي يطبقها المطار لا يجري تنفيذها بشكل متسق في جميع أنحاء العالم (خاصة تلك المتعلقة بالتوصيات الدولية)، فقد تم الاتفاق على تصنيف مواطن الضعف على أنها **متوسطة–منخفضة** (٠,٤).

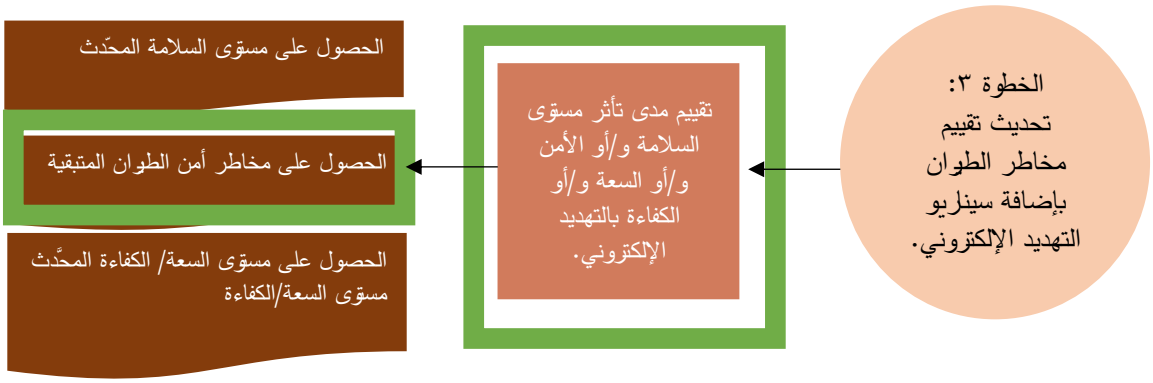
⇦ المخاطر الإلكترونية المتبقية:

- يمكن الآن احتساب المخاطر الإلكترونية المتبقية من خلال ضرب معدلات الاحتمالية والأثر ومواطن الضعف: **(٣ x ٠.٤ x ٥) = ٦ بما يعني أن المخاطر الإلكترونية المتبقية متوسطة – منخفضة.**

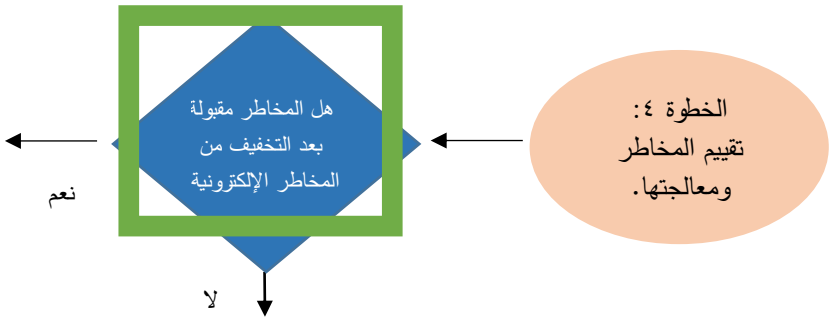
ومن ثم تتخذ مصفوفة المخاطر الإلكترونية بعد ذلك الشكل التالي:

مصفوفة المخاطر الإلكترونية					
السيناريو	**الاحتمالية**	**الأثر**	**التدابير الاحترازية**	**مواطن الضعف الهشاشة**	**المخاطر المتبقية**
مادة محظورة أتى بها راكب على متن الطائرة عن طريق تغيير نتائج أجهزة الفحص الأمني بقصد إسقاط الطائرة.	**٣** **متوسّطة** هل الخصم قادر على ذلك؟ هل هناك مصلحة في مهاجمة هدف للطيران المدني؟	**٥** **مرتفعة** في أسوأ السيناريوهات المعقولة: كم عدد الأرواح التي ستزهق؟ هل من المتوقع حدوث ضرر للبنية التحتية؟ هل سيفقد الجمهور الثقة في النقل الجوي؟ ما هي التكلفة الاقتصادية؟	تُطبّق القاعدة القياسية ٤–٩–١ والتوصية الدولية ٤–٩–٢ للملحق السابع عشر على فحص الركّاب باستخدام أنظمة الكشف.	**٠.٤** **متوسّط–منخفض** إذا أُخذت في الحسبان التدابير الاحترازية الحالية، ما مدى هشاشة الطيران إزاء سيناريو التهديد هذا؟	**٦** ستتم مقارنة هذا المعدل مع معدلات سيناريوهات التهديدات الأخرى واستخدامه لترتيب مستوى التهديدات.

[٢٠] يشير الفصل المنطقي إلى تجزئة الشبكة من خلال إنشاء مناطق منطقية (افتراضية) على نفس الشبكة المادية أو الأجهزة.



