gisf

الأمم المتحدة - مكتب تنسيق الشؤون الإنسانية (UNOCHA) / أنطوان ليمونيه

تطوير استراتيجية وسياسة إدارة المخاطر الأمنية (SRM):
متعدد الوظائف
دليل

دليل منتدى الأمن العالمي المشترك بين الوكالات للمنظمات غير الحكومية

منتدى الأمن العالمي المشترك بين الوكالات

نبذة عن منتدى الأمن العالمي المشترك بين الوكالات

منتدى الأمن العالمي المشترك بين الوكالات (GISF) هو شبكة متنوعة من المنظمات الأعضاء الناشطة في مجالات المساعدات الإنسانية، والتنمية الدولية، وحقوق الإنسان، وحماية البيئة، والتي تقدر إدارة المخاطر الأمنية (SRM) كعنصر مهم في عملياتها وتنفيذ برامجها. في عالم سريع التغير، يقدّر منتدى الأمن العالمي المشترك بين الوكالات GISF أهمية التوثيق المستمر، والتكيف، والابتكار في سياسة وممارسة إدارة المخاطر الأمنية (SRM). لذلك، نتبنى نهجًا شاملًا في إدارة المخاطر الأمنية (SRM) ولا نؤمن بنموذج "قياس واحد يناسب الجميع" للأمن. نحن ندرك أن الموظفين المختلفين يواجهون مخاطر مختلفة، بناءً على تنوع ملفاتهم الشخصية، ومناصبهم، وسياقهم، ومنظمتهم. باختصار، نحن الشبكة الرائدة للمنظمات غير الحكومية في مجال إدارة المخاطر الأمنية (SRM) ومركز شامل لتبادل المعلومات، وإدارة المعرفة، والتنسيق، والتعاون.

تعرف على المؤلفين

المؤلف الرئيسي

بيث تشابمان (سلامة المواقع الدولية)

تمتلك بيث 15 عامًا من الخبرة في مستوى المدير في تقديم وإدارة السلامة والأمن في الخارج، بما في ذلك دورها كمديرة للبرامج في سلامة المواقع الدولية (ILS). وقد عملت بشراكة مع العديد من المنظمات غير الحكومية الإنسانية والتنموية والمناهضة لحقوق الإنسان والبيئية لتقديم زيارات برامجية آمنة وفعالة في بيئات معقدة، بالإضافة إلى دعم المنظمات في تطوير وتنفيذ مشاريع إدارة المخاطر الأمنية (SRM) الاستراتيجية والتشغيلية. هي عضو في لجنة BSI SVS/5 ومجموعة العمل BS8848:2014، ولديها فهم قوي لواجب الرعاية، وإدارة المخاطر المؤسسية، وإدارة المخاطر الأمنية والتدريب.

المؤلفون المشاركون

نايثن توملز (سلامة المواقع الدولية)

نايثن متخصص في تقييم التهديدات، والتخفيف من المخاطر، وبناء قدرات المنظمات غير الحكومية، والحكومات، وقوات الأمن. شغل مناصب إدارية عليا في إدارة الأمن وعمليات البرامج في سياقات سياسية معقدة، بما في ذلك العراق وأوكرانيا ونيجيريا. يمتلك نايثن تسع سنوات من الخبرة كضابط في الجيش البريطاني، وفي مناصب إدارية عليا داخل المنظمات غير الحكومية الدولية.

هانا ايستوود (سلامة المواقع الدولية)

هانا مستشارة مخاطر أولى في سلامة المواقع الدولية (ILS)، ولديها خبرة واسعة في تقديم المشورة التشغيلية والاستراتيجية بشأن المخاطر. عملت سابقًا كمحللة تهديدات أولى في Crisis24 وفي شركة Palladium ضمن مكتب وزارة الخارجية والتنمية البريطانية (FCDO) لشؤون النزاعات والاستقرار والوساطة. لديها خبرة واسعة في عدة دول، بما في ذلك بابوا غينيا الجديدة، مولدوفا، وأوكرانيا، والإمارات العربية المتحدة، ورواندا، وكينيا، وإندونيسيا.

نظرة على هذا الدليل

يهدف هذا المورد إلى أن يكون بمثابة مسار للتعامل مع إدارة المخاطر الأمنية (SRM) على المستوى الاستراتيجي، وتطوير السياسات، والمستوى التنظيمي. إنه ليس دليلًا "إرشاديًا عمليًا"، ولا منهجية "مقاس واحد يناسب الجميع". بدلاً من ذلك، يهدف إلى تقديم التطرق إلى بعض القضايا الرئيسية التي تواجه إدارة المخاطر الأمنية (SRM) وتزويد القادة الكبار بمجالات يمكن أخذها بعين الاعتبار فيما يتعلق بكيفية التعامل مع تطوير وتنفيذ الخطط الاستراتيجية لإدارة المخاطر الأمنية. يهدف هذا المورد أيضًا إلى تقديم الإرشادات والدعم حول كيفية تحسين التواصل، والفهم، والتعاون بين إدارة المخاطر الأمنية (SRM) وقادة الوظائف العليا الآخرين داخل المنظمة. يستهدف هذا الدليل الموظفين الذين يتحملون المسؤولية المباشرة عن تطوير وتنفيذ استراتيجية وسياسات إدارة المخاطر الأمنية (SRM) على مستوى المقر الرئيسي، وكذلك القادة الكبار من مجالات العمل الاستراتيجية الأخرى.

المنهجية

تم إعداد هذا المورد بناءً على 19 مقابلة معمقة شبه مهيكلة مع جهات مخبرة رئيسية (KIIs). شملت لائحة المشاركين مديري أمن على المستوى الأعلى من المنظمات الإنسانية غير الحكومية الوطنية والدولية، وخبراء رئيسيين لديهم خبرة في إدارة المخاطر الأمنية (SRM) في القطاع الإنساني، بالإضافة إلى ممثلين عن الشركات والجهات المانحة. تم أيضًا تنظيم خمس ورش عمل جماعية ميسّرة مع مديري الأمن على المستوى العالي، بالإضافة إلى إجراء استطلاعين عبر الإنترنت (مع 23 مستجيبًا على المستوى الاستراتيجي و29 مستجيبًا على المستوى التشغيلي). أكمل استعراض شامل للأدبيات هذه المعلومات مع مراجعة نهائية يقودها الأقران للمورد والأدوات.

الاستشهاد المقترح

منتدى الأمن العالمي المشترك بين الوكالات. (2024) تطوير استراتيجية وسياسة إدارة المخاطر الأمنية (SRM): دليل متعدد الوظائف. منتدى الأمن العالمي المشترك بين الوكالات (GISF).

شكر وتقدير

استفاد فريق سلامة المواقع الدولية بشكل كبير من الإرشادات ومدخلات أعضاء مجموعة العمل في منتدى الأمن العالمي المشترك بين الوكالات GISF، التي تتكون من خبراء بارزين وناشطين في المجال الإنساني يعملون في هذا القطاع. ونتوجه بالشكر الخاص إلى أوين داكايان، ونيل إليوت، ونويمي مونوز، وبيتر والش، ووحيد الله أحمدزاي، وتوبي وودبريدج على رؤاهم وتعليقاتهم القيمة. استفاد الدليل أيضًا من مدخلات متخصصي إدارة المخاطر الأمنية (SRM) خارج القطاع، ونحن ممتنون للغاية لزملائنا في سلامة المواقع الدولية (ILS) وGISF الذين قدموا مدخلات ودعمًا وضمان جودة كبيرين للمشروع. نحن ممتنون لليزا ريلي (المديرة التنفيذية السابقة لمنتدى الأمن العالمي المشترك بين الوكالات GISF) التي زرعت فكرة هذا المنشور. كما نود أن نشكر بانوس نافروزيديس، ديميتري كوتسيراس، تارا آرثر، دان فورد، وشون بيكلي على مراجعتهم وتعليقاتهم على المسودة. وأخيرًا، نحن ممتنون لفِرق منتدى الأمن العالمي المشترك بين الوكالات GISF التي جعلت من الممكن عرض نتائجنا الأولية في منتديات GISF الخريفية لعام 2023 في مدريد وواشنطن العاصمة.

المنظمة الدولية للهجرة/موسى محمد

مولدافيا

عامل إنساني يجري استطلاعا مع لاجئ قادم من أوكرانيا.

إخلاء المسئولية

GISF CIC هي شركة محدودة، مسجلة في إنجلترا وويلز برقم التسجيل 14937701. يقع مكتبنا المسجل في روميرو هاوس، 55 طريق جسر وستمنستر، لندن، إنجلترا، SE1 7JB. GISF CIC هي منظمة تعتمد على قيادة أعضائها. بينما تشمل الإشارات إلى "GISF CIC" في إخلاء المسؤولية هذا أعضاء منتدى الأمن العالمي المشترك بين الوكالات GISF والمراقبين وأمانتها العامة وموظفيها الإداريين، فإن الآراء أو المواقف المعبر عنها لا تمثل بالضرورة آراء الجهات المانحة أو المنظمات الأعضاء الفردية في GISF CIC.

المعلومات الواردة في هذا المنشور مخصصة لأغراض المعلومات العامة فقط. يتم تقديم المعلومات من قبل GISF CIC، وبينما نسعى جاهدين للحفاظ على دقة المعلومات واكتمالها، فإننا لا نقدم أي إقرارات أو ضمانات من أي نوع، صريحة أو ضمنية، بشأن اكتمالها أو دقتها أو موثوقيتها أو ملاءمتها.

لذلك، فإن أي اعتماد تقوم به على هذه المعلومات يكون على مسؤوليتك الخاصة تمامًا. ينبغي عليك الحصول على نصيحة مهنية أو متخصصة قبل اتخاذ أي إجراء أو الامتناع عنه بناءً على محتوى هذه المعلومات. في أي حال من الأحوال، لن نكون مسؤولين عن أي خسارة أو ضرر، بما في ذلك، على سبيل المثال لا الحصر، الخسارة أو الضرر غير المباشر أو التبعي فيما يتعلق باستخدامها.

تم إصدار هذا المنشور بواسطة منتدى الأمن العالمي المشترك بين الوكالات GISF من خلال الجوائز رقم 720FDA20GR00341 ورقم 720BHA24GR00016، الممولة من وكالة الولايات المتحدة للتنمية الدولية (USAID) ومن خلال منظمة ChildFund International.

خرج هذا الدليل إلى حيز الوجود بفضل الدعم السخي من الشعب الأمريكي من خلال وكالة الولايات المتحدة للتنمية الدولية (USAID). المحتويات هي مسؤولية منتدى الأمن العالمي المشترك بين الوكالات ولا تعكس بالضرورة آراء وكالة الولايات المتحدة للتنمية الدولية (USAID) أو الحكومة الأمريكية.

جدول المحتويات

ملخصات

AI	الذكاء الاصطناعي
BoD	مجلس الإدارة
CINFO	المركز السويسري للتميز في التعاون الدولي
CMAG	مجموعة المستشارين المدنيين والعسكريين
CMT	فريق إدارة الأزمات
CSR	المسؤولية الاجتماعية للشركات
DEI	التنوع والمساواة والشمول
DoC	واجب الرعاية
GISF	منتدى الأمن العالمي المشترك بين الوكالات
ISO	المنظمة الدولية للتوحيد القياسي
KII	مقابلة مع مُبلغ رئيسي
KPI	مؤشر الأداء الرئيسي
MEAL	الرصد والتقييم والمساءلة والتعلم
NGO	منظمة غير حكومية
NSAG	مجموعة مسلحة غير نظامية
OCHA	مكتب الأمم المتحدة لتنسيق الشؤون الإنسانية
PSEAH	منع الاستغلال والاعتداء والتحرش الجنسي
ROI	عائد الاستثمار
SLT	إنقاذ الأرواح سوياً
SOP	إجراءات التشغيل القياسية
SRM	إدارة المخاطر الأمنية
ToC	نظرية التغيير
TRM	إدارة مخاطر السفر
UN	الأمم المتحدة

قاموس

استمرارية الأعمال: التخطيط الاستراتيجي والإجرائي الذي تقوم به المنظمة لضمان استمرار الوظائف الأساسية خلال وبعد حدث تخريبي.

إدارة الأزمات: التخطيط والتنسيق وتنفيذ الإجراءات وخطط العمل المصممة للتنقل بفعالية والتخفيف من آثار الأزمة.

واجب الرعاية: الواجب الأخلاقي، وفي كثير من الحالات، القانوني لصاحب العمل بتوفير مستوى معقول من الرعاية تجاه موظفيه، والتخفيف من جميع المخاطر المتوقعة أو معالجتها والتي قد تضر أو تُصيب موظفيه، أو أولئك الذين يعملون نيابة عنه، أو من يتحمل مسؤولية معينة تجاههم.

إدارة المخاطر المؤسسية/التنظيمية: عملية تحديد وتقييم وإدارة ورصد مجموعة من المخاطر عبر المنظمة التي قد تؤثر على أهدافها وعملياتها والمساهمين فيها.

المرونة التنظيمية: قدرة المنظمة على التنبؤ، والاستعداد، والاستجابة، والتكيف مع التغيرات التدريجية والاضطرابات المفاجئة.

أهمية البرنامج: إطار يُستخدم لاتخاذ القرارات حول المخاطر المقبولة، يضمن التوازن بين تأثير واحتياجات البرامج والأنشطة والمخاطر الأمنية.

إدارة المخاطر الأمنية (SRM): العملية والمنهجية لتحديد التهديدات، وتقييم الثغرات والعواقب، وتخفيف المخاطر المتعلقة بأمن أصول المنظمة ومعلوماتها وموظفيها وعملياتها.

مقدمة

تُعتبر استراتيجية إدارة المخاطر الأمنية (SRM) القوية ضرورية للمنظمة لتحقيق مهمتها ورؤيتها. إن ترسيخ وتنمية ثقافة إدارة المخاطر الأمنية لا يقتصر على حماية الموظفين والمستشارين والمتطوعين والعمل مع المنظمات الشريكة؛ بل إنه بمثابة حافز لتحسين الكفاءة التشغيلية، والامتثال التنظيمي الأقوى، وزيادة ثقة أصحاب المصلحة. علاوة على ذلك، فإنه يؤسس الأساس لبرامج عالية الجودة ومبتكرة ومستدامة على المدى الطويل.

ولتحقيق هذه الغاية، يتطلب النهج الاستراتيجي الجيد لإدارة المخاطر الأمنية أن تقوم المنظمة بإجراء تحليل معمق للسياق التنظيمي ومجالات العمل، لتحديد نقاط القوة والضعف، وتعزيز التعاون الوظيفي المتبادل بين الفرق والأقسام بشكل فعال، وتعزيز وتمكين جميع جوانب البرامج والعمليات. كما يتطلب نهجًا تشاركيًا، حيث تقوم المنظمة بتقييم وتعديل توجهها باستمرار استجابةً للتعليقات الداخلية وتغيرات البيئة الخارجية.

تم تطوير هذه الموارد لتكون بمثابة دليل استراتيجي على مستوى عالٍ، حيث تُعَد إدارة المخاطر الأمنية (SRM) خطرًا تنظيميًا، وتقدم إرشادات شاملة حول كيفية التعامل مع قضايا إدارة المخاطر الأمنية عبر الوظائف واستغلالها كفرصة للتأثير ودعم استراتيجيات السياسات والوظائف التنظيمية الأوسع. يجب أن يتمتع المسؤولون عن قيادة إدارة المخاطر الأمنية (SRM) بالقدرة على التأثير على أعضاء مجلس الإدارة والإدارة العليا والقادة الوظيفيين الآخرين. من خلال توفير الروابط إلى المناقشات القطاعية الجارية وأفضل الممارسات، يمكن لهذا الدليل أن يساعد القادة في تزويدهم بالأدوات اللازمة لتقديم عرض استراتيجي لكيفية تأثير تحديات إدارة المخاطر الأمنية على المنظمة ككل، وضمان تحديد وتنفيذ حلول فعالة ومناسبة عبر الوظائف.

من المستهدف من هذا الدليل؟

تم تطوير هذا الدليل للموظفين في المقر الرئيسي/كبار المسؤولين المكلفين مباشرة بطوير وتنفيذ استراتيجية إدارة المخاطر الأمنية (SRM) التنظيمية. كما أنه ذو صلة للقادة الكبار من وظائف استراتيجية أخرى لمساعدتهم على فهم تأثير وأهمية إدارة المخاطر الأمنية (SRM) عبر جميع الوظائف والمواضيع.

كيفية استعمال هذا الدليل

تم تصميم هذا الدليل ليستخدمه كل من مختصي إدارة المخاطر الأمنية (SRM) وأولئك في الفرق المرتبطة بإدارة المخاطر الأمنية، مثل البرامج/العمليات، الموارد البشرية، تكنولوجيا المعلومات، المالية، والقانون. يوفر أدوات ونصائح حول كيفية دمج إدارة المخاطر الأمنية (SRM) عبر جميع الوظائف داخل المنظمة.

يتبع هذا الدليل هيكلًا خطيًا لتطوير استراتيجية شاملة لإدارة المخاطر الأمنية (SRM) ويتقدم نحو السياسات والتنفيذ عبر وظائف تنظيمية متنوعة. ومع ذلك، يركز كل فصل على منطقة محددة، مما يتيح للقراء التنقل مباشرة إلى القسم الأكثر صلة باستراتيجية إدارة المخاطر الأمنية الشاملة لمنظمتهم:

- **الفقرة 1** يتناول عملية تطوير استراتيجية لإدارة المخاطر الأمنية (SRM) وطرق دمجها في الاستراتيجية التنظيمية الأوسع.
- **الفقرة 2** يتناول عملية تطوير استراتيجية لإدارة المخاطر الأمنية (SRM) وطرق دمجها في الاستراتيجية التنظيمية الأوسع.
- **الفقرة 3** يتناول التكامل العملي لاستراتيجية إدارة المخاطر الأمنية (SRM) عبر سياسات ووظائف تنظيمية متنوعة.
- **الفقرة 4** يتناول كيفية تعزيز التنسيق والتعاون الاستراتيجيين الداخليين والخارجيين، بما في ذلك التعاون الأمني بين الوكالات.
- **الفقرة 5** يستكشف بناء المرونة التنظيمية من خلال نهج مرن لإدارة المخاطر الأمنية (SRM) وتعزيز الاستعداد للأزمات.
- أخيرًا، **الفقرة 6** يتناول دمج نظام الرصد والتقييم والمساءلة والتعلم (MEAL) ضمن استراتيجية شاملة لإدارة المخاطر الأمنية (SRM).

1

الفقرة 1
تطوير استراتيجية إدارة المخاطر الأمنية

2

الفقرة 2
حوكمة إدارة المخاطر الأمنية (SRM)

3

الفقرة 3
التكامل بين الوظائف

4

الفقرة 4
استراتيجية إدارة المخاطر الأمنية (SRM)
التنسيق والتعاون

5

الفقرة 5
مساهمة إدارة المخاطر الأمنية (SRM) في مرونة المؤسسات واستمرارية الأعمال

6

الفقرة 6
رصد وتقييم ومساءلة إدارة المخاطر الأمنية (SRM) (MEAL) والتعلم من

الفقرة 1: تطوير استراتيجية إدارة المخاطر الأمنية تطوير

بعبارات بسيطة، تعتبر استراتيجية إدارة المخاطر الأمنية (SRM) مهمة لأنها توحد منظمتك نحو هدف واحد يدعم رؤيتك ومهمتك. يمكن أن يساعد القيام بذلك في زيادة الشفافية في عملياتك الميدانية، مما يسهل اتخاذ القرارات على مستوى الإدارة العليا. بعبارة أخرى، يجب أن تلعب استراتيجية إدارة المخاطر الأمنية (SRM) دورًا رئيسيًا في تطوير، والمشاركة في تحقيق، الاستراتيجيات والسياسات التنظيمية الأوسع. يعد دمج استراتيجية إدارة المخاطر الأمنية (SRM) بهذه الطريقة أمرًا بالغ الأهمية ليس فقط لتبرير تخصيص الميزانية، ولكن أيضًا لكسب التفاعل والموافقة من القادة الاستراتيجيين في جميع مواقع المنظمة.

1.1 العناصر الأساسية لاستراتيجية إدارة المخاطر الأمنية (SRM)

تتم عادةً هيكلة استراتيجية إدارة المخاطر الأمنية على النحو التالي:

- مقدمة، يفضل أن تكون مكتوبة بواسطة الإدارة العليا، مثل الرئيس التنفيذي أو المدير العام أو أحد أعضاء مجلس الإدارة، لدعم خطتك.
- هدف أو بيان مهمة يتماشى مع استراتيجية المنظمة لدعم الرؤية الشاملة.
- المبادئ والقيم الخاصة بك (يجب أن ترتبط هذه بموقف المنظمة تجاه المخاطر ونهجها في واجب الرعاية).
- بيان السياق (خلفية للسياق الحالي الذي سيعمل إطار إدارة مخاطر الأعمال الخاص بك فيه - داخليًا (السياق التنظيمي) وخارجيًا (السياق التشغيلي).
- بين ثلاثة إلى ستة أهداف أو موضوعات أو أهداف استراتيجية تتوافق مع استراتيجية مؤسستك (انظر الأداة 1: تطوير الاتجاهات الاستراتيجية الخاصة بك).
- إرشادات التنفيذ والمراجعة (قصيرة المدى، متوسطة المدى، طويلة المدى).
- يمكنك أيضًا اختيار تضمين أي افتراضات مدمجة في خطتك، ومخطط لأصحاب المصلحة الرئيسيين، وتفاصيل الأدوار والمسؤوليات المحددة (انظر الفقرة 2).

1.2 دمج إدارة المخاطر الأمنية (SRM) ضمن الاستراتيجيات التنظيمية الأوسع

غالبًا ما تكون الاستراتيجيات التنظيمية مرتبطة بمسار نمو المنظمة، مما يمكن أن يترجم إلى زيادة التغطية، وتوسع الخدمات (وبالتالي زيادة عدد الموظفين)، وفتح مكاتب جديدة في الدول، أو الاستجابة للأزمات الناشئة بشكل مباشر أو من خلال الشركاء. تعتبر السلامة والأمن أمرين حاسمين لضمان تحقيق هذه الأهداف. لكن إدارة المخاطر الأمنية (SRM) ليست دائمًا مدرجة كعنصر عابر للوظائف، أو حتى كعنصر مستقل، في التخطيط لهذه الدورات البرمجية متعددة السنوات.

