



تقييم المخاطر المهنية (HIRA/JSA) وبناء سجل  
مخاطر الموقع



الإمارات العربية المتحدة - دبي

2026 / 09 / 03 – 08/30



## مقدمة:

في إطار التوجه الاستراتيجي نحو السيادة الرقمية وتطبيق مبدأ تصفير البيروقراطية، لم يعد تقييم المخاطر مجرد إجراء ورقي روتيني، بل أصبح "ذكاءً وقائياً" يضمن استمرارية الأعمال وحماية المورد البشري السيادي. تهدف هذه الدورة إلى تمكين القادة من أدوات تحديد المخاطر وتقييمها (HIRA) وتحليل سلامة الوظائف (JSA) باستخدام التقنيات الذكية. يركز البرنامج على كيفية بناء سجل مخاطر ديناميكي (Dynamic Risk Register) يعمل كمحرك لاتخاذ القرار، مما يضمن قيادة المؤسسة وقدرتها على تصفير الحوادث عبر هندسة وقائية تعتمد على النزاهة والبيانات اللحظية.

## أهداف الدورة:

- استيعاب مفاهيم الرشاقة الوقائية وعلاقتها بتصفير البيروقراطية في إجراءات التصاريح والعمليات.
- تطوير مهارات تحديد المخاطر وتقييمها (HIRA) وفق المعايير العالمية الموائمة للهوية الوطنية.
- إتقان فن تحليل سلامة الوظائف (JSA) لتفكيك المهام المعقدة وتصفير فجوات الأمان فيها.
- بناء وإدارة سجل مخاطر الموقع الرقمي لضمان السيادة المعلوماتية والتحكم اللحظي في الأخطار.
- حوكمة ممارسات تقييم المخاطر لضمان النزاهة المطلقة ومنع "التقديرات الشخصية" غير الدقيقة.
- تعزيز السيادة الرقمية من خلال إدارة سجلات المخاطر على سحابات وطنية آمنة ومشفرة.
- تطبيق استراتيجيات "التسلسل الهرمي للتحكم (Hierarchy of Controls)" بذكاء وابتكار.
- تطوير مهارات إدارة المعضلات الأخلاقية المرتبطة بـ "المخاطر المقبولة" مقابل جودة الحياة.
- صياغة خارطة طريق شاملة لتحويل سجل المخاطر إلى "درع سيادي" يحمي الأرواح والمنجزات.



## محتويات الورشة:

### اليوم الأول:

#### فلسفة التقييم السيادي في عصر تصفير البيروقراطية

#### من "الرصد الورقي" إلى "الهندسة الوقائية والرشافة"

- مفهوم التقييم الاستباقي: لماذا تُعد البيانات هي خط الدفاع الأول عن السيادة البشرية للمؤسسة؟
- مواءمة الـ HIRA مع استراتيجية تصفير البيروقراطية: كيف نلغي عناء التكرار في تقارير المخاطر؟
- تحليل العلاقة بين "دقة تقييم الخطر" وبين بناء الثقة والمصادقية الوطنية عالمياً.
- تمرين "هندسة الحصانة": تحديد الأنشطة السيادية في منشآتكم ووضع مصفوفة مخاطر تصفر الاحتمالية بنزاهة.

#### النزاهة والسيادة في بناء "مصفوفة المخاطر"

- مفهوم "السيادة المعلوماتية للمخاطر": حماية سجل المخاطر من التلاعب أو الضغوط الإجرائية.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة والصدق في تحديد "المخاطر الجسيمة".
- سيكولوجية الثقة في التقييم: بناء المصادقية عبر الشفافية في توضيح "الثغرات" وكيفية إغلاقها.
- صياغة ميثاق "أخلاقيات المقيّم المهني" لضمان عدم المحاباة أو التستر على المخاطر بنزاهة سيادية.

### اليوم الثاني:

#### الهندسة التقنية لتحليل سلامة الوظائف (JSA)

#### تصفير الأخطاء البشرية عبر التحليل الذكي للمهام

- خطوات الـ JSA المعززة بالذكاء الاصطناعي: كيف نكسر المهام إلى "نرات معلوماتية" آمنة؟
- الأمان الرقمي كركيزة للتحليل: حماية "قاعدة بيانات التدابير الوقائية" من الاختراق أو التزييف.
- إدارة الهوية الرقمية للفرق (UAE Pass) وأثرها على موثوقية "اجتماعات صندوق الأدوات" (Toolbox Talks).
- تمرين تقني: استخدام الواقع المعزز (AR) لإجراء تحليل JSA ميداني لحظي وتصحيح المسار بنزاهة.