- وبعد ترجمة التهديد الإلكتروني إلى مخاطر إلكترونية موازية لأهداف أمن الطيران، يمكن تحديث التقييم الأولي لمخاطر أمن الطيران بما في ذلك تقييم التهديد الإلكتروني، حيث يجري تناوله الآن في إطار مصفوفة مخاطر أمن الطيران للسيناريو المعني، مما قد يؤدي إلى مخاطر أمنية متبقية جديدة.
- وسيشكّل هذا الأساس للخطوات التالية: تقييم المخاطر ومعالجة المخاطر.



- باستخدام هذه البيانات، ستقوم الدولة بتحديث مصفوفة مخاطر الأجهزة المتفجرة المرتجلة اليدوية لتشمل طريقة العمل هذه.

وينبغي أن يؤدي هذا التقييم إلى اتخاذ قرار: **هل يمكن قبول المخاطر كما هي، أم هل ينبغي تنفيذ تدابير احترازية إلكترونية بالإضافة إلى الضوابط الحالية؟**

- لقد تم التوصل إلى أن المخاطر الإلكترونية المتبقية منخفضة للغاية بحيث لا تؤدي إلى تغيير التقييم الأصلي، وبالتالي فإن المخاطر المتبقية لنوع سيناريو التهديد الخاص بالأجهزة المتفجرة الارتجالية المحمولة لا تتأثر بسيناريو التهديد الإلكتروني هذا (أي أن تهديد أمن الطيران يبقى على نفس مستواه الأعلى).
- كما أبدى خبراء الإنترنت رضاهم عن الضوابط المعمول بها لدعم سلامة عملية الفحص.
- بيد أن خبراء الإنترنت أشاروا إلى أن أي تغيير في المعدات يتطلب إعادة ترخيصها من قِبل السلطة المختصّة، مما قد يعرّض النظام لتهديدات إلكترونية مستقبلية إذا لم يتم تصحيح نقاط الضعف المكتشفة في الوقت المناسب. وبناء عليه، تم الشروع في مشروع لإيجاد نهج متوازن بين ترخيص المعدات وتحديث ضوابط الأمن الإلكتروني المطبَّقة على معدات الفحص، وتم تسجيل نواتج المشروع كإجراء تخفيف إضافي لكي تنفذ في المستقبل لدعم تخفيف المخاطر الإلكترونية.
- وبالتالي فإن مصفوفة المخاطر الإلكترونية المحدّثة لهذا السيناريو هي كما في مصفوفة المخاطر الإلكترونية التالية.

مصفوفة المخاطر الإلكترونية						
السيناريو	**الاحتمالية**	**الأثر**	**التدابير الاحترازية**	**مواطن الضعف**	**المخاطر المتبقية**	**التدابير الاحترازية الإضافية**
مادة محظورة أتى بها راكب على متن الطائرة عن طريق تغيير نتائج أجهزة الفحص الأمني، بقصد إسقاط الطائرة.	٣ **متوسّطة** هل الخصم قادر على ذلك؟ هل هناك مصلحة في مهاجمة هدف للطيران المدني؟	٥ **مرتفعة** في أسوأ السيناريوهات المعقولة: كم عدد الأرواح التي ستُزهق؟ هل من المتوقع حدوث ضرر للبنية التحتية؟ هل سيفقد الجمهور الثقة في النقل الجوي؟ ما هي التكلفة الاقتصادية؟	يجري تطبيق القاعدة القياسية ٤-٩-١ والتوصية الدولية ٤-٩-٢ للملحق السابع عشر على فحص الركّاب باستخدام أنظمة الكشف.	٠.٤ **متوسّط-منخفض** إذا أُخذت في الحسبان التدابير الاحترازية الحالية، ما مدى هشاشة الطيران إزاء سيناريو التهديد هذا؟	٦ ستتم مقارنة هذه الدرجة مع درجات سيناريوهات التهديدات الأخرى واستخدامها لتصنيف التهديدات.	اتخاذ إجراءات لتحقيق التوازن بين تصحيح نقاط الضعف وإعادة ترخيص معدات فحص الأمتعة اليدوية.

الخلاصة

يرِد النهج التدريجي في هذا المثال لأغراض التوضيح ويهدف إلى إظهار الطريقة التي يجب أن يتفاعل بها تقييم الأمن وتقييم المخاطر الإلكترونية بما يتيح التصدي للتهديدات والمخاطر الإلكترونية التي يتعرض لها الطيران المدني. وعلى أرض الواقع، يُتوخى أن تجري هذه العملية بطريقة أكثر تكرارية وتكاملاً، اعتماداً على الهيكل المؤسسي للنُظم الإدارية وأُطرها التنظيمية أو القانونية المعمول بها.

— انتهى —

ISBN 978-92-9275-999-5