لا ينبغي النظر إلى إدارة المخاطر الأمنية (SRM) كنقاش أو نهج منفصل، أو إدخالها فقط لتطبيق استراتيجية معتمدة بشكل "آمن وموثوق". بدلاً من ذلك، ينبغي استخدام إدارة المخاطر الأمنية (SRM) كوسيلة لدعم المهمة والرؤية والأهداف الاستراتيجية للمنظمة (أنظر **الأداة 3: نموذج تخطيط إدارة المخاطر الأمنية**). يجب أن تُظهر استراتيجية إدارة المخاطر الأمنية (SRM) المحددة كيف ستساعد في تحقيق الأهداف طويلة الأجل للمنظمة، مع ضمان توفير مستوى جيد من الرعاية للموظفين والشركاء والزملاء، مع الحفاظ على فهم واضح لموقف المنظمة من المخاطر وحدودها (أنظر **القسم 1.5**).

لدمج إدارة المخاطر الأمنية (SRM) بسلاسة في الخطط الاستراتيجية الأوسع، من الضروري ربط استراتيجية SRM بنشاط مع جميع جوانب النهج الشامل للمنظمة. يتطلب تعزيز ثقافة تنظيمية جيدة ونهج لإدارة المخاطر الأمنية بذل الجهود لضمان فهم القيادة العليا لأهداف استراتيجية إدارة المخاطر الأمنية والاعتراف بتأثيرها الإيجابي على المنظمة ككل.

لمساعدتك في تسليط الضوء على هذه العلاقة، يجب أن تستخدم استراتيجية إدارة المخاطر الأمنية (SRM) نفس التنسيق، ونفس اللغة، ونفس الهيكل مثل استراتيجية المنظمة متعددة السنوات. على سبيل المثال، إذا كانت استراتيجيتك التنظيمية تتحدث عن "الاتجاهات الاستراتيجية" أو "المواضيع الاستراتيجية"، فقم بتكرار هذه الكلمات والعبارات في استراتيجية إدارة المخاطر الأمنية (SRM) الخاصة بك. تأكد من توضيح الأماكن التي ستساعد فيها إدارة المخاطر الأمنية (SRM) الوظائف الأخرى على تحقيق أهدافها الاستراتيجية (والعكس صحيح). على سبيل المثال، إذا كان أحد الأهداف طويلة الأجل لاستراتيجيتك التنظيمية هو "زيادة عدد الشركاء الوطنيين المشاركين في البرامج"، فعليك تحديد كيف ستساعد استراتيجيتك لإدارة المخاطر الأمنية (SRM) أو الأهداف المحددة في تحقيق هذا الهدف. على سبيل المثال، قد يبدو هذا على النحو التالي: 'ستقوم إدارة المخاطر الأمنية (SRM) بتطوير إجراءات تدقيق شاملة وتحديد أولويات الموارد لتمكين دعم أفضل للشركاء الوطنيين'.

إن وضع أهداف وغايات مع خطوط واضحة للمسؤولية، بالإضافة إلى مراقبة هذه الأهداف والإبلاغ عنها إلى فريق القيادة العليا الأوسع، سيساعد أيضًا على تعزيز وإدماج إدارة المخاطر الأمنية (SRM) في الناقشات على المستوى الاستراتيجي. (انظر **الأداة 2: كيفية تبرير استراتيجيتك لإدارة المخاطر الأمنية SRM**).

1.3 فهم البيئة التشغيلية والاتجاهات العالمية

جب أن تبدأ أي منهجية لتطوير استراتيجية واضحة لإدارة المخاطر الأمنية (SRM) بتحليل عميق للسياق الذي يُتوقع أن تعمل فيه إطار إدارة المخاطر الأمنية فيما يتعلق بالأولويات البرنامجية. ينبغي أن يأخذ هذا في الاعتبار السياق الخارجي (البيئي) والسياق الداخلي (التنظيمي).

يجب أن يأخذ تحليل البيئة الخارجية بشكل شامل بعين الاعتبار، على سبيل المثال:

- ما هي العلاقات التي تربط المنظمة بأصحاب المصلحة الخارجيين وما مدى أهمية هذه العلاقات؟ ما هي الاحتياجات أو المتطلبات التي يحتاجها أصحاب المصلحة المختلفون فيما يتعلق بإدارة المخاطر الأمنية (SRM)؟
- ما هي القوانين أو اللوائح أو القواعد أو المعايير التي تنطبق على منظمتك؟ كيف تؤثر هذه على متطلبات واجب الرعاية القانونية لديك؟
- ما هي الاتجاهات الخارجية المتعلقة بإدارة المخاطر الأمنية (SRM)؟ يمكن أن تشمل هذه التغييرات في توقعات الموظفين بشأن إدارة المخاطر الأمنية، والشراكات وتقاسم المخاطر، والتكنولوجيات الجديدة والابتكارات، أو اتجاهات أفضل الممارسات في القطاع.

يجب أن يأخذ تحليل السياق التنظيمي الداخلي بالاعتبار:

- ما هي أهداف المنظمة والأولويات البرنامجية وهيكل ومنهج التشغيل؟
- من هم أصحاب المصلحة الداخليين وكيف ينخرطون حاليا في إدارة المخاطر الأمنية؟ يجب أن يشمل ذلك شركاء تسليم.
- ما هي إجراءات/ عمليات الإدارة الموضوعة حاليا؟ هل هي فعالة؟
- ما هو الهيكل القانوني للمنظمة؟
- ما هي سياسات التأمين وما هي المساعدات الخارجية التي توفرها المنظمة؟

إن فهم تعقيدات منظمتك ككل في هذا الجانب من شانه أن يمنحك إمكانية صياغة استراتيجية إدارة مخاطر أمنية بارزة وعملية.

نصيحة هامة: منهجية تصميم الأنظمة لتطوير استراتيجية فعالة لإدارة المخاطر الأمنية

Systemcraft INSTITUTE

1. حدد استراتيجيتك من خلال التركيز على التعاون.

يجب ألا تُعتبر إدارة المخاطر الأمنية (SRM) نشاطًا منفصلًا أو مهارة تقنية يمكن فهمها فقط من قبل العاملين في هذا المجال. ترتبط إدارة المخاطر الأمنية (SRM) ارتباطًا مباشرًا بتوفير مستوى جيد من الرعاية القانونية وضمان استمرارية الأعمال، وبالتالي فهي ذات صلة بجميع وظائف المنظمة. عندما تعمل إدارة المخاطر الأمنية (SRM) بشكل جيد، يمكن للمنظمة أن تبقى مركزة على مهمتها وتحقق نتائج أفضل في البرامج. لذا، فإن من مصلحة الجميع أن تعمل إدارة المخاطر الأمنية (SRM) بفعالية. استخدم هذه اللغة واستمر في تكرارها عند مناقشة إدارة المخاطر الأمنية. تيسير التعاون من خلال تقييم الهياكل الحالية لمشاركة المعلومات واستخدامها. على سبيل المثال، إذا كان لديك لجنة لإدارة المخاطر في المنظمة، تأكد من أن الأمن جزء من هذه اللجنة.

2. تعيين اتجاه واضح (تكبير/تصغير).

تحتاج أي استراتيجية إلى توجيه واضح بالإضافة إلى إجراءات وأهداف قصيرة وطويلة الأجل لتمكين الأشخاص من التواصل والمشاركة. مثل الانطلاق في رحلة طويلة، يمكن اعتبار السعي نحو استراتيجية كعمل نحو وجهة محددة. يجب دائمًا أن تكون هناك نقاط توقف محددة على الطريق حيث يمكنك أن تأخذ لحظة للتوقف والتفكير وإعادة تقييم أهدافك وإجراءاتك قبل المتابعة. إن من شأن تحديد أهداف قصيرة المدى (ثلاثة أو ستة أشهر) وأهداف طويلة المدى (سنتين إلى ثلاث سنوات) أن يعبد الطريق نحو صياغة استراتيجية إدارة مخاطر أمنية.

3. اجعل الأمر مهمًا.

عند وضع استراتيجية، تأكد من أنها تأخذ بعين الاعتبار ما يهم أعضاء فريق القيادة الاستراتيجية الآخرين. إذا كان الناس بحاجة إلى إجراء تغييرات أو التكيف، فإنهم يحتاجون إلى فهم سبب أهمية ذلك بالنسبة لهم (ولفرقهم/أقسامهم). قم بالتوفيق بين دورة تطوير استراتيجية إدارة المخاطر الاستراتيجية مع الخطة الاستراتيجية الشاملة للمنظمة وتعبئة الموارد. يجب أن تُعترف إدارة المخاطر الأمنية كعامل تمكين رئيسي للنجاح، بنفس الطريقة التي يتم بها تحديد الاستثمارات في برامج التمويل والموارد البشرية الجديدة، أو تدفقات العمل، أو بناء القدرات، على سبيل المثال، كعوامل حيوية لنجاح خطة استراتيجية تنظيمية متعددة السنوات. تفاعل مع الإدارات الأخرى لمناقشة أهدافها الاستراتيجية واهتماماتها. ثم تواصل بلغة بسيطة يمكن فهمها من قبل الجميع، وأطّر الحديث بطريقة تتماشى مع اهتماماتهم وتجاربهم المحددة في إطار وظيفتهم.

نصيحة هامة: منهجية تصميم الأنظمة لتطوير استراتيجية فعالة لإدارة المخاطر الأمنية *مواصلة*

4. تغيير الحوافز

كل منظمة لها حدود عمل واضحة، وهذا في كثير من الأحيان يمكن أن يخلق إحجاماً عن التغيير. يمكن أن يساعد فهم بعض الأسباب التي تجعل الناس يتفاعلون أو لا يتفاعلون مع استراتيجيات إدارة المخاطر الأمنية في خلق وتأسيس حوافز جديدة. في بعض الأحيان، قد يكون هذا الأمر بسيطًا مثل تزويدهم بإمكانية الوصول إلى التكنولوجيا أو التطبيقات (مثل تطبيق الإبلاغ عن الحوادث) أو تبسيط بعض اللغة أو الإجراءات بحيث يسهل فهمها.

5. استغلال الذكاء الجماعي.

عادةً ما يكون الأشخاص في المناصب العليا هم من يقومون بتطوير وإعداد استراتيجيات إدارة المخاطر الأمنية، مُكيّفين إياها لتناسب "المستهلكين" (أي بقية المنظمة). يمكن أن يؤدي ذلك إلى انفصال بين أولئك الذين يضعون الاستراتيجية وأولئك الذين يتعين عليهم في النهاية تحويل الاستراتيجية إلى واقع عملي. المنظمات التي تعاني من ضعف في الذكاء الجماعي، مثل ضعف الوصول إلى المعلومات والتحليلات على مستوى الميدان، ستعزز عادةً الانفصال بين المناهج الاستراتيجية والتشغيلية. العمل نحو نهج تشاركي يستفيد من الذكاء الجماعي من جميع مستويات المنظمة، وخاصة من أولئك الذين يقومون بتنفيذ إدارة المخاطر الأمنية على المستوى الميداني، هو أمر أساسي.

الدكتور سيمبسون، ك، وراندال، إ. (2020)، "تصميم الأنظمة": مقدمة

نصيحة هامة: تعزيز نهج مرن لإدارة المخاطر الأمنية

- ✓ إجراء تحليل "SWOT" (انظر إلى **الأداة 4: قالب تحليل SWOT**) – تأمل في نقاط القوة والضعف في مؤسستك، بالإضافة إلى الفرص والتهديدات التي تقدمها بيئة العمل. تأكد من أخذ عناصر "PESTLE" في الاعتبار، وهي العوامل التي تكون خارج سيطرتك، ولكن قد تؤثر على عملياتك، مثل العوامل السياسية والاقتصادية والاجتماعية والتكنولوجية والقانونية والبيئية.
- ✓ قم بإجراء تمرين "العودة إلى الوراء" (Backcasting) - توصل إلى فهم مشترك للحالة النهائية المرغوبة في المستقبل، وابدأ بالعمل للخلف من خلال تحديد نقاط التوقف للوصول إلى هذه النتيجة المرجوة. حدد أهدافًا تكون (SMART) (محددة، قابلة للقياس، قابلة للتحقيق، ذات صلة، ومحددة بوقت) وحدد مجالات العمل. تأكد من الحفاظ على قنوات التقدم والتعليقات.

نصيحة هامة: تعزيز نهج مرن لإدارة المخاطر الأمنية *مواصلة*

- ✓ تأكد من توافق الرؤى - يجب أن يكون جميع الموظفين على المستوى الاستراتيجي على نفس الصفحة. اعمل على ضمان استخدامهم نفس اللغة، وأن تكون مؤشرات التقرير مكملة، وأن تكون الأهداف أهدافاً مشتركة. يجب أن تتماشى أهداف الفريق مع أهداف الوظيفة، التي يجب أن تتماشى بدورها مع الأهداف الاستراتيجية العامة للمنظمة.
- ✓ استعد للنزاع - يجمع العمل عبر الوظائف فرقًا قد تكون تقليديًا معزولة، مما قد يؤدي إلى تنافس الأفراد على النفوذ والموارد. من المهم أن تكون مستعدا للصراع. قد يعني ذلك منح الفرق المتعددة الوظائف الفرصة للفشل من أجل تحقيق إنجازات جديدة.
- ✓ يجب أن تكون استراتيجية إدارة المخاطر الأمنية (SRM) الخاصة بالمنظمة مرنة، بحيث تبقى ملائمة لجميع بيئات التشغيل الخاصة بك، لكنها يجب ألا تكون نهجًا موحدًا يناسب الجميع. المرونة هي المفتاح: يجب أن تكون استراتيجيات إدارة المخاطر الأمنية (SRM) تمكينية، وليست مكبلة.
- ✓ رفع الوعي - إن دمج الوعي في عمليات التوجيه وإجراء تدريبات منتظمة هي طرق سهلة لدمج إدارة المخاطر الأمنية عبر الوظائف في ثقافة المنظمة.

1.4 ضمان نهج مشترك لإدارة المخاطر

ونظرًا للترابط بين المخاطر المختلفة، فإن النهج التنظيمي المتكامل جيدًا ينبغي أن يأخذ في الاعتبار جميع مجالات إدارة المخاطر بدلاً من تقسيم المخاطر إلى وظائف مختلفة.

يجب على المنظمات عدم فصل أو تمييز خطر عن آخر، وينبغي أن تشكل إدارة المخاطر الأمنية جزءًا لا يتجزأ من نهج المنظمة تجاه إدارة المخاطر. عندما يتم الاعتراف بإدارة المخاطر الأمنية كعنصر حاسم في النهج العام للمنظمة تجاه إدارة المخاطر، يصبح من الأسهل تعزيز ثقافة أمنية شاملة وتشجيع دعم ومشاركة القيادة العليا عبر الوظائف المختلفة.

يجب أن يكون تطوير نهج متكامل لإدارة المخاطر في المنظمة جهدًا تعاونيًا، يستفيد من "الذكاء الجماعي (أنظر منهجية تصميم الأنظمة) لتقييم المخاطر الحرجة المتعلقة بالسلامة والأمان التي تواجهها المنظمة وتأثيرها المحتمل على استمرارية الأعمال.

يجب أن تكون إدارة المخاطر الأمنية (SRM) في مقدمة عملية اتخاذ القرار وجزءًا أساسيًا من أي دورة تخطيط لإدارة المخاطر. تجميع معلومات مخاطر الأمن، وعرضها بشكل متسق، ودمج هذه المعلومات في استراتيجيات إدارة المخاطر العامة للمنظمة أمر حيوي لإبلاغ السياسات والإجراءات وضمان توفير الموارد الكافية للتخفيف من هذه المخاطر عبر المنظمة.

نصيحة هامة: دمج إدارة المخاطر الأمنية (SRM) ضمن إدارة المخاطر التنظيمية:

1. استعمل لغة سهلة وغير تقنية.

قم بإزالة الإشارات والشروحات الفنية المفرطة من المحادثات والعروض التقديمية. بدلاً من ذلك، ركز على التحدث عن المخاطر من حيث أهداف العمل ونتائجه.

2. ربط إدارة المخاطر الامنية باستمرارية الأعمال وتخطيط إدارة الأزمات.

يجب النظر إلى إدارة المخاطر الأمنية باعتبارها آلية وقائية. يمكن أن يساعد ذلك في تحديد ودعم وتمكين أهداف العمل بالكامل، مع تسليط الضوء أيضًا على مشكلات السلامة والأمن المحتملة والعمل مع الإدارات الأخرى لإدارة هذه المخاطر والتخفيف منها.

3. ينبغي أن تكون المعلومات متاحة بسهولة.

ابدأ بمشاركة معلومات في الوقت الفعلي حول التهديدات الأمنية والسلامة الخارجية المحتملة، وعرض المساعدة على رؤساء الوظائف لتقييم ما إذا كانت هذه التهديدات ستؤثر على مجالات مسؤوليتهم وكيف ستؤثر عليها. يمكن أن يتضمن ذلك مساعدتهم في تحديد المحفزات المحددة، وإرساء تدابير التخفيف، وتحديد حدود المخاطر.

تحليل ومشاركة الاتجاهات الداخلية المتعلقة بالسلامة والأمن أمر حاسم أيضًا لإظهار القيمة للوظائف الأخرى في المؤسسة. إن مشاركة المعلومات والتعرف على الحوادث والمواقف التي كادت تقع في مؤسستك تمكن الوظائف الأخرى من اكتساب فهم ملموس لكيفية ولماذا تشكل مخاطر السلامة والأمن أهمية بالنسبة لهم.

4. قم بتطوير وعيك بشأن عوامل الخطر وقياس بيانات المخاطر.

لقد ساعد الذكاء الاصطناعي في إنشاء العديد من تطبيقات جمع معلومات البيانات، التي يمكنها جمع تقارير عن الحوادث المحتملة والاتجاهات عبر المواقع وداخل مجالات البرامج المختلفة. يمكن أن يساعد استخدام هذه الأدوات والبيانات التي تنتجها المنظمات في دعم وتوجيه تقييمات المخاطر النوعية بناءً على تفسيرات أكثر ذاتية، ويقدم طبقة إضافية من المعلومات المبنية على البيانات الكمية.

5. تأكد من وجود المساءلة والوعي على مستوى الإدارة العليا.

بينما يتحمل قادة المخاطر مسؤولية إدارة المخاطر، فإن المجلس التنفيذي وكبار التنفيذيين يتحملون مسؤولية الإشراف على المخاطر المؤسسية. العمل على ضمان الالتزام والمساءلة من جانب هؤلاء القادة، أو على الأقل من جانب "بطل" واحد، لتحديد اللهجة الصحيحة والتواصل بوضوح بشأن أهمية إدارة المخاطر المؤسسية في جميع مواقع المنظمة.

1.5 تحديد استراتيجية إدارة المخاطر الأمنية (SRM) استنادًا إلى المخاطر التنظيمية

يجب أن تستند استراتيجية إدارة المخاطر الأمنية (SRM) الناجحة إلى نهج المنظمة تجاه المخاطر، وخاصةً (أ) موقفها من المخاطر (ب) تحملها للمخاطر و(ج) عتبات المخاطر. يمكن أن تختلف هذه بشكل كبير اعتمادًا على تفويض المنظمة، ورؤيتها، وعملياتها، فضلاً عن متطلبات المانحين.

التعاريف الرئيسية

- **الموقف من المخاطر** هو مقدار المخاطر التي تكون المنظمة مستعدة لقبولها لتحقيق أهدافها.
- **تحمل المخاطر** هو المستويات المقبولة من التباين في موقف المنظمة من المخاطر بناءً على ظروف محددة.
- **حدود المخاطر** هي أقصى مستوى من التعرض الذي تكون المنظمة مستعدة لقبوله..

"يُعتبر بيان الموقف من المخاطر (الشهيّة) بشكل عام أصعب جزء في أي تنفيذ لإدارة المخاطر المؤسسية." ومع ذلك، في غياب لدرجة التخمل المحددة بوضوح والتي يمكن قياسها، فمن الممكن القول إن دورة المخاطر بأكملها وأي إطار عمل للمخاطر قد توقفت."
معهد إدارة المخاطر

الاستجابة للمخاطر يمكن أن تتخذ أشكالًا عديدة، وقد الوكالة الأمريكية للتنمية الدولية حددت ما يلي:

- تجنب المخاطر من خلال عدم اتباع نهج معين أو عدم توقيع اتفاقية مع شريك معين.
- الحد من المخاطر من خلال نظام قوي للرقابة الداخلية، أو تدابير تخفيف مستهدفة، أو جهود التدريب وبناء القدرات، وغيرها من الخيارات.
- مشاركة المخاطر من خلال الشراكات الاستراتيجية مع الجهات الفاعلة الرئيسية.
- قبول المخاطر دون التخفيف منها، مع اتخاذ الاحتياطات المناسبة.

يمكن أن يكون اتخاذ القرار بشأن التوازن بين أهمية البرنامج (العملية التي تحدد مستويات المخاطر المقبولة للمنظمة تجاه برامجها) وإدارة المخاطر الأمنية (SRM) معقدًا، ولا توجد مقاربة واحدة تناسب الجميع (أنظر القسم 1.6 حول كيفية تطوير إطار أهمية المشروع).

يجب على القادة الاستراتيجيين و/أو القيادة العليا النظر في توضيح المستوى من المخاطر التي ترغب المنظمة في تحملها والتي لا ترغب في تحملها في سبيل تحقيق مهمتها وأهدافها الاستراتيجية. يجب أن يتماشى هذا مع قدرتها على تحمل المخاطر، أي مستويات المخاطر (التسامح) التي يمكنها تحملها فيما يتعلق ببصمتها التشغيلية ومواردها، فضلاً عن قدراتها وخبرتها في إدارة المخاطر.

يمكن أن يتخذ ذلك شكل بيان حول الموقف من المخاطر. (أنظر **أداة 5: أمثلة على بيانات الموقف من المخاطر**) بالإضافة إلى تحديد مستوى تحمل المخاطر التنظيمية والحدود التي لن يستمروا في العمل بعدها (أنظر **الأداة 6: إنشاء نهج تنظيمي لإدارة المخاطر**).