## أخلاقيات التفاعل مع أنظمة "التوصية الآلية بالضوابط"

- حدود استخدام الذكاء الاصطناعي في "اختيار معدات الوقاية" دون فقدان الحكمة والمسؤولية البشرية.
- حوكمة مخرجات أنظمة "تقييم التكرارية": الضمان الأخلاقي لعدم التهاون في المخاطر المألوفة.
- مفهوم "الأمانة في الملاحظة": تجنب الاعتماد الكلي على الكاميرات دون "الإرادة القيادية" الميدانية.
- ورشة عمل: وضع ضوابط أخلاقية لاستخدام البيانات الضخمة في "توقع الحوادث بناءً على الـ JSA".

## اليوم الثالث:

### الحياد والعدالة في بناء سجل مخاطر الموقع

#### النزاهة الرقمية ومكافحة الانحياز في "ترتيب أولويات المخاطر"

- أخلاقيات "العدالة الوقائية": ضمان شمولية سجل المخاطر لجميع الفئات والمواقع بنزاهة وشفافية.
- الرقابة الأخلاقية على أنظمة "الخرائط الحرارية": كيف نضمن الشفافية والنزاهة في عرض النتائج؟
- تطبيق قاعدة "الإرادة البشرية القيادية": التدخل لتعديل "مستوى خطر آلي" قد يغفل ظروفًا استثنائية.
- حساب معامل الثقة في سجل المخاطر لتقليل احتمالات الخطأ الناتج عن "الهلوسة الرقمية" للبيانات.

#### حوكمة المسؤولية عن مخرجات "سجلات المخاطر المؤتمتة"

- المسؤولية المهنية للقائد عند حدوث "حادث" ناتج عن خطر لم يدرجه النظام الذكي في السجل.
- إدارة العلاقة مع مزودي حلول "Safety Software" ضمان السيادة والشفافية في الخوارزميات.
- بناء أنظمة "التحقق المزدوج" لضمان عدم غياب الحكمة البشرية في القرارات المصيرية.
- تمرين محاكاة: إدارة أزمة تواصل ناتجة عن "خطر مكتشف حديثاً" وكيفية تحديث السجل بنزاهة وريادة.



## اليوم الرابع:

### المسؤولية المهنية وإدارة السمعة عبر "الوقاية"

#### القيادة الاتصالية وحماية السمعة في بيئة هجينة

- أخلاقيات إدارة السمعة عبر "سجل المخاطر": الموازنة بين الشفافية والوقار والسيادة الحكومية.
- الرقابة على "البصمة الرقمية لسجلات السلامة" وأثرها على حيادية ومصداقية القرار السيادي.
- بناء نظام "الإفصاح الاستباقي للجهازية": ضمان الشفافية لتصفير فرص انتشار الشائعات حول الموقع.
- التدقيق الأخلاقي على سلاسل "إنتاج المعلومات الوقائية" لضمان خلوها من الممارسات غير العادلة.

#### أخلاقيات الاستجابة للانتهاكات المهنية والاختراقات

- المسؤولية الأخلاقية في التبليغ عن الثغرات التقنية التي قد تؤدي لتشويه "سجل مخاطر الموقع".
- فن التواصل الأخلاقي أثناء تعطل أنظمة الرصد: حماية الثقة عبر بيانات صادقة ونزيهة دون تضليل.
- إدارة "التعافي المؤسسي": إجراءات إعادة بناء الصورة بعد رصد انحراف في دقة تقييم المخاطر الرقمي.
- بناء خطة "الحصانة الوقائية الشاملة": تحصين منظومة التقييم ضد الهجمات أو الإهمال الممنهج.