نصيحة هامة: الفروق بين الموقف من المخاطر، التسامح والحدود:

فكر في المخاطر المرتبطة بالقيادة. تدرك المنظمات أن هناك مخاطر متأصلة مرتبطة بالقيادة، وكلما زادت سرعة السيارة، زادت المخاطر. ومع ذلك، لا يُمكن لأي منظمة أن تُصرّ على عدم السفر في المركبات على الإطلاق أو القيادة بسرعة 10 أميال في الساعة بشكل مستمر، حيث إن ذلك يعني أنها لن تصل أبدًا إلى وجهتها أو أهدافها الاستراتيجية.

لذا، تكون المنظمات مستعدة لقبول مستوى معين من المخاطر، لكنها قد تضع تدابير تخفيف معينة للمساعدة في إدارة هذه المخاطر. على سبيل المثال، ارتداء أحزمة الأمان أو وضع حدود للسرعة سيشكلان تدبيرين للتخفيف من المخاطر. يشار إلى هذا النهج في إدارة المخاطر غالبًا باسم "موقف المؤسسة تجاه المخاطر" أو "شهية المؤسسة لمجابهة المخاطر".

ولكن في الواقع، هناك عادة مجال للمناورة حيث تكون المنظمة مستعدة لإظهار المرونة. هذا ما يسمى بتحمل المخاطر. هذا مشابه لكيفية عدم احتمال أن يوقف ضابط الشرطة سائقًا ويصدر له مخالفة مرورية إذا كان يسير بسرعة أقل من 10 في المئة فوق الحد الأقصى للسرعة. ومع ذلك، فإن تجاوز هذا المستوى من التحمل سيؤدي في النهاية إلى وقف أي قيادة. هذا ما يسمى بحدود المخاطر.

تشابل، م، (2023): الرغبة في المخاطرة مقابل تحمل المخاطر؛ ما الفرق بينهما؟

يمكن أن يتيح إنشاء بيان عن الموقف التنظيمي تجاه المخاطر، يتعلق بإدارة المخاطر الأمنية (SRM)، إجراء تقييمات أكثر دلالة للمخاطر التي تتعلق بتحقيق الأهداف التنظيمية. بدون الإطار الذي يوفره موقفك تجاه المخاطر، يصبح من الأصعب على فرق إدارة المخاطر الأمنية (SRM) تنفيذ الإجراءات عند الحاجة. علاوة على ذلك، يُترك الموظفون في جميع مواقع المنظمة بدون المعلومات اللازمة لاتخاذ القرارات اليومية التي تتماشى مع النهج الاستراتيجي لإدارة المخاطر الأمنية (SRM).

تشجيع الموظفين على اتخاذ مخاطر مستنيرة ومناسبة، بناءً على نهج المنظمة تجاه المخاطر (وقدرتها على التكيف عند الحاجة)، يمكن أن يساعد في كسر التصور بأن إدارة المخاطر الأمنية (SRM) هي "عائق" أمام فرق البرامج لتحقيق أهدافها. يمكن أن يؤدي إنشاء نهج واضح ومتسق للمخاطر، يتم التواصل عنه بشكل جيد وفهمه على جميع المستويات، إلى تعزيز علاقات عمل أفضل بين وظيفة إدارة المخاطر الأمنية (SRM) وبقية المنظمة.

نصيحة هامة: كيفية صياغة بيان الموقف من المخاطر في إدارة المخاطر الأمنية

تعيين السياق: قدم شرحًا موجزًا عن كيفية ارتباط مخاطر إدارة المخاطر الأمنية (SRM) بالاستراتيجية العامة للمنظمة وكيف يمكن أن تؤثر عليها، استنادًا إلى مهمتها وأهدافها وغاياتها والسياق التشغيلي. هل هناك أي عوامل خارجية يجب أخذها بعين الاعتبار؟

تحديد الحدود: حدد بوضوح ما هي المواقف التي لا تقبل المخاطر على الإطلاق، وما هي المواقف التي تتطلب الحذر، ولماذا يمكن أن يكون هناك في بعض الظروف مستوى أعلى من تقبل المخاطر (مثل متطلبات المانحين أو المواقع ذات المخاطر العالية). يمكن تصور حدود المخاطر على طيف أو باستخدام المعدلة **مصفوفة قرار أيزنهاور** التي تتراوح من "تجنب"، "حذر"، "فتح"، إلى "قبول".

تعيين المؤشرات: حدد مؤشرات المخاطر الرئيسية التي ستُستخدم لتقييم ما إذا كانت المنظمة تعمل ضمن حدود المخاطر، أو بجوارها منها، أو خارجها. ستساعد هذه المؤشرات أيضًا في تحديد مسار العمل المتعلق بإدارة المخاطر المختلفة.

دونوفان، ل (2022)، "ما هي الشهية لمجابهة المخاطر وكيف يتم تنفيذها؟"، شبكة قيادة المخاطر.

نظرًا لأن الموقف تجاه المخاطر غالبًا ما يكون مقياسًا نوعيًا، يجب على القادة الاستراتيجيين أيضًا النظر في كيفية التواصل بشأن الموقف الاستراتيجي تجاه المخاطر مع الموظفين في جميع مواقع المنظمة وكذلك مع المنظمات الشريكة. إذا تم اعتبار إدارة المخاطر الأمنية (SRM) عملية تشاركية عبر المنظمة، تتضمن ليس فقط موظفي الأمن، فإن ذلك يمكن أن يمنع الفجوة بين القرارات التي تتخذها الإدارة العليا على مستوى المقر والقرارات التي يتخذها الموظفون الميدانيون.

طرق بسيطة لتأسيس وتفعيل الموقف من المخاطر فيما يتعلق بإدارة المخاطر الأمنية (SRM) وما بعدها:

- ✓ ملصقات تحمل مرئيات واضحة حول حدود المخاطر الرئيسية، مثل عدم التسامح مطلقًا مع التحرش الجنسي أو عدم القيادة بعد حلول الظلام. يجب أن تتضمن هذه الملصقات تفاصيل الاتصال في حال الحاجة إلى مزيد من التوجيه.
- ✓ خطوط واضحة من المسؤولية - يجب على الموظفين معرفة من يمكنهم الرجوع إليه للحصول على النصيحة أو التوجيه فيما يتعلق بالموقف من المخاطر والحدود.
- ✓ التوافق مع الموقف من المخاطر كعنصر دائم في جدول أعمال اجتماعات تخطيط البرامج.
- ✓ قنوات اتصال سهلة عندما يحتاج الموظفون أو الشركاء إلى توجيه. قد يشمل ذلك اجتماعات دورية لمراجعة المخاطر، توجيهات فورية، قنوات اتصال مخصصة أو عناوين بريد إلكتروني لتلقي الاستفسارات وتقديم الدعم.
- ✓ إدراج سياسات وإجراءات وممارسات إدارة المخاطر الأمنية (SRM) في حزم التوجيه للموظفين الجدد.

✓ قائمة من 10 قواعد ذهبية على الأكثر، تكون سهلة الفهم وقابلة للترجمة، وتقدم توجيهات واضحة حول حدود المخاطر في منظمتك وأي 'موانع' محددة لا يمكن تجاوزها. يجب أن تكون هذه القواعد قابلة للتكيف مع السياقات المختلفة وسهلة الفهم من قبل المنظمات الشريكة والموظفين على جميع المستويات.

1.6 تحقيق التوازن بين أهمية البرنامج والموقف من المخاطر في إدارة المخاطر الأمنية (SRM)

الدافع الإنساني والحاجة إلى الوصول إلى المجتمعات التي يصعب الوصول إليها هما من المحركات الرئيسية في قطاع المنظمات غير الحكومية. غالبًا ما يمكنهما دفع حدود موقف المنظمة تجاه المخاطر. ومع ذلك، يجب التوفيق بين أهمية البرامج مع المخاطر المحتملة على السلامة والأمن، والتأثير الذي قد تشكله هذه المخاطر على استمرارية العمل في المنظمة. على سبيل المثال، قد تؤثر وفيات الموظفين على السمعة وقد تؤدي إلى أضرار مالية إذا قرر المانحون سحب تمويلهم.

تحديد كيفية تحقيق التوفيق بين تلبية الأهداف الاستراتيجية العامة للمنظمة والمخاطر الأمنية المحتملة أمر بالغ الأهمية. يمكن أن يوفر 'إطار أهمية البرنامج' عملية منظمة لهذا القرار. يمكن أن يساعد أيضًا المنظمة في التوفيق بين المخاطر المتبقية مقابل الالتزامات تجاه المبادئ الإنسانية، لا سيما تلك التي توجه من يتم مساعدته، ومبادئ الإنسانية وعدم التحيز.

نصيحة هامة: أدوات للتوفيق بين أهمية البرنامج وتقييم المخاطر الأمنية

إطار أهمية البرنامج هو نظام الأمم المتحدة لاتخاذ القرارات بشأن المخاطر المقبولة. تحدد هذه المبادئ التوجيهية نهجًا هيكليًا منظّمًا لضمان توافق الأنشطة التي تشمل موظفي الأمم المتحدة مع المخاطر الأمنية.

مجموعة توجيهية بشأن الأهمية الحاسمة لبرامج الأمم المتحدة (2016)، إطار الأهمية الحاسمة لبرامج منظومة الأمم المتحدة، CEB/2016/HLCM/23

غالبًا ما يُكلف مدراء المخاطر الأمنية باتخاذ قرارات أو تقديم نصائح للفرق البرنامجية والتشغيلية بمجرد أن يتم تطوير الاستراتيجية البرنامجية والموافقة عليها. كبديل، يجب أن تشارك إدارة المخاطر الأمنية في المناقشات الاستراتيجية حول الموقف من المخاطر في مرحلة التخطيط. يجب أن تكون المعلومات حول المخاطر الأمنية وتحليلها جزءًا من أي قرار بشأن الأنشطة والبرامج.

إن شكيل لجنة لإدارة المخاطر متعددة الوظائف، مع وجود تمثيل لإدارة المخاطر الأمنية، هو وسيلة ممتازة لإدارة هذا الأمر. يجب أن تجتمع اللجنة بانتظام لمناقشة المخاطر والتهديدات والمخاوف الناشئة، وأن تمتلك السلطة لاتخاذ القرارات. على سبيل المثال، يمكن للجنة أن تقرر ما إذا كانت منطقة جديدة من البرمجة، سواء كانت جغرافية أو تقنية، تتوافق مع نهج الموقف من المخاطر الخاص بالمنظمة أو تتجاوزه. أنظر الفقرة 2 لمعرفة المزيد.

موارد مفيدة

- أداة تصميم الأنظمة - مقدمة
- التخطيط الاستراتيجي للمنظمات غير الحكومية: دليل لفهم أسس التخطيط الاستراتيجي
- كيفية القيام بالتخطيط الاستراتيجي: دليل للمنظمات غير الحكومية الصغيرة ومنظمات الشتات - إنترأك

منظمة العفو الدولية

سوريا

باحثون من منظمة العفو الدولية يجمعون الأدلة حول الغارات الجوية. إن الوصول إلى مناطق خطرة مثل هذه يمكن أن يتجاوز حدود موقف المنظمة من المخاطرة.

الفقرة 2: حوكمة إدارة المخاطر الأمنية (SRM)

الحوكمة الجيدة والهياكل المسؤولة هما العمود الفقري لأي إطار عمل فعال لإدارة المخاطر الأمنية. يتحمل الموظفون في جميع المستويات داخل المنظمة درجة من المسؤولية عن أمنهم الشخصي. لكن المنظمات مسؤولة عن ضمان وجود هياكل حوكمة فعالة وأن الموظفين على دراية وفهم بأدوارهم ومسؤولياتهم ضمن هذه المنظومة.

تشير حوكمة إدارة المخاطر الأمنية (SRM) إلى أن المنظمة تسيطر بشكل نشط المخاطر التي تواجهها وتوفر توجيهًا لأمان منظمتها. يجب على المنظمات، بغض النظر عن حجمها وتعقيد مهمتها ومدى عملياتها، أن تضمن وجود هيكل حوكمة مناسب أثناء العمل في بيئات معقدة ومتغيرة باستمرار.

2.1 وضع إدارة المخاطر الأمنية (SRM) ضمن إطار حوكمة المخاطر التنظيمية

يجب وضع إدارة المخاطر الأمنية (SRM) ضمن هيكل إدارة المخاطر في المنظمة، بحيث تعزز ثقافة إيجابية تمتد عبر كامل المنظمة. سيختلف هذا بناءً على حجم المنظمة، وموقفها من المخاطر، وطريقة تنفيذ البرامج. لكن المفتاح للنجاح هو التأكد من أن موقعه مناسب للمنظمة.

يجب على المنظمات أن تقرر من هو الوصي النهائي على كل جانب من جوانب استراتيجية إدارة المخاطر الأمنية، وكيفية ضمان نهج متكامل لإدارة ذلك ضمن إطار الالتزام العام بالرعاية، حتى لا يتم إغفال أو تفويت أي شيء. يجب على المنظمات أن تفكر في استخدام مصفوفة المسؤولية والمسائلة والاستشارة والإبلاغ RACI لمساعدتها في تحليل ذلك بشكل مفصل.

نصيحة هامة: مصفوفة المسؤولية والمسائلة والاستشارة والإبلاغ

يشير الاختصار RACI إلى:

- **R** – المسؤولية
- **A** – المسائلة
- **C** – الاستشارة
- **I** – الإبلاغ

نصيحة هامة: مصفوفة المسؤولية والمسائلة والاستشارة والإبلاغ مستمر

المسؤولية

هؤلاء الأشخاص هم "المنفذون" للعمل (المديرين الوظيفيين). يجب عليهم إكمال المهمة أو اتخاذ القرار يمكن أن يكون أكثر من شخص مسؤولاً بشكل مشترك.

المسائلة

هذا الشخص هو "صاحب" العمل. يجب عليهم التوقيع أو الموافقة عند اكتمال المهمة أو الهدف أو القرار. يجب على هذا الشخص التأكد من توزيع المسؤوليات في المصفوفة لجميع الأنشطة ذات الصلة. هناك شخص واحد فقط مسؤول، مما يعني أنه لا يمكن مسائلة شخص آخر.

الاستشارة

هؤلاء هم الأشخاص الذين يتعين عليهم تقديم مدخلاتهم قبل أن يتم إنجاز العمل والتوقيع عليه. هؤلاء الأشخاص مشاركون ونشطون.

الإبلاغ

يجب إبقاء هؤلاء الأشخاص على دراية بما يحدث. إنهم يحتاجون إلى تحديثات بشأن التقدم أو القرارات، ولكن لا يلزم استشارتهم رسميًا، ولا يساهمون بشكل مباشر في المهمة أو القرارات.

يُمكن تحديد الأشخاص المسؤولين من خلال تطوير التوجهات الاستراتيجية لمنظمتك. (كما رأينا في القسم 1.2).

دائرة الأمم المتحدة للأعمال المتعلقة بالألغام في جنوب السودان

جنوب السودان

يرتدي أحد أعضاء الفريق معدات وقائية أثناء العمل على إزالة الألغام الأرضية. على الرغم من أن المنظمات يجب أن تضمن وجود بروتوكولات فعالة للسلامة والأمن، فإن الموظفين يتحملون أيضًا بعض المسؤولية عن سلامتهم.

يمكن أن يبدو نموذج مصفوفة المسؤولية والمسائلة والاستشارة والإبلاغ RACI لإدارة المخاطر الأمنية كما يلي:

المهمة/ أصحاب المصلحة	كل لموظفين	نقطة الاتصال الأمنية داخل الدولة (SFP)	المدير القطري / الجهوي	مدير الأمن العالمي	لجنة إدارة المخاطر	قادة وظائف أخرى (على سبيل المثال البرامج والموارد البشرية)	الرئيس التنفيذي/ الرئيس المالي/ الرئيس التشغيلي	مجلس الإدارة/ الأمناء
المهمة 1: اعتماد سياسة السلامة والأمن العالمية	I	C	C	C	R	C	A	I
المهمة 2: تحديد عتبة الموقف من المخاطر	I	C	C	C	R	C	A	I
المهمة 3: تطوير/تنفيذ إطار إدارة المخاطر الأمنية (خطط الأمان والسلامة للبلد، ملخصات الأمان، خطة إدارة الحوادث)	C	R	R	R	A	I	I	I
المهمة 4: تطوير سياسة إدارة مخاطر السفر	I	C	C	R	R	C	A	I
المهمة 5: تطوير خطة إدارة الأزمات التنظيمية	I	C	C	C	R	R	A	I
المهمة 6: بناء القدرات من خلال التدريب على إدارة المخاطر الأمنية	I	R	R	R	A	I	I	I
المهمة 7: مراجعة الحوادث، وتحديد إجراءات المتابعة، ومشاركة الدروس المستفادة	I	R	R	R	A	I	I	I
المهمة 8: مراجعة سياسة وإطار إدارة المخاطر الأمنية (SRM)	I	C	C	C	R	C	A	I

المسؤولية والمسائلة والاستشارة والإبلاغ

R – المسؤولية
الأشخاص الذين يقع على عاتقهم تنفيذ المهام. هم المسؤولون عن تنفيذ الأعمال واتخاذ القرارات. يمكن أن يكون هناك أكثر من شخص مسؤول عن مهمة معينة، ولكن لجعل عملية اتخاذ القرار فعّالة، حاول تعيين شخص واحد فقط مسؤول عن كل مهمة.

A – المسائلة
الأشخاص المسؤولون عن تنفيذ المهمة أو تحقيق النتائج. قد لا يقومون بالعمل بأنفسهم، ولكنهم مسؤولون عن التأكد من إنجازه بشكل نهائي. لتفادي لتجنب الالتباس وتفريق المسؤولية، من الأفضل أن يكون هناك شخص واحد مسؤول عن كل مهمة في المشروع.

C – الاستشارة
الأشخاص أو الدور أو المجموعة التي ستساعد في إكمال المهمة. سيتواصلون بشكل ثنائي مع الأشخاص المسؤولين عن المهمة من خلال تقديم المدخلات والملاحظات المتعلقة بإتمام المهمة.

I – الإبلاغ
الأشخاص أو الأدوار أو المجموعات التي تحتاج إلى متابعة مستمرة لتقدم المهمة. لن يكون لديهم تواصل ثنائي الاتجاه، ولكن من الضروري إبقاؤهم على اطلاع، حيث سيتأثرون بالنتيجة النهائية للمهمة/المشروع.

متبنى من طرف السلامة الدولية في المواقع من نموذج وفرته الأكاديمية من أجل الإبتكار.

فهم هيكلية الحوكمة لإدارة المخاطر في المنظمة بهذه الطريقة يمكّنك من ضمان تخصيص جميع جوانب إدارة المخاطر الأمنية (SRM) وتحديد المجالات التي يجب أن تشارك فيها الوظائف الأخرى، وكيفية مشاركتها (مثل البرامج، الموارد البشرية، الشؤون القانونية، والالتزامات المالية). تم تفصيل هذه الروابط في **الفقرة 3**.

مع ضمان اتباع نهج متعدد الوظائف في إدارة المخاطر الأمنية (SRM)، من المهم أيضًا مراعاة اتباع نهج شامل وتشاركي. إن تعزيز ثقافة إدارة المخاطر الأمنية (SRM) يمر بالضرورة عبر إشراك جميع أصحاب المصلحة الرئيسيين. سيتيح هذا التفاعل فهم الواقع التشغيلي للعواقب المحتملة لهذه السياسات، كما سيُمكّن الأشخاص المسؤولين عن تحقيق أهداف المنظمة، ويعزز ثقافة إيجابية ومستدامة حول إدارة المخاطر الأمنية (SRM).

2.2 بناء هيكل فعال للسلامة والأمن

يمكن أن يختلف هيكل وظيفة السلامة والأمن في المنظمة بناءً على عوامل مثل حجم المنظمة، وحجم ودرجة تعقد برامجها، ونضج نهجها في إدارة المخاطر، وهيكلها الوظيفي. من الضروري إذن أن يضمن القادة الكبار أن تكون إدارة المخاطر الأمنية (SRM) مطروحة بطريقة تمكّن المنظمة من تحقيق أهدافها البرنامجية ورسالتها. يشمل ذلك دمج إدارة المخاطر الأمنية (SRM) في إطار حوكمة إدارة المخاطر، مما يمنحها دورًا هامًا في عمليات صنع القرار.

يجب على جميع المنظمات، بغض النظر عن هيكلها، أن تفكر في إنشاء مجموعة عمل مشتركة عبر الأقسام، أو لجنة، أو مجموعة توجيه تمثل أدوارًا ومستويات مختلفة داخل المنظمة. يجب تحديد أعضاء اللجنة من مختلف الوظائف مع تعريف المسؤوليات الأساسية ضمن مصفوفة المسؤولية والمسائلة والاستشارة والإبلاغ لإدارة المخاطر الأمنية. تشجع هذه المقاربة الجماعية على شعور أكبر بالمسؤولية، مما يساعد في النهاية على التنفيذ والامتثال. (أنظر **الأداة 7: مثال على الشروط المرجعية (ToR) للجنة إدارة المخاطر**).

تملك بعض المنظمات قسما كاملا مخصصا للأمن والسلامة، بينما تدمجه منظمات أخرى في وظائف أخرى في ما يخص الهيكل، تضع بعض المنظمات اعتبارات أساسية تتماشى مع ما يلي:

- هل يمكن تزويد استراتيجيتنا لإدارة المخاطر الأمنية (SRM) بالموارد المناسبة (البشرية والمالية) ضمن هيكلنا الحالي؟
- هل لدينا المعرفة المناسبة بالسلامة والأمن بين الوظائف التي تتحمل مسؤوليات إدارة المخاطر الأمنية (SRM)؟
- هل لدينا ثقافة مناسبة داخل المنظمة لضمان تنفيذ استراتيجيتنا بشكل فعال؟
- هل لدينا البنية التحتية الناعمة والبنية التحتية المادية اللازمة لدعم تنفيذ استراتيجية إدارة المخاطر المستدامة؟ يمكن أن تشمل البنية التحتية الناعمة رأس المال البشري، والتدريبات الشاملة، وإطارًا سياسيًا قويًا، واتفاقيات مع مقدمي الخدمات الخارجيين. يمكن أن تشمل البنية التحتية الصلبة أجهزة الاتصالات، معدات الحماية الشخصية، والمجمعات المكتبية الآمنة.

إذا كانت الإجابة "لا" على أي من هذه الأسئلة، فيجب على المنظمة إما إعادة هيكلة أو تحسين مهارات موظفيها لضمان الأداء الفعال.

فيما يتعلق بالهيكل، لا يوجد حل واحد يناسب الجميع في هذه الحالة. ولكن هناك بعض الاعتبارات الأساسية التي يجب أخذها بعين الاعتبار فيما يتعلق باحتياجات المنظمة، والتي قد تتطور مع مرور الوقت. هناك ثلاث هياكل شائعة تستخدمها المنظمات:

- المواقع الأمنية المنظمة
- المسؤوليات الأمنية المضمنة
- مقدمي خدمات الأمن الخارجيين.

إن اختيار الأشخاص المناسبين، في الأدوار المناسبة، للقيادة في مجال الأمن هو مفتاح نجاح أي منظمة. تتضمن أمثلة الأدوار المختلفة ما يلي:

المواقع الأمنية المنظمة

أفراد مختصون في إدارة المخاطر الأمنية، موضوعة في مستويات رئيسية داخل المنظمة، ولديهم أدوار ومسؤوليات مخصصة فقط لإدارة المخاطر الأمنية. يمكن أن يكون ذلك على المستوى العالمي أو الإقليمي أو الوطني. ليس من الضروري أن تكون هذه المناصب على جميع المستويات، ولكن حيثما تكون الحاجة إليها أكبر.

المزايا: تسمح للخبراء في إدارة المخاطر الأمنية عبر المنظمة بتطوير وتنفيذ وضمان أطر إدارة المخاطر الأمنية. توفر خطوط واضحة للمسؤولية والمحاسبة عن إدارة المخاطر الأمنية داخل المنظمة.

العيوب: لا تضمن دائمًا ثقافة أمنية إيجابية. يمكن أن تصبح الأقسام الأمنية معزولة، لذا تحتاج هذه الطريقة إلى جهد كبير لضمان التعاون بين أقسام إدارة المخاطر الأمنية وغيرها من الوظائف، بالإضافة إلى ضمان شعور جماعي بالوعي والمسؤولية. العنصر الأكثر أهمية هو أن يدرك القادة الحاجة إلى إدارة المخاطر الأمنية النشطة كجزء من تقديم البرامج الفعّالة

المسؤوليات الأمنية المضمنة

لا تمتلك بعض المنظمات الموارد، أو تفضل ببساطة تضمين مسؤوليات الأمن ضمن أدوار أخرى.

المزايا: إذا تم توفير أطر قوية لإدارة المخاطر الأمنية، وتم تزويد الأفراد بالوقت والدعم والتدريب، فإن ذلك يتيح فرصة رائعة لتمكين الأفراد وخلق ثقافة أمنية إيجابية تكون مدمجة بشكل جيد ضمن الهيكل التنظيمي.

العيوب: إن دمج المسؤوليات الأمنية يعتمد على ضمان أن الأفراد المحددين يمتلكون كل من المعرفة والفهم لإدارة المخاطر الأمنية، فضلاً عن القدرة على تنفيذ هذه المسؤوليات جنبًا إلى جنب مع واجباتهم الأخرى. غالبًا ما تفشل المنظمات عند محاولة دمج مسؤوليات إدارة المخاطر الأمنية بسبب عدم ضمان توفير الوقت الكافي، أو الدعم، أو التدريب للموظفين.

مقدمي خدمات الأمن الخارجيين

بعض المنظمات تستعين بمستشارين خارجيين للأمن، إما للعمل كممثلين وحيدين لإدارة المخاطر الأمنية داخل منظماتهم، أو لدعم وظائف أخرى لا تملك القدرة أو المهارات التقنية لإدارة المخاطر الأمنية.

المزايا: يمكن لمقدمي خدمات الأمن الخارجي أن يجلبوا خبرة واسعة وروابط إلى شبكات إدارة المخاطر الأمنية الأوسع، فضلاً عن معرفتهم بأفضل الممارسات في القطاع. يمكنهم أيضًا تقديم وجهة نظر خارجية مفيدة ومنظور غير متحيز، مما قد يكون مفيدًا عندما تحتاج إلى اتخاذ قرارات صعبة، أو لإجراء مراجعات خارجية والتوصيات المرتبطة بها.

العيوب: لا يمتلك مقدمو الخدمات الخارجيون بالضرورة (أو يحتاجون إلى وقت لتطوير) المعرفة المدمجة بالمنظمة وهياكلها ونهجها الثقافي تجاه إدارة المخاطر الأمنية. يمكن أن يفتقروا أيضًا إلى العلاقات الداخلية والروابط التي قد تكون ضرورية لتنفيذ وتطبيق أطر إدارة المخاطر الأمنية. من الجدير بالذكر أن الاعتماد المفرط على مقدمي الخدمات الخارجيين يمكن أن يقلل من المسؤولية، وفي النهاية يضعف القدرة الداخلية والمعرفة المؤسسية.

2.3 أدوار ومسؤوليات إدارة المخاطر الأمنية (SRM)

يجب أن تكون الأدوار والمسؤوليات المتعلقة بإدارة المخاطر الأمنية (SRM) محددة بوضوح، بحيث تُظهر من هو المسؤول عن تقديم المشورة الأمنية، ومن يتخذ القرارات. سيساعدك استخدام مصفوفة RACI وفهم كيفية هيكلة الأمن في المنظمة على تحديد الأدوار والمسؤوليات بشكل فعال.

نصيحة هامة: اعتبار المسميات الوظيفية

إذا كانت المنظمة تعتبر أنه من الضروري وجود موظفين أمنيين مخصصين، فيجب إيلاء اهتمام خاص للمسميات الوظيفية.

مستشار أمني

تقديم نصائح منظمة لتوجيه عمليات اتخاذ القرار للآخرين.

مدير أمني

يدير الأمن على صعيد المنظمة، بما في ذلك اتخاذ القرارات اليومية.

مدير السلامة والأمن / كبير موظفي الأمن / نائب الرئيس لإدارة المخاطر الأمنية.

تشكل هذه الوظيفة جزءًا من فريق القيادة ولديها إمكانية الوصول إلى مجلس الإدارة. يضمن أن يكون الأمان جزءًا من إطار إدارة المخاطر في المنظمة ويساهم في مؤشرات الأداء الرئيسية لمجلس الإدارة التي يعقد كل ربع سنة.

يمكن أن يؤثر المسمى الوظيفي على مستوى النفوذ الذي يحظى به الشخص، خاصةً فيما يتعلق بالأنشطة البرمجية، إلا إذا تم توضيح ذلك بشكل صريح. جدير بالمعرفة أن هذا يسبب تحديات تنظيمية بسبب النزاعات بين أقسام الأمن والبرمجة. بينما يتم توجيه هذا أيضًا من خلال الشخصية، فإن المسمى الوظيفي والأدوار والمسؤوليات الواضحة تحدد كيف تحقق المنظمة إدارة مخاطر الأمن. كما أنه من المهم أيضًا النظر في النطاق الجغرافي لكل وظيفة. يمكنك دمج مصطلحات مثل "وطني"، أو "إقليمي"، أو "عالمي" في العناوين المذكورة أعلاه.

المسؤوليات التنظيمية

بالإضافة إلى تحديد أدوار ومسؤوليات الموظفين، تحتاج السياسات أيضًا إلى توضيح مسؤوليات المنظمة تجاه الموظفين من منظور واجب الرعاية (بما في ذلك الموظفين الوطنيين حيث قد تكون الأطر القانونية والأنظمة في البلاد مختلفة). يجب على المنظمات أن تفهم بوضوح وتبلغ عن مسؤولياتها القانونية والأخلاقية المتعلقة بواجب الرعاية تجاه الموظفين والمستشارين والمتطوعين ومنظمات الشركاء.

ستظل هناك دائمًا مناطق رمادية، لذا يجب أن تكون السياسات أقل تركيزًا على تحديد الحدود الصارمة وأكثر تركيزا على من يتخذ القرارات في نهاية المطاف وما هو نطاق عملهم. (أنظر القسم 1.5 في الموقف من المخاطر و القسم 3.8 في الربط بالقانون).

من الأمور الأساسية لتحقيق النجاح هو الاعتراف بأن مشاركة القيادة على المستويات العليا أمر حاسم. ومع ذلك، لكي تنجح إدارة المخاطر الأمنية، يجب على جميع أفراد المنظمة تحمل مستوى من المسؤولية عن سلامتهم وأمنهم.

موارد مفيدة

- إدارة مخاطر الأمن GISF: دليل أساسي
- أدوات التفكير: كيفية إنشاء RACI

صندوق الطفل/جايك ليبل

كينيا

موظفو مؤسسة ChildFund International يزورون قرية ريفية في كينيا. يجب أن يكون لدى مختلف أعضاء الفريق أدوار ومسؤوليات محددة بوضوح في مجال إدارة المخاطر الأمنية، والتي يمكن أن تشمل أيضًا حماية الطفل.

الفقرة 3: التكامل الوظيفي المتبادل بين إدارة المخاطر الأمنية وتطوير السياسات

تستند استراتيجية إدارة المخاطر الأمنية (SRM) الناجحة إلى تعزيز وعي مشترك وإحساس بالمسؤولية بين القيادة العليا وبين مختلف الوظائف الرئيسية في المنظمة. هذا يضمن دمج إدارة المخاطر الأمنية (SRM) في جميع جوانب التخطيط والأنشطة داخل المنظمة.

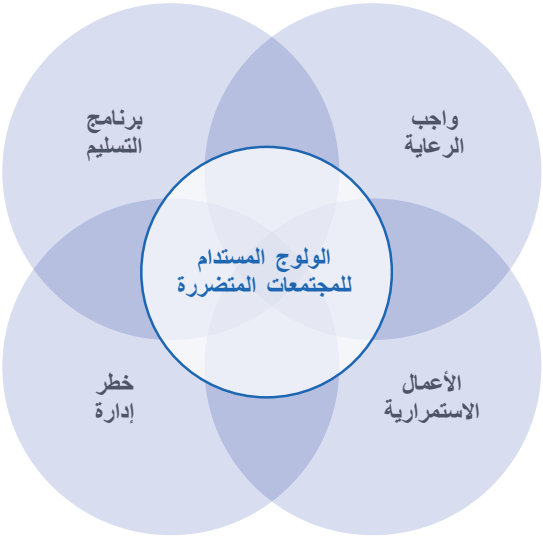
من ناحية، يمكن للقادة الكبار أن يلعبوا دورًا محوريًا في دعم إدارة المخاطر الأمنية (SRM) والتأكيد على أهميتها الاستراتيجية في جميع أنحاء المنظمة. ومع ذلك، لضمان فعالية جهود إدارة المخاطر الأمنية (SRM)، من الضروري أن تفهم جميع الوظائف داخل المنظمة أهمية SRM بالنسبة لأدوارها ومسؤولياتها المحددة. (أنظر الفقرة 1). يجب على الجميع أيضًا إدراك التأثيرات السلبية المحتملة، بما في ذلك تكلفة الحوادث، إذا لم يتم أخذ إدارة المخاطر الأمنية (SRM) في الاعتبار ضمن تخطيطهم الاستراتيجي الخاص.

> *"يجب على الأقسام الأخرى فهم التداعيات الأمنية لأنشطتها وقراراتها."* **(مشارك في المقابلة الفردية الرئيسية، قائد استراتيجي لإدارة المخاطر الأمنية في إحدى المنظمات غير الحكومية).**

قد تختار المنظمات المختلفة اتباع أساليب متنوعة في تنظيم هذه التعاونات بين الوظائف الاستراتيجية. على سبيل المثال، قد تقوم هذه المنظمات بتسهيل عمل مجموعات العمل، الاجتماعات الفردية، قنوات الرسائل عبر الإنترنت، التقارير المشتركة، أو المراجعة المتبادلة الداخلية بين السياسات. بغض النظر عن الطريقة المتبعة، فإن العنصر الحاسم هو فهم وتوضيح كيفية تقاطع إدارة المخاطر الأمنية (SRM) مع كل وظيفة لضمان استدامة مرونة المنظمة على المدى الطويل.

3.1 تحديد سبب أهمية إدارة المخاطر الأمنية (SRM)

لتمكين الوظائف الاستراتيجية الأخرى من رؤية أهمية إدارة المخاطر الأمنية (SRM) بالنسبة لهم، يمكن أن يكون من المفيد ربط إدارة المخاطر الأمنية بأربعة أعمدة أساسية للمرونة التنظيمية:



هذه العناصر الأربعة ليست دائمًا مفهومة على نطاق واسع عبر جميع الأقسام. لكن يجب استخدامها كأرضية مشتركة لإظهار كيف أن إدارة مخاطر الأمن (SRM) تهم جميع الوظائف وكيف تتصل بمخاطر أخرى، مثل:

- الوصول إلى المجتمعات المحتاجة وتقديم المساعدة اللازمة.
- زيادة الإنتاجية العامة من خلال توفير بيئة عمل منظمة وآمنة.
- توفير ضمان للمانحين والممولين بوجود برامج مستقرة ومدارة بشكل جيد وفعّال، مما يمكن أن يزيد من فرص إعادة الاستثمار.
- حماية الأفراد والبيانات والملكية الفكرية والأصول.
- تقليل المخاطر القانونية والمالية.
- تمكين العمليات/البرمجة من الوصول إلى المواقع عالية المخاطر.
- تعزيز سمعة المنظمة ومصداقيتها، مما يمكن أن يؤثر إيجابًا على قدرتها التنافسية، ودوران الموظفين، واكتساب المواهب.
- تحسين ثقة الموظفين ورفاهيتهم النفسية والبدنية.
- المساهمة في قدرة استمرارية الأعمال ومرونة المؤسسة.
- إظهار قدرة المنظمة على السيطرة على مخاطر السلامة والأمن بشكل فعال وناجع، مما يمكن أن يساعد في خفض أقساط التأمين.
- إنشاء عمليات أكثر فعالية لإدارة الأزمات.

(مقتبس من **IEC 31010:2019: إدارة الأزمات تقنيات تقييم المخاطر**).

يبين المربع أدناه مجالات محددة حيث ترتبط استراتيجية إدارة المخاطر الأمنية بشكل مباشر بوظائف أخرى لدعم تقديم البرامج بشكل جيد، وتوفير واجب الرعاية، وتعزيز إدارة المخاطر، وضمان استمرارية الأعمال. يمكن أن توفر هذه الأمثلة نقاط بداية مقترحة للمحادثات بين قادة إدارة المخاطر الأمنية وكبار القادة في وظائف أخرى في المنظمة.

الجدول 1 خريطة الترابطات بين إدارة المخاطر الأمنية والوظائف التنظيمية الرئيسية

البرامج/ العمليات	• الوصول إلى الخدمات وتقديمها بطريقة آمنة • تخطيط البرامج • تغير البيئات التشغيلية • تغير بيئات التمويل • الوصول إلى الشركاء ومواقع المشاريع • التخطيط للطوارئ (الإخلاء/السبات/إعادة التوطين) • الأمن في البيئات الرقمية، بما في ذلك البرامج والأجهزة الجديدة في البرامج والعمليات • الدعم للشركاء (واجب الرعاية، الموقف من المخاطر/نقل المخاطر، التوطين)
المالية	• التقليل من فقدان الأصول (الأشخاص/الموارد) • الاحتيال والفساد (غياب الوصول والرقابة) • إدارة الموارد • أموال الطوارئ (مركزية أو خاصة بمشروع) • تكلفة حوادث السلامة والأمن (المباشرة وغير المباشرة) • توفير التأمين

الجدول 1 خريطة الترابطات بين إدارة المخاطر الأمنية والوظائف التنظيمية الرئيسية مستمر	
الاتصالات	• التضليل/المعلومات الخاطئة • التهديدات عبر وسائل التواصل الاجتماعي • التواصل الداخلي حول إدارة المخاطر الأمنية • السمعة • المناصرة الخارجية • الرؤية والعلامة التجارية
تكنولوجيا المعلومات	• تهديدات الأمن السيبراني • المراقبة الرقمية • أمن الشبكات والمعلومات • النسخ الاحتياطي للبيانات
الموارد البشرية	• التنوع والمساواة والإدماج (DEI) • الصحة العقلية والرفاهية • بناء القدرات • التوظيف والاحتفاظ
القانون	• تحديد واجب الرعاية • العناية الواجبة • العمل مع المنظمات الشريكة - العقود، والاختصاصات المحلية، والعمليات التنظيمية المحددة حسب السياق
الحماية	• سلامة الموظفين والمستفيدين
السفر	• إدارة مخاطر السفر • تحليل السياق • الترخيص والموافقة • تتبع/مراقبة المسافرين • إجلاء/نقل
المناصرة* * *تمت مناقشتها في الفقرة 4*	• التنسيق المدني العسكري • وصول المساعدات الإنسانية • شركات الأمن الخاصة والشركات العسكرية • استخدام المرافقين المسلحين • استخدام القوافل

3.2 أهمية إدارة المخاطر الأمنية المرنة (SRM)

بدون وجود تدفقات عمل فعالة بين الأقسام المختلفة، وتواصل ومشاركة المعلومات، هناك خطر من أن القسم الذي يتلقى إشعارًا بحدوث حادث أو تغيير في السياق قد يفسر تلك المعلومات من منظوره الخاص. قد يتجاهلون أيضًا مشاركة هذه المعلومات مع القادة الاستراتيجيين الآخرين، مما يعرض لخطر تفاقم الوضع أو زيادة تأثير الحادث.

كما هو موضح في الفقرة 1، ضمان فهم الإدارة العليا لكيفية ارتباط استراتيجية إدارة المخاطر الأمنية مباشرة بالوظائف الداخلية الأخرى هو وسيلة ممتازة لتطوير نهج مرن في إدارة المخاطر الأمنية. هذا يضمن أن تكون المنظمة بأكملها على دراية بالتهديدات المحتملة لاستمرارية الأعمال.

3.3 الربط بالبرامج/العمليات

تتبوأ فرق البرامج دور الطليعة في الدفع بمهمة المنظمة إلى الأمام. غالبًا ما يتعرضون لضغوط لتحقيق الأهداف الاستراتيجية الرئيسية. لذلك، تلعب أهمية البرنامج دورًا مهمًا عند النظر في المخاطر الأمنية وفهم إدارة المخاطر الأمنية كوظيفة تمكينية (بدلاً من كونها عائقًا). إنها عنصر أساسي في دمج إدارة المخاطر الأمنية في عمليات البرنامج.

تخطيط البرامج

يمكن أن تتطور الحواجز عندما يُنظر إلى إدارة المخاطر الأمنية على أنها عائق أمام تحقيق أهداف البرنامج. غالبًا ما تنشأ هذه التحديات عندما لا يتم تضمين إدارة المخاطر الأمنية خلال مراحل التطوير الأولى للبرنامج، ويتم اعتبارها بدلاً من ذلك كمتطلب نهائي قبل الموافقة على البرنامج. قد تنشأ تحديات أيضًا عندما تُعتبر إدارة المخاطر الأمنية وظيفة دعم استجابية فقط على الحوادث.

يجب على قادة إدارة المخاطر الأمنية العمل عن كثب مع قادة البرامج عند تطوير استراتيجياتهم المعنية. سيساعد ذلك موظفي البرنامج على التعرف على الفوائد المترتبة على دمج إدارة المخاطر الأمنية. على سبيل المثال، يمكن لفرق إدارة المخاطر الأمنية العمل جنبًا إلى جنب مع فرق البرنامج لتحديد متى قد تكون الأنشطة أو المواقع المخطط لها قريبة من عتبات المخاطر التنظيمية، والاستعداد والتخفيف من هذه المخاطر معًا.

يجب على قادة إدارة المخاطر الأمنية مشاركة تحليلاتهم وفهمهم للسياقات العالمية والإقليمية والوطنية والبيئات التشغيلية مع فرق البرنامج. ينبغي عليهم بدورهم استخدام ملاحظات ومساهمات موظفي البرنامج، بما في ذلك الموظفين المحليين. يمكن أن يساعد ذلك في توضيح وتوطين عمليات إدارة المخاطر الأمنية بدلاً من الاعتماد على نهج من أعلى إلى أسفل أو "نموذج موحد للجميع". سيدعم ذلك فرق البرامج من خلال تقديم نصائح عملية وواقعية حول كيفية تحقيق أهدافهم بشكل آمن ومأمون. يمكن أن يساعد ذلك أيضًا في دمج أساليب وتقنيات إدارة المخاطر الأمنية الجديدة في خطط البرنامج.

يجب أن يتشارك قادة إدارة المخاطر الأمنية وقادة البرنامج في هدف تنفيذ الأنشطة البرمجية بشكل آمن ومأمون. يجب على قادة إدارة المخاطر الأمنية أن يحددوا بوضوح أن الهدف هو تمكين فرق البرنامج من تحقيق برامجها بشكل آمن ومأمون. إدارة المخاطر الأمنية ليست عائقًا. إنها موجودة لتسهيل البرمجة المستدامة على المدى الطويل. من المهم أيضًا أن تكون هذه المحادثات والقرارات موجهة بواسطة النهج الاستراتيجي للمنظمة تجاه موقفها من المخاطر وتحملها.

تسليم البرامج ووصول المساعدات الإنسانية

يمكن أن تكون قيود الوصول مادية أو بيروقراطية، حيث أدرج مكتب الأمم المتحدة لتنسيق الشؤون الإنسانية (OCHA) القيود التالية باعتبارها الأكثر شيوعًا للوصول إلى السكان المتضررين:

- الإجراءات البيروقراطية التي تؤخر أو تعرقل أو تتدخل في العمليات الإنسانية.
- المعلومات المضللة والخاطئة التي تشوه سمعة الجهات الإنسانية.
- العقوبات والإجراءات الخاصة بمكافحة الإرهاب التي تحول دون دفع الرسوم أو شراء البضائع أو توريد المواد.
- شدة الأعمال العدائية والذخائر المتفجرة التي تعيق حركة العاملين في المجال الإنساني.
- الهجمات على العاملين الإنسانيين والمنشآت الإنسانية، وسرقة الممتلكات.