## اليوم الخامس:

هندسة الاستجابة الوقائية وتصفير البيروقراطية في إدارة سجل المخاطر المهنية والسيادة البشرية

مختبر "الدرع الوقائي السيادي" وإدارة مصفوفة المخاطر الديناميكية تحت محاكاة الأزمات الميدانية

- محاكاة "الخطر المتغير والسيادة المعلوماتية": وضع القادة في سيناريو يحاكي نشوء خطر مفاجئ وغير متوقع في موقع إنشائي أو صناعي حيوي، واختبار قدرتهم على استخدام "سجل المخاطر الديناميكي" لإعادة تقييم الموقف لحظياً، وتفعيل بروتوكول "الحماية الاستباقية" بنزاهة ووضوح تام لضمان استمرارية الأعمال دون وقوع إصابات.
- تصفير البيروقراطية في "هندسة تصاريح العمل الذكية": تطبيق مسار قرار صفري الإجراءات لإصدار تصاريح العمل (PTW) بناءً على الربط اللحظي بين نتائج تحليل سلامة الوظائف (JSA) وبين الحالة الميدانية المرصودة عبر الحساسات، لضمان انتقال الفرق للمهام دون انتظار الموافقات الورقية أو التدقيق اليدوي المجهد، مع الحفاظ على الحصانة الرقمية والريادة العالمية الشاملة.
- هندسة "النزاهة والصدق" في التقييم الميداني: اختبار مهارة القائد في الموازنة بين مخرجات أنظمة "التحليل السلوكي للألات" وبين "الحكمة البشرية السيادية" لضمان عدم التغاضي عن المخاطر الجسيمة مقابل سرعة التنفيذ، ومنع أي انحيازات خوارزمية قد تجمل واقع المخاطر الميدانية، مما يعزز ريادة الدولة كبيئة عمل فائقة الأمان والنزاهة والشفافية.
- ورشة "تفكيك صوامع المخاطر والربط السيادي": مراجعة فورية لنتائج المحاكاة باستخدام التحليلات التنبؤية لتحديد الفجوات في "منظومة الرصد الموحدة"، وتطوير حلول هندسية استباقية تمنع تضارب البيانات بين سجل المخاطر وخطط الطوارئ، مما يحقق التميز في الأداء الوطني والوضوح التام أمام صانع القرار لبناء "رادار سلامة وطني معصوم".

## المخرجات الرئيسية للدورة:

- امتلاك استراتيجيات "حصانة وقائية" تضمن نزاهة التعامل مع مخاطر السلامة بنسبة 100%.
- القدرة على هندسة سجلات مخاطر "ديناميكية وسيادية" بمرونة وتوافق مع متطلبات الريادة.
- إتقان أدوات الرقابة الأخلاقية على الأنظمة الذكية لضمان الشفافية وتصفير مخاطر الانحياز الرقمي.
- بناء سجل ممارسات فضلى في إدارة "الذكاء الوقائي" يدعم اتخاذ القرار القيادي الآمن والمستدام.
- تحقيق جاهزية كاملة للمؤسسة والمسؤول للمنافسة في فئات التميز والريادة في السلامة والابتكار.



## الفئة المستهدفة:

- القيادات ومدراء إدارات السلامة والصحة المهنية، العمليات، والمشاريع الإنشائية والميدانية.
- مسؤولو التميز المؤسسي، مدراء الحوكمة، وخبراء إدارة المخاطر في الجهات السيادية.
- مستشارو الأمان المهني، مهندسو المواقع، وفرق التفتيش والرقابة الحكومية.
- رؤساء فرق مشاريع تصفير البيروقراطية وتطوير منظومات العمل الرقمي الذكي.
- الكوادر الطموحة الساعية لامتلاك جدارات "خبير تقييم المخاطر والنزاهة الرقمية".

## أساليب التدريب:

يتم استخدام بعض من الأساليب التالية أو الكل حسب المتطلبات لكل تخصص :

- دراسة الحالة المعقدة (Complex Case Studies)
- المحاكاة والألعاب الاستراتيجية (Simulation and War Gaming)
- ورش العمل القائمة على التفكير التصميمي (Design Thinking Workshops)
- حلقات النقاش مع خبير من القطاعين العام أو الخاص. (Expert Panels)
- المختبرات التكنولوجية التفاعلية (Interactive Technology Labs)
- التعلم من الأقران عبر الجهات الحكومية (Inter-Agency Peer Learning)
- نهج التعلم المدمج والمستمر (Blended & Continuous Learning Approach)