يُعد "القبول" استراتيجية أساسية للأمن والوصول. يشير إلى استعداد المستفيدين والسلطات المحلية والأطراف المتنازعة وأصحاب المصلحة الآخرين لاستقبال المنظمات الإنسانية والتنموية في مجتمعاتهم. ينبغي للمنظمات غير الحكومية أن تعمل بشكل نشط على تعزيز موافقة أصحاب المصلحة المحليين والحفاظ عليها لتمكين القبول المستمر. سيدعم ذلك بدوره وصول المنظمات غير الحكومية إلى الفئات الهشة ويسمح لها بتنفيذ الأنشطة البرامجية.

ومع ذلك، فإن مفهوم القبول يتعرض بشكل متزايد للتهديد بسبب تراجع الفضاء المدني في العديد من السياقات. تتزايد الاتهامات الموجهة من قبل الحكومات إلى المنظمات غير الحكومية (I) بأنها تعيق الأمن الوطني أو تحمل قيمًا سياسية أو ثقافية أو دينية تتناقض مع المصالح الوطنية. إذا تم اعتبار المنظمة مرتبطة بأي هدف سياسي أو عسكري، فقد يعرض ذلك حياة موظفيها للخطر ويزيد من قيود وصولهم.

رأي الخبراء

"بالنسبة للعديد من المنظمات غير الحكومية، فإن القبول هو أساس الممارسة الأمنية الجيدة." "لذا، يجب أن تكون أي تهديدات للقبول مصدر قلق لفرق الأمن في المنظمات غير الحكومية."

"مورّو، إ. (2023) "الوصول الإنساني وإدارة الأمن: اعتبارات لأمان الموظفين'."

يجب على قادة البرنامج وإدارة مخاطر الأمن العمل معًا عن كثب لتطوير استراتيجيتهم بشأن الوصول. هذا أمر مهم بشكل خاص في الحالات التي لا تكون فيها مبادئ الإنسانية المتعلقة بالحياد والموضوعية والاستقلال خيارًا أو قد تتعرض للخطر. على سبيل المثال، قد تشمل هذه البرامج التي تركز على المناصرة أو دعم حقوق الإنسان. علاوة على ذلك، فإن الربط الصريح على المستويين السياسي والاستراتيجي بين الوصول وإدارة المخاطر الأمنية (SRM) أمر مهم لضمان تقديم الخدمات بشكل مستدام إلى المجتمعات التي يصعب الوصول إليها.

نصيحة هامة: تحقيق إدارة المخاطر الأمنية الاستراتيجية الفعالة ضمن تخطيط البرامج
1. مشاركة قيود الوصول وتثليثها وتحليلها داخليًا
فهم أنواع ودوافع وآثار عوائق الوصول هو الخطوة الأولى لمعالجتها. التفكير في إنشاء مجموعة عمل استراتيجية داخلية تتكون من قادة البرامج والأمن والعمليات والمناصرة والاتصالات. يمكن لهذه المجموعة معًا تحديد القيود، وتحليل وتخفيف المخاطر، وتطوير استراتيجيات الوصول التنظيمية، وتحديد الخطوط الحمراء (حدود المخاطر) والمواقف التنظيمية.
2. تدريب الموظفين وخلق ثقافة المشاركة ومسارات التصعيد.
يمكن لموظفي الأمن أن يلعبوا دورًا حاسمًا في تعزيز الاتصالات وتوفير التدريب وتشجيع تبادل المعلومات. هم يلعبون دورًا رئيسيًا في تحويل الثقافة التنظيمية من "التنفيذ بأي ثمن" إلى تشجيع المشاركة الأكثر تأملاً واستراتيجية في قضايا الوصول. بالنسبة للمنظمات التي لا يوجد لديها موظفون مخصصون للوصول، يجب تحديد مسارات واضحة للموظفين لتصعيد القضايا الداخلية والخارجية. يمكن لموظفي الأمن دعم أو قيادة تحليل المخاطر المتعلقة بقضايا الوصول، والمساعدة في تطوير وتوزيع السياسات الداخلية وإجراءات التشغيل القياسية.

نصيحة هامة: تحقيق إدارة المخاطر الأمنية الاستراتيجية الفعالة ضمن تخطيط البرامج مستمر

3. كن استباقيًا في بناء العلاقات وفهم السياق.

بناء العلاقات مع السلطات الحكومية والمجموعات المسلحة غير الحكومية، حيثما وُجدت، أمر حيوي لتحقيق القبول. ورغم أن العمل "تحت الرادار" قد يكون مناسباً في بعض السياقات، فإنه نادراً ما يكون استراتيجية قبول قابلة للتطبيق على المدى الطويل. يعد بناء العلاقات والشبكات مهارة حيوية لموظفي الأمن ويمكن أن يكون موردًا قيمًا لتوجيه الموظفين المنخرطين في قضايا الوصول.

4. إشراك المجتمع الإنساني من أجل استجابة أكثر أمانًا

عندما يواجه موظفو الأمن في المنظمات غير الحكومية عوائق الوصول أو مشاكل أمنية، يتعين عليهم أن يسألوا أنفسهم السؤال التالي - هل تؤثر هذه المشكلة على منظمتي فقط، أم أنها قد تؤثر على المنظمات غير الحكومية الأخرى والأشخاص المحتاجين؟ في كثير من الحالات، الجواب هو الأخير. في هذه الحالات، لا بد من مشاركة تحديات الوصول ومناقشتها (بعناية) مع الوكالات الأخرى لتثليث المعلومات وإدارة المخاطر وتحديد المواقف المشتركة قبل التعامل مع النظراء. هذا أمر بالغ الأهمية لتعزيز قبول العمل الإنساني وسلامة الموظفين.

المصدر: مورّو، إ. (2023) إدارة الوصول الإنساني والأمن: اعتبارات لفرق الأمن.

موارد مفيدة

- دليل عمل المدافعين في الخطوط الأمامية حول الأمن
- أداة الأمن في GISF - تحليل القبول.
- GISF تحقق عمليات آمنة من خلال القبول
- إنقاذ الأطفال: أدوات القبول

3.4 الربط بالمالية

هناك تكاليف لا مفر منها مرتبطة بإدارة السلامة والأمن. إن تطوير وتنفيذ نهج شامل لإدارة المخاطر الأمنية قد يتطلب موارد مالية كبيرة. يجب إدخال التكاليف المرتبطة بإدارة مخاطر السلامة والأمن في المراحل المبكرة من التخطيط. من الضروري أن ندرك أنها جزء لا يتجزأ

من تصميم البرنامج، وأنها ضرورية لاستدامته ونجاحه. إلى جانب تأمين الموارد اللازمة للأمن، من المهم أيضًا تقدير الأثر المالي المحتمل الناتج عن حادث أمني، وضمان الاعتراف الكافي على المستوى الاستراتيجي بعدم الأمان كخطر مؤسسي أو تجاري.

يمكن أن تؤثر الحوادث الأمنية على العديد من المجالات الأخرى داخل المؤسسة. على سبيل المثال:

- موظفين إضافيين داخليين/خارجيين للتعامل مع الحادث/القيام بمهمة التتبع.
- دعاية إضافية لإصلاح الضرر الذي لحق بالعلامة التجارية.
- تداريب إضافية.
- إيقاف عمليات البرنامج خلال حادث أمني.
- حالات الاحتيال والفساد الناتجة عن الخسارة المالية.
- خسارة ممكنة للمانحين بعد وقوع حادث أمني.

لذا، فإن التعاون بين قادة المالية وإدارة المخاطر الأمنية (SRM) ضروري لتطوير منظمة أكثر استعدادًا وقدرة على الصمود.

التخفيف من فقدان الأصول/الموارد

يمكن أن تكون المناقشات المتعلقة بالميزانيات صعبة بشكل خاص بالنسبة للمهنيين في مجال الأمن. في معظم الوظائف، من الممكن تقديم عائد استثمار واضح وقابل للتنبؤ (ROI). ومع ذلك، فإن النفقات المتعلقة بالأمن الفعّالة غالبًا ما تتعلق بمنع أو تقليل الخسائر، بدلاً من تحقيق مكاسب صافية، وهو ما يصعب تحديده للمعنيين بالقرارات المالية.

يجب على قادة إدارة المخاطر الأمنية توضيح حجم كل خطر والتكاليف المحتملة والخسائر والآثار الأخرى إذا لم يتم التخفيف منها من خلال الأنظمة والإجراءات الأمنية. يمكن أن يتعلق ذلك بمنع الاحتيال أو الفساد. يمكن أن يرتبط أيضًا بمخاطر أخرى ليس لها تكلفة مالية مباشرة، ولكنها يمكن أن تؤثر بشكل كبير على النتائج النهائية. على سبيل المثال، يمكن أن يؤدي حدوث خرق أمني إلى تضرر السمعة، مما يؤثر على ولاء المانحين والموظفين ويتسبب في انخفاض التمويل أو تراجع الاحتفاظ بالموظفين. أو إذا كانت المنظمة تفتقر إلى الوصول، يمكن أن تؤدي فجوة الإشراف إلى فراغ يمكن أن تتجذر فيه أنشطة ضارة.

تحريك الموارد، تخصيصها وإدارتها

يجب أن تتضمن تعبئة الموارد وتخصيصها وإدارتها بشكل فعّال وطويل الأمد مراعاة جوانب السلامة والأمن. تقليديًا، تعتبر السلامة والأمن من أوائل المجالات التي تتأثر بتراجع الإيرادات. غالبًا ما يُعامل أيضًا كبند مالي لتغطية الفجوات في وظائف الدعم الأخرى. الموارد المتعلقة بإدارة المخاطر الأمنية (SRM) ضرورية لتمكين فرق البرامج ودعمها في تحقيق الأهداف الاستراتيجية طويلة الأمد للمؤسسة.

"يجب عدم النظر في فتح مكاتب ميدانية جديدة إلا إذا توفرت ميزانية كافية لتغطية الحد الأدنى من معايير التشغيل الأمنية كما هو منصوص عليه في خطط الأمن على مستوى البلد." **مقابلات مع المعنيين الرئيسيين (KII)**

من الضروري استخدام الموارد بشكل أكثر كفاءة من خلال القضاء على الهدر وتحقيق عائد استثمار أعلى. إذا لم يتم استثمار موارد السلامة والأمن بشكل صحيح، أو إذا لم تتم إدارتها وصيانتها بشكل جيد، فقد تتحول إلى عبء مالي أو تؤدي إلى تكاليف أكبر عند الحاجة إلى "إصلاح" مشكلة بعد وقوعها، بدلاً من التخطيط لها والتخفيف من آثارها مسبقًا. على سبيل المثال، يعد الاستثمار في صيانة المركبات المنتظمة وتدريب السائقين أكثر كفاءة من حيث التكلفة من الانتظار حتى تتعطل المركبات وتضطر لتوفير وسائل النقل الطارئة أو إجراء إصلاحات مكلفة في اللحظة الأخيرة.

يعتبر العائد على الاستثمار من تعزيز مرونة المنظمة أيضًا مقياسًا يهم معظم أقسام المالية. يمكن أن تساعد دورات تدريب الوعي الأمني المنظمة على توفير المال من خلال تقليل فرصة حدوث حادث أمني نتيجة خطأ بشري.

كيفية تقدير تكلفة وتمويل إدارة المخاطر الأمنية

موارد GISF **"تكلفة إدارة المخاطر الأمنية للمنظمات غير الحكومية"** يوضح بالتفصيل كيف أن القيمة مقابل المال غالبًا ما تكون أحد الأهداف الرئيسية للمنظمات غير الربحية. توجد نظرة عامة تشير إلى أنه كلما كانت التكاليف غير المتعلقة بالبرنامج أقل، كانت المنظمة أكثر كفاءة في تخصيص معظم التمويل للنفقات المباشرة للبرامج. ومع ذلك، فإن إنفاق معظم التبرعات على تكاليف البرامج لا يعني بالضرورة أن البرنامج يحقق أهدافه المعلنة أو أنه يُنفذ بطريقة آمنة ومأمونة (وبالتالي مستدامة).

ممارسة شائعة أخرى هي تخصيص نسبة مئوية من إجمالي ميزانية البرنامج لتكاليف إدارة المخاطر. ومع ذلك، فإن المواقف والافتراضات حول ما يعتبر "نسبة مقبولة" تختلف اختلافًا كبيرًا عبر القطاع. من ناحية أخرى، يعني التعامل مع إدارة المخاطر كتكلفة مؤسسية غير برنامجية عامة أنه غالبًا ما يتم تقليلها إلى أدنى مستوى ممكن، سواء لتكون أكثر قبولًا لدى المانحين (كتكلفة غير مباشرة)، أو ليتم النظر إليها بشكل إيجابي من قبل الهيئات الخارجية، مثل المدققين.

التوافق مع دورات الميزانية السنوية أمر مهم لتخصيص الموارد اللازمة في الوقت المناسب. من الضروري أيضًا العمل مع فرق التمويل لتطوير المنهجية الإدارية اللازمة (التي تتطلب اهتمامًا خاصًا بها). يعد تعزيز المهارات الإدارية المناسبة بين المتخصصين في إدارة المخاطر الأمنية خطوة بالغة الأهمية في هذه العملية أيضًا. تتضمن الأسئلة المفيدة التي يمكن مناقشتها مع فرق التمويل ما يلي:

- هل يقوم قسمك بإعداد الميزانية لكل مشروع على حدة، أم أنك تتبع نهجًا أكثر استراتيجية؟
- هل يتم دعم إدارة الموارد البشرية من خلال التمويل الأساسي، أم أنها تعتمد حصريًا على دعم الجهات المانحة؟
- هل تأخذ دورة حياة الأصول المادية في الاعتبار عند إعداد الميزانية؟
- كيف يُتوقع منك تخصيص الموارد لخطط الطوارئ والاستعداد؟

توفير التأمين

غالبًا ما يتم اتخاذ قرارات تخصيص التأمين من قبل فرق المالية (أو العمليات) مما يمكن أن يؤدي إلى ظهور طرحين محتملتين:

- يؤدي نقص التواصل حول احتياجات المنظمة من التأمين، استنادًا إلى ملفات المخاطر المتعلقة بأنشطة ومواقع الموظفين (أي المواقع، ومستوى التغطية، وأي إضافات مطلوبة) إلى نتائج غير مرضية.
- نقص فهم الموظفين في الميدان حول كيفية الوصول إلى التأمين، وما هي الشروط المحددة المتاحة، وعدم وضوح من يشملهم التأمين وعلى أي مستوى (مثل الموظفين الدوليين مقابل الموظفين الوطنيين).

مناقشة هذه القضايا بشكل تعاوني مع فرق المالية وإدارة المخاطر الأمنية (SRM) وفرق البرنامج في مرحلة التخطيط الاستراتيجي أمر ضروري لضمان أخذ القرارات المتعلقة بأنشطة البرنامج بعين الاعتبار متطلبات التأمين، وتحديد أي مواقع أو أنشطة تمثل "مؤشرات خطر" (red flags)، وضمان توفير التأمين المناسب لجميع الموظفين.

موارد مفيدة

- GISF تكلفة إدارة المخاطر الأمنية للمنظمات غير الحكومية
- GISF تأمين سلامة العاملين في مجال الإغاثة من خلال الميزانية الفعالة، (الصفحة 76)

3.5 الربط بالاتصالات

يجب أن تعمل فرق الاتصالات وإدارة المخاطر الأمنية (SRM) لدعم بعضها البعض من منظورين خارجي وداخلي. من منظور خارجي، ينبغي على وظائف الاتصالات وإدارة المخاطر الأمنية (SRM) العمل معًا لإدارة وتخفيف المخاطر الناتجة عن المعلومات المضللة/المغلوطة، ووسائل التواصل الاجتماعي، وحوادث الأمن. داخليًا، يمكن لقادة الاتصالات أن يلعبوا دورًا رئيسيًا في الحفاظ على فعالية إطار عمل إدارة المخاطرالأمنية وتعزيزه (SRM)، من خلال دعم قادة SRM في تبسيط الرسائل، وإشراك الموظفين.

التعاريف الرئيسية

- **معلومات مضللة:** المعلومات المضللة، ولكن المصدر الذي ينشرها ليس لديه نية للإيذاء.
- **المعلومات المزيفة:** معلومات كاذبة ويحاول المصدر التلاعب بالحقائق عمداً.

التضليل والمعلومات الزائفة

تزداد المخاطر المتعلقة بالمعلومات المضللة والبيانات الزائفة بسرعة بالنسبة للمنظمات، لا سيما تلك التي تعمل في بيئات ذات مخاطر سياسية عالية. يمكن أن يكون تأثيرها على الأمن كبيرًا. على سبيل المثال، يمكن أن تؤدي البيانات الكاذبة إلى إلقاء القبض على موظفي المنظمات غير الحكومية أو الاعتداء عليهم جسديًا.

من الضروري فهم أن تهديدات الأمن الإلكتروني يمكن أن تضر مباشرة بالأمن الجسدي للموظفين أو الأشخاص المرتبطين بالمنظمة. يمكن أن يؤدي انتشار المعلومات المضللة والزائفة عبر الإنترنت إلى إثارة الغضب على نطاق واسع، مما يمكن استخدامه لتبرير الهجمات الجسدية.

تجعل المعلومات الزائفة والمضللة عبر الإنترنت من الصعب معرفة ما هي الأخبار الحقيقية وما هو الزائفة. هذا يعيق قدرة مختصي إدارة المخاطر الأمنية على الاعتماد على وسائل الإعلام عبر الإنترنت لجمع المعلومات حول مكان ما واتخاذ قرارات حاسمة، خاصة في أوقات الأزمات أو الطوارئ. في هذه الحالات، يُجبر الخبراء الأمنيون على البحث من خلال طبقات من الأخبار الزائفة للعثور على معلومات صحيحة، مما قد يضيع وقتًا حاسمًا. هذا يعيق قدرة هذه المنظمات والأفراد على تقديم الدعم المنقذ للحياة بسرعة وبشكل حاسم لموظفيهم. تتطلب طبيعة الاتصالات الرقمية والتهديدات التي تشكلها حلولًا متكاملة من مختلف التخصصات. استجابةً لذلك، ينبغي على المنظمات ربط أقسام الاتصالات—التي عادةً ما تضم متخصصين في وسائل التواصل الاجتماعي وتقنيات الاتصالات عبر الإنترنت—مع فرق إدارة المخاطر الأمنية، بحيث يمكن لكل منهما تبادل الأفكار حول كيفية وضع استراتيجيات فعالة لإدارة وتخفيف المخاطر المرتبطة بانتشار المعلومات المضللة.

يمكن لقادة الاتصالات دعم قادة إدارة المخاطر الأمنية في تطوير طرق ديناميكية لتحديد المعلومات المضللة والاستجابة لها، والانتقال من أنظمة الاستجابة العشوائية إلى تدفقات عمل أكثر تنظيماً حول التعامل مع المعلومات المضللة.

وسائل الإعلام

تشكل وسائل التواصل الاجتماعي جزءًا أساسيًا من الاتصالات التنظيمية والمناصرة واستراتيجيات التسويق. لكن التهديدات المرتبطة بوسائل التواصل الاجتماعي تتزايد، مما يشكل مخاطر مباشرة وحادة على سلامة وأمن الموظفين، فضلاً عن تأثيرها على سمعة المؤسسات. يوصى بتبني نهج شامل على مستوى المنظمة لتطوير استراتيجيات وسائل التواصل الاجتماعي، بما في ذلك إشراك موظفي إدارة المخاطر الأمنية.

على سبيل المثال، قد لا تكون فرق الاتصالات على دراية بكيفية تأثير بعض الرسائل على وسائل التواصل الاجتماعي على سلامة وأمن الموظفين في سياق معين. بالمثل، يجب إبلاغ الموظفين والاستشاريين والمتطوعين بجوانب السلامة والأمن المرتبطة باستخدام وسائل التواصل الاجتماعي لمشاركة التحديثات المتعلقة بالعمل على ملفاتهم الشخصية.

الاتصالات الداخلية

يعد تطوير اتصالات داخلية جيدة حول إدارة المخاطر الأمنية أمرًا بالغ الأهمية لضمان المشاركة والتنفيذ الناجح لأي استراتيجية لإدارة المخاطر الأمنية (إنظرالفقرة 1). يمكن أن يكون التعاون مع قادة الاتصالات لتبسيط الرسائل الداخلية لإدارة المخاطر الأمنية، بالإضافة إلى النظر في كيفية ترجمة الرسائل الرئيسية لإدارة المخاطر الأمنية في سياقات مختلفة، من الأصول القيمة.

يمكن أن تشمل أساليب التواصل محتوى المنصات الاجتماعية الداخلية، مثل صفحة إنترانت أو نشرة إخبارية. تشمل الخيارات الأخرى الفعّالة للتواصل في إدارة المخاطر الأمنية: مقاطع الفيديو، والاجتماعات العامة، والفعاليات عبر الإنترنت ووجهًا لوجه، والبريد الإلكتروني، والبث المباشر من المسؤولين الرئيسيين.

الاتصالات الخارجية

تتطلب الاستجابة لحدث أمني التعاون بين الأقسام والتخصصات المختلفة. قد يعمل المستجيبون

لحوادث إدارة المخاطر الأمنية على إدارة وتخفيف تأثير الحادث بينما تقوم فرق الاتصالات بتطوير استجابة عامة. ستؤثر طريقة تعامل منظمة غير حكومية مع الإبلاغ العام عن حادث أمني أو تجاهله بشكل كبير على سمعتها وقدرتها على مواصلة العمل بأمان.

لذا، فإن التواصل الواضح، والتحضير، والتخطيط بين هتين الوظيفتين أمرٌ أساسي.

يمكن لقادة الاتصالات وإدارة المخاطر الأمنية بل وينبغي عليهم العمل معًا لتطوير مقاربات استراتيجية للمناصرة الخارجية حول إدارة المخاطر الأمنية على سبيل المثال، قد يشمل هذا العمل مع مسؤولي الاتصالات لتطوير الرسائل الخارجية حول واجب الرعاية الجيد وكيف يدعم ذلك المرونة التنظيمية.

موارد مفيدة

- **التفاعل** أداة تقييم المخاطر: تقييم المخاطر التنظيمية المتعلقة بالتضليل (الصفحة 25).
- **مقابلات إدارة المعلومات المضللة في السياق الإنساني**
- **شبكة التواصل مع المجتمعات المعرضة للكوارث CDAC**
- **أدوات إدارة مخاطر الأمن في GISF الاستراتيجيات** (الصفحات 14-15)

3.6 الربط بتكنولوجيا المعلومات

كجزء من نهج شامل متزايد لإدارة المخاطر الأمنية، تعمل العديد من وظائف السلامة والأمن في الوقت الراهن عن دمج الأمن الرقمي. يتضمن ذلك كيفية تمكين الموظفين من حماية أنفسهم وتقليل تعرضهم الفردي للتهديدات عبر الإنترنت. ومع ذلك، فإن هذا يؤدي أحيانًا إلى انفصال بين إدارة مخاطر الأمن الرقمي ونطاق ومسؤوليات إدارات تكنولوجيا المعلومات (التي تركز عادةً أكثر على التهديدات الأمنية السيبرانية على مستوى المنظمة).

ينبغي على قادة إدارة المخاطر الأمنية وتكتولوجيا المعلومات مشاركة مقارباتهم حول التهديدات السبرانية والرقمية وإبلاغ اقتراحاتهم بخصوص التخفيف من حدة إدارة المخاطر عبر الإنترنت. سيكون لذلك تأثير على تعزيز أمن وسلامة الموظفين وضمان استمرارية الأعمال بشكل جيد.

التعاريف الرئيسية:

- **الأمن السيبراني:** حماية كل الشبكات والحسابات والأنظمة المعلوماتية بالإضافة إلى مستعملي المعلومات.
- **الأمن الرقمي:** حماية حضورك على الإنترنت وبياناتك الشخصية وأصولك ومعلوماتك.
- **أمن المعلومات:** حماية الخصوصية وشمولية وتوافر المعلومات.

التقارب بين الأمن المادي والرقمي والسيبراني

بيمكن أن ترتبط التهديدات عبر الإنترنت بشكل مباشر بالأمن المادي. على سبيل المثال، يمكن أن تؤدي المراقبة الرقمية إلى وصول الجهات الفاعلة الضارة إلى المعلومات الشخصية لشخص ما عبر الإنترنت أو مشاركتها مع جهات تهديد مختلفة. يمكن أن يمكّن ذلك الجهة التي سرقت البيانات أو جهة أخرى حصلت على الوصول إليها من تعقب الأفراد وإيذائهم جسديًا.

إلى جانب التهديدات الرقمية الفردية، يمكن أن تؤثر الهجمات الإلكترونية على مستوى المنظمة أيضًا على سلامة الأفراد وأمنهم الجسدي. نظرًا للطبيعة السرية للبيانات الإنسانية والتسييس المتزايد للعمل الإنساني، فإن فقدان البيانات الشخصية في هجوم إلكتروني واسع النطاق يمكن أن يكون كارثيًا. يمكن أن يؤثر ذلك ليس فقط على الموظفين المباشرين، ولكن أيضًا على أولئك الذين تسعى المنظمة لدعمهم، من خلال زيادة خطر التعرض لهجوم جسدي مستهدف.

أمثلة من القطاع: هجوم إلكتروني كبير على اللجنة الدولية للصليب الأحمر

في يناير 2022، واجهت اللجنة الدولية للصليب الأحمر خرقًا كبيرًا في الأمن السيبراني، مما أدى إلى كشف البيانات الشخصية لأكثر من 515,000 فرد حول العالم. لقد أثر الخرق، الذي شمل بيانات شخصية مثل الأسماء والمواقع ومعلومات الاتصال، على الأشخاص المفقودين وعائلاتهم، والمعتقلين، وغيرهم من الأشخاص الذين يتلقون خدمات من الحركة الدولية للصليب الأحمر والهلال الأحمر في ظل النزاعات المسلحة أو الكوارث الطبيعية أو أزمات الهجرة.

سلط خرق البيانات الضوء على اتجاه مثير للقلق في العمليات السيبرانية التي تستهدف المنظمات الإنسانية. تشكل هذه الأنواع من الهجمات مخاطر جسيمة على الفئات السكانية الهشة والتي قد تواجه ضررًا محتملاً بسبب الكشف عن معلوماتها الحساسة.

ردا على الخرق، تعمل اللجنة الدولية للصليب الأحمر حاليا مع شركائها في الحركة لتعزيز الإطار القانوني والسياسي لحماية البيانات والبنية الأساسية للمنظمات الإنسانية. وهي تعمل حاليا بشكل نشط مع الحكومات من أجل تعزيز الحماية عبر الإنترنت.

اقرأ المزيد: https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

حتى ولو لم تكن المنظمات أو الأشخاص مستهدفين بشكل مباشر، يمكن أن يتأثروا حينما يستهدف الهجوم السيبراني فاعلا خاصا تربطه علاقة بالمنظمة أو الفرد. في عام 2020، تعرضت شركة SolarWinds-وهي شركة تكنولوجيا معلومات أمريكية خاصة-للاختراق وتعرض جزء كبير من بياناتها للسرقة. نظرًا لأن الشركة كانت تستضيف بيانات العديد من الشركات والوكالات الحكومية والمنظمات غير الربحية، فقد تم سرقة بيانات ومعلومات مجموعة متنوعة من المنظمات المختلفة.

وقد أدى هذا إلى تعريض صحة وسلامة الأشخاص الذين يتم تخزين بياناتهم بواسطة SolarWinds للخطر.

رأي الخبراء

"[الهجمات الإلكترونية] تضع ضغطًا هائلًا على الموارد المحدودة للمنظمات غير الحكومية، مما يمنعها ليس فقط من تحقيق مهامها على المدى القصير، بل قد يتسبب أيضًا في أضرار سمعة طويلة الأمد ويضعف الثقة في قدرتها على القيام بدورها في الأزمات والطوارئ الحالية والمستقبلية."

ريليفويب، "الهجمات الإلكترونية: تهديد حقيقي للمنظمات غير الحكومية وغير الربحية"، 2022.

من الضروري تحسين التواصل والتنسيق بين القادة في مجال تكنولوجيا المعلومات الذين يعملون مباشرةً على إدارة تهديدات الأمن السيبراني الخاصة بالمنظمة، وأولئك الذين يقومون بإنشاء استراتيجيات إدارة المخاطر الأمنية لحماية الموظفين من تهديدات الأمن الرقمي. غالبًا ما تكون الفجوات والضعف داخل ملف المخاطر السيبرانية للمنظمة نتيجة لعدم فهم المخاطر على المستوى البشري. يجب على فرق إدارة المخاطر الأمنية وتكنولوجيا المعلومات العمل معًا عن كثب لتحديد التهديدات الرئيسية، وتقييم أماكن الفجوات المحتملة، وتطوير أساليب التدريب والدعم للموظفين على جميع مستويات المنظمة.

تبسيط اللغة التقنية

تقييم مخاطر الأمن السيبراني والرقمي وعرضها بلغة غير تقنية يعد أيضًا أمرًا حيويًا للتفاعل مع قادة إدارة المخاطر في المنظمة وتمكين اتخاذ القرارات على المستوى الاستراتيجي بناءً على المخاطر المعنية. يعد تحويل هذه المخاطر وتدابير التخفيف إلى لغة واضحة ومبسطة تُظهر التأثير المحتمل على عمليات المنظمة أمرًا أساسيًا. يجب أن يساعد ذلك في نهاية المطاف على ضمان أن يتم التعامل مع هذه المخاطر بجدية كافية ويساعد المنظمات على إجراء التغييرات اللازمة لتصبح أكثر أمانًا.

موارد مفيدة

- GISF الأمن الإنساني في عصر عدم اليقين: تقاطع المخاطر الرقمية والفيزيائية
- التكامل بين الأمن السيبراني وإدارة مخاطر المؤسسات (ERM)
- أمن سهل الوصول من GISF الوحدة 4 الأمن الرقمي
- أمن المعلومات الرقمية للعاملين في المجال الإنساني من مجتمع الميم (LGBTQ+) + عمال الإغاثة من GISF

3.7 الربط بالموارد البشرية

إن العلاقة بين الموارد البشرية وإدارة المخاطر الأمنية جزء لا يتجزأ من التخطيط الفعال والإدارة والتخفيف من مخاطر السلامة والأمن للموظفين في جميع بيئات التشغيل. على الرغم من وجود مجالات مسؤوليات مختلفة بوضوح بين وظائف إدارة الموارد البشرية وإدارة المخاطر الأمنية، إلا أن هناك اعتمادًا أساسيًا متبادلاً، يعد أساسيًا للوفاء بواجب الرعاية الذي تتحمله المنظمة.

المقالة الخاصة بـ GISF بعنوان "نحو إدارة مخاطر أمنية شاملة" تسلط الضوء على المنظمات غير الحكومية التي تنظر بشكل متزايد إلى ملفات تعريف عمال الإغاثة الذين تستأجرهم وتنشرهم من أجل تعظيم القبول وتخفيف المخاطر. إت إنشاء أنظمة تعترف وتقر بملفات الموظفين المختلفة، وتمكن من فهم أفضل للمخاطر التي يواجهها كل فرد، وضمان وجود تدابير كافية للتخفيف منها، هو أمر حيوي لتحسين الوصول وحماية الموظفين. ومع ذلك، لا يكفي مجرد تحديد ملفات تعريف الموظفين كاستراتيجية للتخفيف من المخاطر في حد ذاتها. يجب على قادة الموارد البشرية وإدارة المخاطر الأمنية التعاون أيضًا لضمان أن يتم التواصل بشكل كافٍ بشأن هذه الأساليب الأمنية المعدلة والتدابير المحددة لكل موظف على حدة. الموارد المذكورة أدناه تقدم أمثلة إضافية حول كيفية تحسين المنظمات لنهجها الذي يركز على الأفراد.

التنوع والإنصاف والشمول (DEI)

على غرار المسائل الأمنية، فإن التنوع والإنصاف والشمول DEI متعدد الوظائف قد يكون له أدوار مخصصة أو نقاط محورية عبر المنظمة. ومع ذلك، يتم تنظيم التنوع والإنصاف والشمول DEI، أو تسميته، داخل المنظمة، حيث يظل هناك رابط جوهري لكل من الموارد البشرية وإدارة المخاطر الأمنية لتعزيز بيئة تشغيلية أكثر أمانًا وشاملة، يجب على إدارة الموارد البشرية وإدارة المخاطر الأمنية تطوير إطار عمل لمشاركة المعلومات الأساسية المتعلقة بالسلامة والأمن. إن إشراك ممارسي وخبراء التنوع والإنصاف والشمول DEI يمكن أن يضمن نشر المعلومات الأمنية على حسابات الموظفين وفقًا للخصائص الشخصية المختلفة. تشمل هذه الاختلافات العرق، الإثنية، الدين، الإعاقة الجسدية أو العقلية، الهوية الجندرية، وغيرها. وتشمل العوامل الأخرى الاحتياجات الطبية والخبرة السابقة.

نصيحة هامة: اختصارات ومصطلحات التنوع والإنصاف والشمول DEI

يمكن أن يُعرف التنوع والإنصاف والشمول DEI بعناوين مختلفة بناءً على التنظيم وأهداف تلك الوظيفة. قد تشمل بعض الأمثلة على ذلك GEDI (النوع والإنصاف والتنوع والشمول) وJEDI (العدالة والإنصاف والتنوع والشمول) وغيرها. هناك حالات قد تكون فيها هذه الوظيفة مستقلة عن قسم الموارد البشرية، رغم أن هناك تداخلًا في المسؤوليات بينهما.

يمكن أن يساعد توفير قنوات آمنة ومأمونة تشجع جميع الموظفين على الإبلاغ عن المخاوف، الحوادث، والحالات القريبة من الوقوع، خاصةً فيما يتعلق بملفات تعريف محددة، المنظمات على مراجعة الممارسات وتقييمها وإجراء التعديلات اللازمة عند الحاجة. لا يلزم أن تكون آليات تيسير ذلك معقدة، ويمكن أن تعزز ممارسات إدارة المخاطر الأمنية الفعّالة. من الأمثلة على ذلك ضمان تمثيل شريحة متنوعة من الموظفين أثناء إعداد تقييمات المخاطر، أو إعادة

تنشيط العمليات للإلتفاف حول التغذية الراجعة المستمرة. يمكن أن يساعد العمل جنبًا إلى جنب مع ممارسي التنوع والإنصاف والشمول (DEI) وفريق الموارد البشرية إدارة المخاطر الأمنية (SRM) على الحفاظ على المرونة والاستجابة لاحتياجات الموظفين المتعددة الأبعاد.

الصحة العقلية والرفاهية

يمتد مفهوم إدارة المخاطر الأمنية إلى ما هو أبعد من الأمن الجسدي ليشمل السلامة النفسية. تتجاوز إدارة المخاطر الأمنية (SRM) نطاق الأمن المادي لتشمل أيضًا السلامة النفسية. يمكن أن يكون لذلك تأثير إيجابي كبير على أنشطة البرنامج والأهداف الاستراتيجية على المدى الطويل.

تحمل المخاطر والضغوطات المرتبطة بالعمل الإنساني في طياتها مخاطر تجبر المنظمات الإنسانية على اتخاذ خطوات لحماية الصحة النفسية لموظفيها. تسجيلات صوتية ل GISF حول **"السلامة النفسية"** توثق التحديات التي تواجه الصحة العقلية والرفاهية في القطاع الإنساني. يمكن أن تؤثر تحديات الصحة العقلية في كثير من الأحيان على الصحة البدنية. وبالمثل، يمكن أن تتراكم أمراض الصحة العقلية غير المعالجة - وما يترتب عليها من تحديات تتعلق بالصحة البدنية - لتخلق نفقات كبيرة على الفرد والمشغل. ومن ثم، فإن تبخيسا الصحة العقلية يشكل خطرا رئيسيا على الأعمال.

بحث حديث أجرته شركة ماكينزي آند كومباني يوضح أن الأمان النفسي القوي هو أحد أقوى المؤشرات على أداء الفريق والإنتاجية والجودة والسلامة والإبداع والابتكار. كما أنه ينبئ بتحسن الصحة العامة. إن تحسين ظروف المؤسسات لإنشاء بيئات آمنة نفسياً واستدامتها يمكن أن يكون له تأثيرات إيجابية شاملة على أمن المنظمة. من المرجح أيضًا أن يؤدي هذا إلى تعضيد ثقافة أمنية مندمجة ذات نتائج متقاطعة.

من شأن ارتضاء هذا الوصول بشكل ناجع وجود علاقة قوية ومستمرة بين قيادات إدارة المخاطر الأمنية ونظيرتها الملمة بالموارد البشرية. هذا مهم بشكل خاص في مجالات مثل الحوافز التشغيلية والإبلاغ عن الحوادث والجهود المستمرة على المستوى الاستراتيجي لتوطيد الثقافة التنظيمية حول الصحة العقلية والرفاهية.

إن التقدم الكبير في بناء الوعي بالاحتياجات المتعلقة بالصحة العقلية للعاملين في قطاع المساعدات طرح لا مسائلة في تحققه. بيد أنه لا تزال هناك حاجة إلى مزيد من المجهودات على مستوى إيقاض الوعي على المستوى الاستراتيجي ومناقشة حيثيات مدى تأثير ضعف الصحة العقلية للموظفين على أهداف المنظمة. إن التداول بشأن الموارد البشرية وإدارة المخاطر الأمنية بين قادة هذه التخصصات حول أفضل السبل لإدارة التعثرات الناشئة والتخفيف منها أمراً بالغ الأهمية. وهي مهمة بشكل خاص في المجالات الأقل توثيقًا على نطاق واسع. يمكن أن يشمل ذلك الصدمات غير المباشرة ودعم الموظفين من سياقات ثقافية مختلفة أو العاملين فيها، حيث لا يتم الاعتراف بالصحة العقلية والرفاهية على نطاق واسع أو التحدث عنها على سبيل المثال.

التوظيف والاحتفاظ

تواجه العديد من المنظمات صعوبة متزايدة في جذب الموظفين الأكفاء وتدريبهم والاحتفاظ بهم وتحفيزهم في مجال إدارة المخاطر الأمنية. يشكل هذا مصدر قلق كبير يمكن أن يكون له تأثيرات شديدة على العمليات وقدرة المنظمة على الصمود. نظراً للمشهد المتغير باستمرار، فإن قيود التمويل تفرض نقاط ضعف إضافية في توظيف موظفي إدارة المخاطر الأمنية والاحتفاظ بهم. إضافةً إلى ذلك، فإن التحديات التي يواجهها بعض المختصين في إدارة المخاطر الأمنية في إثبات أثرهم، وعدم توافق مؤشرات الأداء الرئيسية دائمًا مع الأهداف الاستراتيجية، تجعل من الصعب تقديم المعلومات اللازمة والتأثير على صانعي القرارات على المستوى الاستراتيجي بشكل كافٍ. على سبيل المثال، قد لا يتمتع متخصص إدارة المخاطر الأمنية المؤهل بأي وصول أو خط تقرير إلى صانعي القرار الرئيسيين في المنظمة أو إلى الإدارة التنفيذية. مع ذلك، لا يزال لديهم تفويض لتعزيز ثقافة أمنية أفضل.

ينبغي أيضًا لمسؤولي إدارة المخاطر الأمنية والموارد البشرية مناقشة ومراجعة نهجهم في توظيف موظفي إدارة المخاطر الأمنية والاحتفاظ بهم بشكل منتظم. بدلاً من استخدام مواصفات وكفاءات محددة لجميع موظفي إدارة المخاطر الأمنية، ينبغي للنهج الاستراتيجي الأكثر قدرة على التكيف أن يسمح بمرونة أكبر فيما يتعلق بالخبرة والمهارات اللازمة لأدوار محددة في المنظمة.

بناء القدرات

يجب أن يشكل تحديد احتياجات التعلم والتطوير جزءًا أساسيًا من التخطيط على المستوى الاستراتيجي، مع التعاون المرتبط بين قادة إدارة المخاطر الأمنية وقادة الموارد البشرية. (أنظر **الأداة 8: نموذج خطة التعلم والتطوير**). ينبغي النظر إلى تحديد الأهداف الإستراتيجية التي تهدف إلى بناء قدرات موظفي إدارة المخاطر الأمنية (SRM) على أنه استثمار، وليس كنفقة إضافية (أنظر **الأداة 9: مثال على مصفوفة التدريب الاستراتيجي**). ومن الأمور الحاسمة في هذا الأمر ضمان اتباع نهج استراتيجي لمواصلة التطوير المهني - وهو النهج الذي يحدد ويشجع فرص التقدم والنمو لموظفي إدارة المخاطر الأمنية، مما يسمح لهم بالبقاء مرنين في مواجهة الاحتياجات المتغيرة مع تعميق الممارسات الجيدة.

موارد مفيدة

- **إدارة GISF لأمن عمال الإغاثة ذوي الملامح المتنوعة**
- **GISF نحو إدارة مخاطر أمنية شاملة**
- **أمن سهل الوصول من GISF إدارة الناس**
- **بودكاست GISF – حلقة عن السلامة النفسية**
- **شركة ماكينزي آند كومباني: ما هي السلامة النفسية؟**
- **GISF الأمن الإنساني في عصر عدم اليقين: تقاطع المخاطر الرقمية والمادية**

3.8 الربط بالشؤون القانونية

تتمتع الوظائف القانونية ووظائف إدارة المخاطر الأمنية بهدف مشترك وهو حماية المنظمة من الضرر. من خلال التعاون والتواصل الوثيق، يمكن لكل وظيفة أن تساعد الأخرى على تحسين الأمن والامتثال في جميع أنحاء المنظمة. من المحتم أيضًا أن تؤثر القوانين المختلفة على عمل فريق الأمن. إن تحديد الأطر التنظيمية التي تنطبق لا يشكل سوى الخطوة الأولى، إذ يتعين على مسؤولي إدارة المخاطر الأمنية والقانونيين أيضًا مناقشة وتحديد كيفية تفسير هذه اللوائح ضمن سياقات تشغيلية محددة.

تلبية متطلبات واجب الرعاية

يشير واجب الرعاية إلى المتطلبات القانونية (والأخلاقية) للمنظمة لاتخاذ جميع الخطوات اللازمة لضمان الصحة البدنية والعقلية لموظفيها. على الرغم من أن معظم المنظمات لديها فهم جيد لكيفية ارتباط واجب الرعاية بموظفيها المباشرين، إلا أن التعقيدات تنشأ عند تحديد مسؤوليات واجب الرعاية تجاه:

- الموظفين العاملين في سياقات قانونية مختلفة.
- الموظفون العاملون بأنواع مختلفة من العقود، مثل الموظفين الدوليين والموظفين الوطنيين والمستشارين والمتطوعين والمعالين.
- الموظفون العاملون لدى شركاء التوصيل الخارجية أو الاستشاريين الخارجيين.
- شركاء التسليم (أنظر GISF موارد: الإدارة الأمنية وتنمية القدرات: الوكالات الدولية العاملة مع الشركاء المحليين).

نصيحة هامة: أداة التقييم الذاتي لواجب الرعاية

قام المركز السويسري للكفاءة في التعاون الدولي (CINFO) وGISF بتطوير أداة شاملة للتقييم الذاتي لواجب الرعاية. يسمح هذا للمنظمات بتقييم جوانب السلامة والأمن المتعلقة بواجب الرعاية لديها. تستخدم الأداة خمس خطوات، من المستوى الأولي إلى المستوى الأمثل، لتحديد نقاط القوة والمجالات التي تحتاج إلى تحسين في المنظمة في أربعة مجالات: المعلومات والمراقبة والوقاية والتدخل.

موارد: https://dutyofcare.cinfo.ch/index.html

أمثلة من القطاع:

"كان تقاسم المخاطر يشكل تحديًا كبيرًا بالنسبة لنا عندما كنا نعمل مع المستشارين والمنظمات الشريكة. غالبًا ما كان عملاؤنا وشركاؤنا في التسليم يواجهون صعوبة في التعامل مع احتمالية وجود درجة من واجب الرعاية للمستشار، حيث لم يكونوا موظفين لديهم أو متعاقدين معهم بشكل مباشر. لحل هذه المشكلة، قامت فرق الأمن والقانون لدينا بإعداد عدد من مذكرات التفاهم لتوضيح الأدوار، حيث لم يكن هناك وضوح بشأن من يجب أن يتحمل المسؤولية. وهذا يعني في بعض الأحيان تأخير المشاريع بشكل كبير، وتصبح العمليات مستهلكة للموارد بشكل كبير".

(مشارك في المقابلات الفردية، مستوى العمليات في منظمة غير حكومية)

"إن مسألة واجب الرعاية للموظفين الوطنيين من الناحية الطبية في مؤسستي الأخيرة تعني أنه عندما يتعرض أحد الموظفين لحادث سيارة ولا تتوفر الجراحة لمنع البتر، كان علينا نقله جواً من الصومال إلى إثيوبيا وتمويل تكاليف باهظة للرعاية المستمرة والعلاج الطبيعي".

(مشارك في المقابلات الفردية، قائد استراتيجي في منظمة غير حكومية)

من منظور استراتيجي، من الضروري للعديد من القادة الوظيفيين أن يكون لديهم فهم واضح لموضع وجود تعقيدات واجب الرعاية وتحديد موضع المسؤوليات. يجب على فرق إدارة المخاطر الأمنية (SRM) والموارد البشرية (HR) والبرامج والقانون إجراء تمارين لرسم خريطة المعنيين لمساعدتهم في توضيح وتقييم تعقيدات واجب الرعاية في منظماتهم. يمكن أن تُغذي نتائج هذه الأنشطة التخطيط الاستراتيجي والتنفيذ العملي.

مثال لتخطيط أصحاب المصلحة:

أصحاب المصلحة	واجب الرعاية المباشرة	واجب الرعاية المشترك	الواجب الأخلاقي في الرعاية
موظف مباشر (دوام كامل، دوام جزئي)	X		
مستشار (داخلي)	X		
متطوع	X		
زائر	X		
شريك تسليم شخصي		X	
مستشار (منظمة خارجية)		X	
الموظفين المعارين لمنظمة خارجية		X	
موظف جمعية عضو			X

أصحاب المصلحة	واجب الرعاية المباشرة	واجب الرعاية المشترك	الواجب الأخلاقي في الرعاية
مستفيد			X
تابع لموظف			X
عندما يكون هناك واجب رعاية مشترك، فيجب إجراء العناية الواجبة المناسبة بين المنظمات الشريكة. ينبغي وضع اتفاقيات أو مذكرات تفاهم واضحة تحدد المسؤوليات والتوقعات وأي معايير دنيا متفق عليها تتعلق بواجب الرعاية.			
عندما يكون هذا واجبًا أخلاقيًا للرعاية، يجب على المنظمة أن تحدد بوضوح الدعم والموارد والآليات التي يمكن تقديمها. قد يتم أيضًا تقديم التوجيه والمشورة، ولكن لا يوجد التزام قانوني يفرض على أصحاب المصلحة الامتثال.			

خلق ثقافة التفاهم حول "الواجب تجاه الأفراد"

يقع على عاتق أصحاب العمل واجب رعاية موظفيهم. لكن يقع على عاتق الموظفين أيضًا مسؤولية تجاه منظماتهم للمشاركة بنشاط في التخطيط للسلامة والأمن، واتباع إجراءات الطوارئ والتشغيل القياسية في سياسات الشركة، واستخدام الفطرة السليمة العامة لتجنب المخاطر غير الضرورية عند القيام بأنشطة نيابة عن أصحاب العمل.

من الناحية المثالية، تسير الواجبات على المستوى التنظيمي والفردي جنبًا إلى جنب. يجب عليهم معًا خلق ثقافة يهتم فيها أصحاب العمل بصحة موظفيهم وسلامتهم وأمنهم ورفاهيتهم. ينبغي لأصحاب العمل تطوير وإخراج سياسات وإجراءات وإرشادات إدارة المخاطر الأمنية المناسبة لحماية الموظفين من الضرر. وبدوره، ينبغي للموظفين أن يشاركوا بشكل نشط في هذه البروتوكولات ويتبعوها.

لخلق ثقافة المسؤولية المشتركة على المستوى الاستراتيجي، هناك حاجة إلى علاقة صحية ومتبادلة بين صاحب العمل والموظف. ينبغي للموظفين التصرف بطريقة مسؤولة وآمنة، ولكن يتعين على أصحاب العمل أيضًا أن يكونوا استباقيين في تحديد المعايير المناسبة. إن تحديد توقعات غير واقعية على المستوى الاستراتيجي من شأنه أن يؤدي إلى نقص المشاركة إذا شعر الموظفون أنهم غير قادرين عمليًا على تحقيق أهدافهم من خلال العمل ضمن تلك المعايير.

من ثم فمن الضروري تحديد موقف المنظمة بشأن واجب الرعاية والتوقعات من الأفراد. لا ينبغي أن يعتمد هذا على الالتزامات التعاقدية فحسب، بل أيضاً على ردود أفعال الموظفين ومشاركتهم. إن توفير طرق واضحة وسهلة لتقديم الملاحظات هي نقطة بداية أساسية.

قد تشمل الخيارات ما يلي:

- مراجعات دورية لمدير الخط المباشر.
- آليات تقديم التقارير مجهولة المصدر.
- خطوط مساءلة محددة بوضوح حتى يعرف الموظفون الجهة التي يمكنهم الإبلاغ عن مخاوفهم إليها.
- إعداد التقارير على أساس التطبيق.
- مقابلات الخروج.
- خلق ثقافة إيجابية حول الإبلاغ عن الحوادث الوشيكة (على سبيل المثال، ربط الإبلاغ عن الحوادث الوشيكة/المخاوف بمؤشرات الأداء الرئيسية لمدير الخط المباشر).

موارد مفيدة

- تقرير ISOS العالمي لمعايير واجب الرعاية، 2015
- نموذج واجب الرعاية من CINFO

3.9 الربط بالحماية

مع الأخذ في الاعتبار أن التعريفات الدقيقة ونطاق الحماية قد تختلف بين المنظمات، إلا أن هناك العديد من المجالات التي تتوافق فيها الحماية والأمن. وفي المجال الإنساني، تعني الحماية على نطاق واسع منع إلحاق الضرر بالناس - والبيئة - أثناء تقديم المساعدات الإنمائية والإنسانية. من خلال تطور الحماية في القطاع، قامت العديد من المنظمات بتضمين حماية صحة, رفاهية و الناس حقوق لجميع الأفراد - مع التركيز على المجتمعات التي نخدمها - للعيش بعيدًا عن سوء المعاملة والضرر والإهمال. يوضح هذا الحاجة المستمرة للتعاون الوثيق بين وظائف الحماية وإدارة المخاطر الأمنية.

التعاون في وضع النهج

من الضروري أن ندرك أن قضايا الحماية يمكن أن تتحول بسرعة إلى قضايا تتعلق بالسلامة والأمن لجميع الأفراد المعنيين - بدءًا من أولئك الذين يقدمون الشكوى، إلى الجاني المزعوم وأولئك المكلفين بالتحقيق.

رأي الخبراء

"لا توجد قضايا تتعلق بالحماية ولكنها في الوقت نفسه قضايا تتعلق بالسلامة والأمن."
(مشارك في المقابلات المعمقة، مسؤول استراتيجي في إدارة المخاطر الأمنية لمنظمة غير حكومية)

يمكن أن تتحول الحملات المستهدفة والاعتداءات تجاه المنظمة وموظفيها إلى تصعيد سريع حتى من مجرد ادعاء واحد يتعلق بالحماية. إن العمل في سياقات تفتقر إلى القدرة على مراقبة وتقييم والإبلاغ عن قضايا الحماية يمكن أن يؤدي أيضًا إلى زيادة المخاطر، مما يتطلب نهجًا أكثر تكاملاً واستراتيجية.

أمثلة من القطاع:

"في الصومال، يظل خطر تجنيد الموظفين القصر أو الموظفين الذين لديهم سجلات إجرامية سابقة حاضراً على الدوام، وغالباً ما تعتمد عملية التحقق على الاتصال بالشرطة المحلية وقادة المجتمع في المناطق الريفية.

أثار التوظيف في هذا السياق العديد من القضايا، بما في ذلك التنافس بين المجتمعات المحلية على المنظمة التي كنت أعمل بها. كان علينا أن نحقق توازنًا متساويًا بين الأعداد المعينين من مجموعات عرقية مختلفة، وكان الزعماء العرقيون يحضرون إلى المكتب للمطالبة بالتبرير إذا ظنوا أنه تم تجاهلهم. لقد تم تنبيهنا إلى حالة بيع وظائف مقابل الجنس من قبل أحد زعماء المجتمع مما دفعنا إلى إجراء مراجعة أمنية. ثم ظهرت إحدى النساء، التي تأكدنا من أن عمرها يزيد عن 18 عامًا من خلال المجتمع، تشير إلى أن عمرها 16 عامًا فقط بالنسبة لموظف آخر، واضطررنا للدفاع عن أنفسنا ضد اتهامات عمالة الأطفال.

يبدو أن أحد أعضاء الموظفين أخبر زملاءه أنه على وشك الزواج من إحدى فتيات المجتمع، وأبلغني هؤلاء الموظفون أن عمرها لا يتجاوز 13 أو 14 عامًا. بعد مقاومة كبيرة من المجتمع، تمكنا في النهاية من التحدث إلى الفتاة التي أفادت بأنها تبلغ من العمر 18 عاماً ووافقت على الزواج، ولكن يبدو أنها كانت تحت ضغط المجتمع. "تم وضع تدريب إضافي في مجال الحماية من خلال ميسرين محليين، لكن حالات الزواج المبكر وبيع الوظائف لا تزال تظهر."

من مشارك في المقابلات الاستقصائية الرئيسية (KII)، مدير إدارة المخاطر الأمنية التشغيلية في منظمة غير حكومية

من منظور استراتيجي، يتعين على قادة إدارة المخاطر الأمنية والحماية والموارد البشرية والبرامج العمل في تعاون وثيق لضمان تحديد المخاطر المحتملة والاتفاق على التخفيف منها وتوضيح الأدوار في الوقاية والرد والتعافي. من الأهمية بمكان لهذه العلاقة ضمان الفهم السياقي للعملية والأدوار اللازمة للتخفيف من الحماية وتصاعد المخاطر الأمنية.

قد تختلف دورات حماية إدارة الحوادث قليلاً بين المنظمات. لكن هناك نقاط دخول حيث يمكن للعلاقة المتينة بين الأمن والحماية أن تساعد في تبسيط العمليات وتمكين نتائج أكثر أمانًا لجميع الأطراف المعنية، فضلاً عن تعزيز الفهم والنهج المستنيرة للإبلاغ عن الحوادث.

إن إحدى الطرق لضمان التعاون الوثيق هي من خلال عقد تدريبات التحقيق. ينبغي أن توضح هذه الجلسات الأدوار التنظيمية أثناء وقوع حادث يتعلق بالحماية، مع التأكد من مشاركة نقاط الاتصال الخاصة بالحماية وإدارة المخاطر الأمنية، وأن جميع الأطراف تتبع بروتوكولات واضحة ومبنية على الأدلة. تذكّر أنه رغم الحاجة إلى إطلاع موظفي إدارة المخاطر الأمنية (SRM) على الحادث، إلا أنهم على الأرجح ليسوا الفريق المناسب لإدارة أو قيادة حادثة تتعلق بالحماية.

في بعض المنظمات، تكون العلاقة بين السلامة والأمن أكثر تشابكًا. على سبيل المثال، قد يكون محور الاهتمام بالحماية هو محور الاهتمام بالأمن أيضًا. لا توجد طريقة واحدة لإنشاء هذه العلاقة أو عملها على النحو الأمثل، حيث أنها تعتمد إلى حد كبير على احتياجات المنظمة وتوقعاتها. الأمر المهم هو أن تفهم المنظمة وظائف كل من الحماية والأمن بشكل مستقل بالإضافة إلى الترابط بينهما.

موارد مفيدة

- مركز دعم الموارد والحماية
- ندوة GISF عبر الإنترنت: تقاطع الأمن والحماية
- مدونة التفاعل: إطلاق مجموعة الأدوات المرئية لحماية المجتمع
- مذكرة إرشادية من مؤسسة GISF حول تنفيذ دورة الحماية

3.10 الربط بإدارة السفر

غالبًا ما تكون إدارة ومراقبة سفر الموظفين خاضعة إلى حد كبير للمتطلبات المالية. يتزايد أيضًا الاعتماد على سياسات المسؤولية الاجتماعية للشركات، مثل أهداف الحد من الانبعاثات الكربونية. ومع ذلك، فإن النشر الأخير من المنظمة الدولية للمعايير (ISO) ISO 31030: إدارة مخاطر السفر، يقدم هذا التقرير بوضوح الحجة التي تؤكد على ضرورة دمج إدارة مخاطر السلامة والأمن بشكل وثيق في التخطيط الاستراتيجي لسفر الموظفين (سواء الدولي أو الوطني).

دارة مخاطر السفر (TRM)

تقدم ISO 31030 المشورة والتوجيهات الأساسية للمنظمات حول كيفية ضمان قدرة المسافرين على أداء واجباتهم بأفضل شكل ممكن في بيئة سليمة وآمنة بقدر الإمكان.

ينبغي أن تشارك وظائف إدارة المخاطر الأمنية (SRM) بشكل كبير في تطوير ودعم أفضل الممارسات في سياسات إدارة مخاطر السفر (TRM)، وتقديم مدخلات تقنية أساسية في:

- تحليل السياق والإحاطة، مثل مصادر المعلومات التي يجب استخدامها وكيفية تقديمها والإعلام بها.
- الترخيص والموافقة، مثل إنشاء نظام للموافقة على السفر والترخيص به على أساس تقييمات المخاطر وملفات تعريف المسافرين وأنشطتهم، وليس فقط الاعتبارات المالية.
- تتبع ورصد المسافرين، مثل ضمان وعي شامل داخل المنظمة بمواقع المسافرين في حالة وقوع حوادث.
- الإخلاء وإعادة التوطين، مثل تطوير خطط طوارئ ملائمة للسياق.

- تطوير إجراءات التشغيل القياسية (SOPs) للمنظمة، والتي قد تشمل معدلات نفقات البدلات، بالإضافة إلى سياسات اختيار الإقامة والنقل التي تدعم إدارة مخاطر الأمن بشكل جيد.
- تطوير إجراءات تخطيط السفر والتنقل داخل البلد.

موارد مفيدة

- **ISO 31010: إدارة مخاطر السفر لعام 2021: إرشادات للمنظمات**

مدغشقر

يسافر أحد أعضاء فريق عمل مطبخ العالم المركزي إلى مدغشقر للمساعدة في توزيع الوجبات في أعقاب الإعصار. ينبغي لأي سفر للموظفين أن يسترشد دائمًا بسياسات قوية لإدارة مخاطر السفر.

مكتب تنسيق الشؤون الإنسانية/إيفيان راكوتوارينوني

الفقرة 4: التنسيق الاستراتيجي لإدارة المخاطر الأمنية (SRM)، والتعاون، والشراكات

نظرًا لتنوع التهديدات الجديدة، بدءًا من التغيرات الجيوسياسية إلى المخاطر الرقمية والإلكترونية، أصبحت أهمية التعاون الاستراتيجي على مستوى الأمن أمرًا بالغ الأهمية. يشمل ذلك تعزيز الشراكات على مستوى القطاع، وإنشاء شبكات عالمية وإقليمية ومحلية مخصصة، وتشكيل مجموعات عمل، والحفاظ على الروابط الأساسية مع الوكالات الأخرى والهيئات الرسمية وغير الرسمية. يتم تنفيذ هذه العملية غالبًا بشكل فعال على المستوى التشغيلي. لكن المنظمات قد تواجه صعوبة في صياغة وتنفيذ هذه الشراكات والشبكات ومجموعات العمل بشكل استراتيجي، حيث تعتمد على الموظفين في المستوى التشغيلي لتشكيل العديد من هذه العلاقات، سواء بشكل رسمي أو غير رسمي.

إرشادات إدارة المخاطر ISO 31000:2018 تسلط الضوء على أهمية مشاركة أصحاب المصلحة من خلال الاتصال والتشاور خلال عملية إدارة المخاطر.

إن إشراك مختلف أصحاب المصلحة على المستوى التشغيلي أمر حيوي لتبادل المعلومات الأمنية، وتقييم المخاطر، وتنفيذ تدابير أمنية فعالة. ومع ذلك، فإن غياب التنسيق والتعاون على المستوى الاستراتيجي مع مختلف الفاعلين، المدعوم والموجه من القيادة العليا، يعرض الموظفين لمخاطر إضافية. هذا أمر مهم بشكل متزايد في بيئات العمل المعقدة عند التعامل مع الجماعات المسلحة من غير الدول وضمان الامتثال لتشريعات مكافحة الإرهاب.

4.1 التعاون الأمني بين الوكالات

يجب على المنظمات الانخراط على مستوى القطاع بأكمله والتنسيق مع مجموعات العمل الإنساني والتنمية وحقوق الإنسان لتبادل المعرفة والخبرات في التصدي للتهديدات. إن المشاركة بين القطاعات أمر أساسي لضمان إدارة جيدة للمخاطر الأمنية. توجد بالفعل عدة آليات تشغيلية واستراتيجية للتنسيق بين الأمم المتحدة والمنظمات غير الحكومية على المستويات الوطنية والإقليمية والعالمية في إدارة مخاطر الأمن الإنساني والتخصصات الموازية. وتشمل هذه المجموعة الاستشارية المدنية العسكرية (CMAG)، ومجموعة العمل العالمية للوصول، وإنقاذ الأرواح معًا (SLT) ومجموعات العمل القطرية المعنية بالوصول والأمن، والفرق القطرية الإنسانية.

وفي السنوات الأخيرة، قامت المنظمات غير الحكومية أيضًا بتشكيل شبكات ومنصات أمنية مختلفة على مستوى البلدان والأقاليم والمقار الرئيسية. تساعد شبكات ومنصات التعاون الأمني هذه على تسهيل تبادل المعلومات الأمنية، وزيادة الوعي بإدارة المخاطر الأمنية الجيدة من خلال التدريبات وورش العمل، وتعزيز أفضل الممارسات بين المنظمات.

يجب على المنظمات أن تسعى إلى إضفاء الطابع الرسمي على هذا التعاون على المستوى الاستراتيجي والتأكد من الترويج له وفهمه على المستوى التشغيلي لدعم الموظفين في المشاركة والتعاون مع المنظمات. **GISF دليل التعاون الأمني للمنظمات غير الحكومية** يقدم المشورة والموارد العملية لدعم المنظمات غير الحكومية في تسهيل التعاون الأمني الفعال مع المنظمات الأخرى التي تعمل في نفس السياق.

تعد المشاركة والتعاون بين القطاعات ذات أهمية خاصة بالنسبة للمنظمات غير الحكومية الصغيرة، والشركات الناشئة داخل الدولة، وفرق الاستجابة لحالات الطوارئ، لأنها تمكن من الوصول الفوري إلى المعلومات المهمة التي قد لا تمتلك المنظمة الموارد اللازمة لتحديدها بنفسها. هناك العديد من الحواجز الخارجية والداخلية التي تعوق التعاون الفعال في مجال إدارة المخاطر الأمنية، وتحتاج المنظمات إلى محاولة التغلب على هذه التحديات لضمان التعاون الوثيق.

تشمل بعض الاعتبارات الهامة ما يلي:

- ✓ المناصرة - هل نعزز الحاجة إلى التعاون مع المنظمات الأخرى؟ هل تم فهم فوائد التعاون الأمني عبر المنظمات وداخلها؟ من الأمثلة الجيدة على ذلك جمع الأموال من خلال الجهات المانحة المؤسسية والتأثير على أطر السياسات المتعلقة بالتكاليف المباشرة/غير المباشرة.
- ✓ المساءلة - هل يتحمل موظفونا المسؤولية عن الحفاظ على العلاقات مع المنظمات الأخرى؟ إذا لم تتم إدارة العلاقات مع المنظمات الأخرى بشكل فعال، فكيف يمكننا تحسين ذلك؟
- ✓ الموارد - هل قمنا بتوفير الموارد البشرية والمالية اللازمة لتمكين المنظمة من التواجد في آليات التنسيق هذه؟ هل نحتاج إلى النظر إلى بنية الأمن لدينا كمنظمة؟ هل لدينا الأنظمة المناسبة لوضع الميزانية المخصصة للأمن؟
- ✓ تنوع المناهج الأمنية - تتمتع المنظمات المختلفة بمناهج وقدرات أمنية مختلفة، ولكن كيف يمكننا أن نتعلم من الآخرين؟ هل نقارن بين مناهجنا الأمنية ومنهجيات المنظمات الأخرى التي تعمل في نفس البيئات؟
- ✓ السرية - لا ترغب المؤسسات في مشاركة المعلومات الحساسة لأن ذلك قد يعرضها لمخاطر إضافية. ما هي المعلومات التي يمكننا مشاركتها وكيف يمكننا مشاركتها؟ إن بناء العلاقات مع الآخرين أثناء عمليات الاستجابة للطوارئ أو قبلها بشكل مثالي يمكن أن يؤتي ثماره لأنه يساعد في تعزيز الثقة والتبادل المتبادل للمعلومات.
- ✓ الأولويات والقيود الزمنية - إن حضور اجتماعات الأمن والتواصل مع المنظمات الأخرى يتطلب وقتًا وموارد. كيف نضمن إعطاء الأولوية للتعاون الأمني واعتباره عامل تمكين يعزز ويحسن تنفيذ البرنامج؟

قد تؤدي الإجابة على هذه الأسئلة إلى الحاجة إلى التوجيه والمسؤوليات الإضافية والموارد. إن توضيح الحاجة إلى التعاون والشراكة في استراتيجيتك لإدارة المخاطر الأمنية سيزيد من قدرة المنظمة على المدى الطويل لتعزيز تبادل المعلومات والتنسيق بشكل أكثر فعالية بين المنظمات.

ومن الأمثلة على كيفية عمل ذلك هو (SLT) إطار عمل إنقاذ الأرواح معًا، الذي تم إنشاؤه لتنسيق العمل بين الأمم المتحدة والمنظمات غير الحكومية. يهدف برنامج SLT إلى تعزيز قدرة المنظمات الشريكة على اتخاذ قرارات مستنيرة، وإدارة المخاطر، وتنفيذ ترتيبات أمنية فعّالة تُمكّن من تقديم المساعدات وتحسين أمان الأفراد واستمرارية العمليات. قم بتضمين هذا في استراتيجية إدارة المخاطر الأمنية الخاصة بك واطلب من موظفيك المشاركة وفقًا لذلك.

لفهم هيئات التنسيق أو فرص التعاون المتاحة والملائمة، ينبغي للمنظمات إجراء تحليل لأصحاب المصلحة الرئيسيين فيما يتعلق بإدارة المخاطر الأمنية. ينبغي أن يتم ذلك على المستوى الاستراتيجي مع الفهم الشامل المستنير لهيئات التنسيق على المستوى التشغيلي التي يشارك فيها الموظفون والمبادرات التي تم تشكيلها. إن القيام بهذه العملية من خلال نهج تشاركي، سيمكن المنظمات من تطوير استراتيجيات تنسيق إدارة المخاطر الأمنية مع المخاطر التي تربط العمليات العالمية بالعمليات الميدانية والعكس صحيح.

4.2 التعاون والتنسيق الداخلي

هناك موضوع متكرر عند ضمان تنفيذ استراتيجية إدارة المخاطر الأمنية (SRM) بشكل فعال داخل المؤسسة وهو إشراك جميع أصحاب المصلحة. وهذا لا يعني مجرد التحدث مع أعضاء الفريق التشغيلي، بل إشراكهم في العملية. يمكن أن يشمل ذلك إشراك الموظفين التشغيليين في مجموعة عمل إدارة المخاطر متعددة الوظائف (أنظر الفقرة 2) وإشراكهم في رحلة تطوير السياسات. للقيام بذلك، ينبغي على المنظمات أن:

- تقييم الاحتياجات التشغيلية بانتظام – إجراء مقابلات مع المخبرين الرئيسيين (KIIs)، وعقد اجتماعات إدارة مخاطر أمنية SRM دورية، وتحديد المخاطر الأكثر شيوعًا أو الأشد خطورة التي يواجهونها في أدوارهم. يمكن استخدام هذه المعلومات للتأثير على أولويات إدارة المخاطر الأمنية.
- مناقشة السيناريوهات الواقعية - حاول أن تجعل السيناريوهات مرتبطة بما يواجهه الموظفون في احتياجاتهم اليومية. تسليط الضوء على كيفية تمكين إدارة المخاطر الأمنية SRM من أداء البرمجة الفعالة.

بمجرد تحديد المخاوف والقضايا، من الضروري متابعتها وتحديد الأولويات:

- التواصل والإعلام – سيتفاعل الموظفون التشغيليون بشكل أكبر إذا كانوا على اطلاع دائم بالعملية التنظيمية. يمكن للنهج الشفاف أن يمكّن الموظفين من فهم كيف ومتى يتم تطوير استراتيجيات إدارة المخاطر الأمنية. سوف يؤدي هذا إلى زيادة المشاركة ودعم ثقافة الأمن.

- مواءمة إدارة المخاطر الأمنية (SRM) للمنظمة مع موقفها من المخاطر وثقافتها الأمنية – يتطلب ذلك توضيح كيفية تكامل إدارة المخاطر ضمن استراتيجية المنظمة ورؤيتها وأهدافها، وإبراز دورها في تعزيز استراتيجية المنظمة وتمكين برمجيات مستدامة.

اعتبارات عند تنفيذ السياسات العالمية على المستوى التشغيلي

هناك العديد من العوامل التي يجب أخذها في الاعتبار عند تنفيذ السياسات العالمية على المستوى الإقليمي أو الوطني. إذا كان هناك القليل من المشاركة أو عدم وجود مشاركة على الإطلاق مع الموظفين التشغيليين عند تقديم سياسات جديدة، فقد يؤدي هذا إلى العديد من التحديات الكبيرة:

- السياق - غالبًا ما تعمل المنظمات عبر مناطق متعددة، ولكل منها بيئات مختلفة بشكل كبير. لا يمكن أن يكون هناك إجراء واحد يناسب الجميع داخل منظمة.
- ملائمة ثقافيا - من الناحية الثقافية، يتعامل الأشخاص مع إدارة المخاطر بشكل مختلف، وغالبًا ما يكون ذلك بطريقة بديهية للبيئة التي ينتمي إليها هؤلاء الأشخاص.
- التكنولوجيا - في السنوات الأخيرة، سعت المنظمات إلى إيجاد حلول تكنولوجية. يمكن أن تكون هذه تطبيقات جوال تتيح التواصل الجماعي أو توفر تنبيهات التتبع والأمان. هل هذه العناصر متاحة للموظفين داخل المنظمة؟ هل ستقوم المنظمة بتمويل هذا وتوفير الموارد اللازمة له بشكل مناسب؟
- اللغة - يمكن أن تكون لغة إدارة المخاطر الأمنية SRM معقدة وفنية. قد يواجه الموظفون الذين يتحدثون الإنجليزية كلغة ثانية صعوبة في فهم المصطلحات. البساطة هي المفتاح عند التفكير في إدارة المخاطر الأمنية. من الضروري على أخصائيي إدارة المخاطر الأمنية (SRM) أن يُعدلوا لغتهم لتكون مفهومة للآخرين، بدلاً من توقع أن يفهم الآخرون مصطلحات إدارة المخاطر الأمنية SRM الخاصة. إدارة المخاطر الأمنية (SRM) هي عامل تمكين، وبالتالي يجب أن تبذل قصارى جهدها لاكتساب الدعم والالتزام. يمكن أن يؤدي ذلك إلى تحقيق تواصل أكثر فعالية ودقة.

أمثلة من القطاع:

"لقد اتبعت منظمتي بعض السياسات والاستراتيجيات الجيدة للغاية لتحسين إدارة المخاطر الأمنية، لكنها لم تأخذ في الاعتبار الحقائق على أرض الواقع. لا يقرأ الموظفون اللغة الإنجليزية، وإشارة الإنترنت غير موثوقة في مواقع مكاتبنا الميدانية، لذا فإن الأنظمة القائمة على التطبيقات ليست مناسبة. لقد قضينا أيضًا عددًا من الأشهر في محاولة توضيح أن سياسة الحماية التي تم تقديمها ليست مناسبة للسياق."

من مشارك في المقابلات مع المخبرين الرئيسيين، مدير قطري في الشرق الأوسط

4.3 تطوير السياسات للشراكات

عند تطوير الشراكات مع المنظمات غير الحكومية الأخرى ووكالات الأمم المتحدة والجهات المانحة، فإن الفهم الكامل لاستراتيجية إدارة المخاطر الأمنية للمنظمة أمر بالغ الأهمية. يتضمن ذلك فهم نهج المخاطر التنظيمية وسياساتها بشأن العمل في الشراكات بما في ذلك تحديد واضح لمسؤوليات واجب الرعاية.

يمكن أن تأتي الشراكات بأشكال متعددة: دولية، وطنية ومحلية؛ جمعيات الأعضاء؛ شركاء التنفيذ الخارجي؛ وزيادة العمل ضمن الاتحادات. دليل العمل المشترك لشركاء GISF يقدم إرشادات مفصلة حول إنشاء شراكات عادلة بين المنظمات غير الحكومية الدولية والمنظمات غير الحكومية المحلية أو الوطنية.

يقدم هذا الدليل مجموعة كبيرة من الأدوات والتوجيهات حول كيفية إضفاء الطابع الرسمي على إدارة المخاطر الأمنية ضمن الشراكات. ومع ذلك، تحتاج المنظمات أيضًا إلى تحديد سياسة أو موقف عالمي بشأن تشكيل الشراكات. يجب أن تكون هذه سياسة متعددة الوظائف تتيح مراعاة جميع جوانب واجب الرعاية، بما في ذلك الأمن.

على المستوى الأساسي، ينبغي للشراكات أن تتوافق مع استراتيجية المنظمة. من المهم أيضًا أن نتساءل عن سبب تشكيل الشراكات. هل يتم ذلك من أجل توطين تسليم المساعدات الإنسانية أم أنه يتم تشكيل شراكات لتقليل المخاطر التي تتعرض لها المنظمة؟ إذا كان الأمر كذلك، فهل يتم "نقل" المخاطر إلى الشركاء أو "تقاسمها" مع الشركاء؟

يتعلق نقل المخاطر بالنقل الكامل للمخاطر من طرف إلى آخر، وهو ما قد يكون مناسبًا في بعض الظروف إذا كان شفافًا تمامًا ومحددًا ومتفقًا عليه من قبل الطرفين. مع ذلك، لكي يحدث تقاسم المخاطر حقًا، يحتاج الطرفان إلى فهم المخاطر التي يتعرض لها كل طرف، والاتفاق عليها على قدم المساواة، دون اختلالات في التوازن في القوة، وأن الموارد اللازمة لمعالجتها يتم تخصيصها بشكل عادل.

نصيحة هامة: الجهات المانحة والمخاطر

من الممكن أيضًا توجيه أسئلة رئيسية حول المخاطر والشراكات إلى الجهات المانحة، وخاصةً إذا كانت تقوم بنقل المخاطر بشكل كامل. إن الضغط من جانب الجهات المانحة هو أحد الاستجابات الأكثر شيوعاً عند مناقشة المخاطرة غير الضرورية. لذا، يجب على المانحين أيضًا أن يفهموا مستويات المخاطرة التي ترغب في العمل بها.

كما هو موضح في ورقة البحث التي أعدتها GISF، **الشراكات وإدارة المخاطر الأمنية: من وجهة نظر الشريك المحلي**، من الأهمية بمكان أن تنظر المنظمات غير الحكومية إلى الشراكات من منظور المنظمات غير الحكومية المحلية التي تعمل معها.

تتطلب الشراكات الناجحة إنشاء المخاطر الأمنية ونقلها ومشاركتها بين الشركاء. يتطلب القيام بذلك فهمًا تفصيليًا للتحديات الأمنية التي تواجه كلتا المنظمتين في الشراكة، وكيف يمكنك، كشريك داعم، العمل معًا لتحسين الأمن العام لجميع المنظمات المعنية.

هناك قلق شائع آخر بين الموظفين التشغيليين، والذي لا يستطيع العديد من الموظفين على المستوى الاستراتيجي الإجابة عليه، وهو: ما هو واجبي في رعاية شركائنا؟ للإجابة على هذا السؤال، يجب توثيق نهج واجب الرعاية بشكل مناسب وتقديم التوجيهات للموظفين. وللقيام بذلك ينبغي النظر في الأسئلة التالية:

أسئلة حول شراكة إدارة المخاطر الأمنية (الربط مع استراتيجية إدارة المخاطر الأمنية الخاصة بك)	
واجب الرعاية	ما هو واجبنا القانوني والأخلاقي في رعاية شركائنا؟ ينبغي أن تحدد الإجابة معايير الرعاية التي ينبغي للمنظمة أن تقدمها.
الحوكمة والمساءلة	ما هو مستوى إدارة المخاطر الأمنية الذي نتوقعه من شركائنا؟ كيف سنقيس هذا؟ هل اتفاقيات الشراكة توثق إدارة المخاطر الأمنية؟

أسئلة حول شراكة إدارة المخاطر الأمنية (الربط مع استراتيجية إدارة المخاطر الأمنية الخاصة بك) مستمر	
نقل المخاطر مقابل تقاسم المخاطر	هل نقوم بنقل كافة المخاطر ومسؤولية إدارة هذه المخاطر إلى الشركاء، أم أن النية هي تقاسم المخاطر مع الشركاء؟ هل نحن على استعداد لأن يتحمل شريكنا مخاطرة أكبر مما نتوقع من موظفينا أن يتحملوه؟ إذا كانت الإجابة بنعم، ما هو مستوى المخاطرة هذا؟ ما هو الدعم الذي يجب أن نقدمه لمساعدتهم في إدارة هذه المخاطر؟ هل نحن على استعداد لزيادة الدعم لشركائنا بما يتماشى مع مستوى المخاطر التي ينطوي عليها الأمر؟ إذا كانت الإجابة بنعم، ما هو الدعم الذي يجب أن نقدمه؟
السياسات والمبادئ	هل يحتاج شركاؤنا إلى التوافق مع مبادئنا الإنسانية وسياساتنا المحددة؟
إدارة الحوادث الحرجة	ما هو الدعم الذي سنقدمه لشركائنا في حالة وقوع حادث خطير؟ هل يختلف هذا عن الدعم الذي نقدمه لموظفينا؟
نهاية الشراكة	ما مدى واجبنا في الرعاية تجاه الشركاء في نهاية اتفاقية الشراكة؟

إن إدارة الشراكات والعناية الواجبة هي عملية معقدة، ولكنها تحتاج إلى أن تتوافق مع استراتيجية المنظمة وقيمها. لذلك، لضمان الاتساق داخل جميع الشراكات، يجب نشر السياسات التي تحدد واجب المنظمة في رعاية الشركاء على نطاق واسع ومراجعتها على المستوى الاستراتيجي (انظر أيضًا القسم 3.8 الربط بالشؤون القانونية)

موارد مفيدة

- إرشادات إدارة المخاطر وفقًا لمعيار ISO 31000:2018
- تنسيق GISF لإدارة الأمن الإنساني
- GISF، إدارة مخاطر الأمن التعاونية حالة من أجل التنمية المحلية
- إطار عمل الأمم المتحدة لإنقاذ الأرواح معًا
- GISF دليل العمل المشترك للشراكات وإدارة المخاطر الأمنية

جوزيف مالكاميا/مكتب تنسيق الشؤون الإنسانية-جمهورية الكونغو الديمقراطية

جمهورية الكونغو الديمقراطية

يناقش موظفو المفوضية الأوروبية للمساعدات الإنسانية ومكتب تنسيق الشؤون الإنسانية ومنظمة العمل ضد الجوع ومنظمة أوكسفام الاستجابة الإنسانية المشتركة. عند العمل مع الشركاء، من الضروري أن يكون الواجب القانوني والأخلاقي للرعاية راسخًا ومفهومًا.

الفقرة 5: مساهمة إدارة المخاطر الأمنية (SRM) في مرونة المؤسسات واستمرارية الأعمال

إن أن تكون منظمة مرنة يعني أن تكون مستعدة لمواجهة الشدائد، وقادرة على الاستجابة بفعالية للاضطرابات والأزمات، وقادرة على التكيف بشكل إيجابي في مواجهة الظروف الصعبة. تجد المنظمات الإنسانية والتنموية نفسها غالبًا مضطرة للتنقل في بيئات متزايدة التسييس، حيث لم تعد تُعتبر محايدة سياسيًا وتواجه انكماشًا في المساحات المدنية. إن حجم وتواتر الأزمات التي تواجه المنظمات غير مسبوق. يتعين على الاستراتيجيات التنظيمية أن تعترف وتتناول العلاقة بين مخاطر الأمن والسلامة واستمرارية الأعمال والمرونة التنظيمية. يتعين على جميع المنظمات أن تمتلك آليات شاملة للاستجابة بفعالية والتغلب على التحولات - التي لا يمكن التنبؤ بها في بعض الأحيان - في سياقات التشغيل والأحداث الحرجة.

5.1 الاستعداد والتخطيط

يجب على متخصصي إدارة المخاطر الأمنية أن يكونوا حاضرين على الطاولة عندما يتم التخطيط للاستعداد التنظيمي. يجب تعريف المرونة لدى المنظمات والفرق والأفراد والإشارة إليها في السياسات المتعلقة بإدارة المخاطر الأمنية، إلى جانب التدابير العملية حول كيفية دعم إدارة المخاطر الأمنية للمنظمة على نطاق أوسع في المناقشات حول الاستعداد والتخطيط للاستجابة. تلعب السلامة والأمن دورًا مهمًا في إعدادات الاستجابة للأزمات التقليدية وكذلك في حوادث الاحتيال ومخاطر السمعة والحماية أو الأوبئة العالمية.

مكتب تنسيق الشؤون الإنسانية/جيما كورتيس

فنزويلا

عامل إغاثة يقيس درجات حرارة عائلة خلال جائحة كوفيد-19. يتعين على المنظمات أن تضع آليات لتكييف إجراءاتها الأمنية استجابة للأحداث الحرجة، مثل حالات الطوارئ الصحية العامة.

التعاريف الرئيسية:

- **استمرارية الأعمال:** التخطيط الاستراتيجي والإجرائي الذي تقوم به المنظمة لضمان استمرار الوظائف الأساسية أثناء وبعد وقوع حدث تخريبي.
- **أزمة:** حدث أو سلسلة من الأحداث التي تعطل العمليات العادية بشكل كبير، أو تسببت، أو من المرجح أن تتسبب، في عواقب وخيمة تؤثر على المنظمة بأكملها. تتطلب الأزمة عادة استجابة تتجاوز آليات الإدارة العادية لمعالجة التأثير وعواقبه.
- **حادثة حرجة:** حدث سلبي يؤدي أو يمكن أن يؤدي إلى ضرر جسيم للموظفين، أو تعطل البرامج والأنشطة، أو خسارة أو ضرر لأصول المنظمة أو سمعتها، ولكن يمكن إدارته ضمن البروتوكول العادي بدعم من المقر الرئيسي.
- **حادث:** تتم إدارة الحادث عادة من قبل الأفراد الموجودين في البلد أو بالقرب من المكان الذي وقع فيه الحادث أو يحدث فيه.
- **المرونة التنظيمية:** قدرة المنظمة على توقع التهديدات الأمنية أو الحوادث أو الاضطرابات ومواجهتها والاستجابة لها والتعافي منها مع الحفاظ على وظائفها الأساسية وسمعتها وثقة أصحاب المصلحة.

الاستعداد للأزمات المتعلقة بإدارة المخاطر الأمنية أو الأزمات التي لها آثار على إدارة المخاطر الأمنية

إن النجاح في حل وإدارة أي حالة أزمة يعتمد على قدرة المنظمة على اتخاذ القرارات المناسبة بسرعة. ويتطلب ذلك الاستعداد وتدفقًا جيدًا للمعلومات وقنوات اتصال واضحة يفهمها جميع الموظفين. في حين أن كل أزمة تختلف عن الأخرى ولا يمكنك التخطيط لكل الاحتمالات، إلا أنه يمكنك التخطيط لكيفية الاستجابة بشكل فعال لكل أزمة، مما يسمح بنطاق ترددي حرج للمنظمة لمواصلة العمل دون استخدام جميع مواردها لحل حدث واحد. يلعب النهج الاستراتيجي التنظيمي لإدارة الأزمات واستمرارية الأعمال دورًا مهمًا في تخصيص الموارد اللازمة لإدارة مخاطر الأزمات للاستعداد والاستجابة للأحداث التخريبية.

تختلف الاستعدادات والتخطيط حسب المنظمة وبين الوظائف الاستراتيجية المختلفة. على سبيل المثال، من المرجح أن تقوم المنظمات التي تعمل في بيئات معرضة للنزاع بتطوير إطار عمل لاتخاذ قرارات مستندة إلى المخاطر، واستثمار الموارد في بناء منشآت أكثر أمانًا، وتوظيف أفراد أمن مدربين، وإقامة شراكات استراتيجية وآليات للتنسيق بشكل أفضل في استجابتها للأزمات. في المقابل، قد تقوم المنظمات التي تعمل بشكل أساسي في سياقات ذات مخاطر منخفضة بإجراء استثمارات متواضعة فقط في بنيتها التحتية، أو مراجعة خطط إدارة الأزمات الخاصة بها بشكل دوري، أو وفقًا لفترات التنبؤ بعدم الاستقرار، مثل الانتخابات أو المخاطر المرتبطة بالطقس الموسمي. إن كلا السياقين يفرضان مخاطر تشكل تهديدًا كبيرًا للعمليات التنظيمية، لذا فمن الأهمية بمكان ألا ننظر إلى إدارة المخاطر الأمنية والاستعداد لها من خلال عدسة السلامة والأمن فقط.

يمكن أن يأخذ الاستعداد الاستراتيجي للمنظمة شكل تقييمات شاملة للمخاطر، وتخطيط السيناريوهات الاستراتيجية، وتخصيص الموارد على أساس المخاطر، والتعلم المستمر والتحسين. يمكن لمسؤولي إدارة المخاطر المؤسسية أيضًا إجراء تقييم لاحتياجات التدريب للمنظمة بأكملها، مما يؤدي إلى توفير الفرص للموظفين للحصول على المؤهلات ذات الصلة وبناء القدرات التنظيمية.

5.2 نهج متعدد الوظائف لإدارة الأزمات

إن النهج المتعدد الوظائف هو المفتاح لإدارة الأزمات التي تؤثر على مؤسستك أو موظفيك و/أو أصولك بنجاح. إن النجاح في التعامل مع أي أزمة يعتمد على وجود فريق متعدد الوظائف يعمل معًا ويتعاون ويتواصل لتحقيق هدف مشترك: حل الأزمة. إن هذا التعاون المتعدد الوظائف يحتاج إلى الرعاية والتطوير قبل وقوع الأزمة، وليس أثناء محاولة الاستجابة لموقف ما.

التعدد الوظيفي أثناء الاستجابة للأزمة

رغم أهمية تحديد قائد فريق الأزمات (عادةً ما تختار المنظمات الرئيس التنفيذي أو المدير التشغيلي أو مديرًا لديه معرفة مؤسسية كبيرة أو خبرة في إدارة الأزمات لشغل هذا الدور)، فإن جميع الوظائف الممثلة داخل فريق إدارة الأزمات تُعتبر "مالكة إجراءات"، حيث تتمتع بدور ومسؤوليات متصلة ولكنها مع ذلك محددة. ينبغي النظر إلى قادة إدارة المخاطر الأمنية على أنهم متساوون في فريق يتألف من ممثلين من وظائف رئيسية أخرى.

جهاز PAD-SL

سريلانكا

يشارك المشاركون في تمرين البحث والإنقاذ استعدادًا للفيضانات. يعد التدريب أمرًا حيويًا للحفاظ على سلامة جميع أعضاء الفريق عند العمل في بيئات عالية الخطورة.

يوضح مخطط العلاقات أدناه العلاقات متعددة الوظائف ضمن فريق إدارة الأزمات.

أمثلة من الوظائف المتعددة أثناء الاستجابة للأزمة، سلامة المواقع الدولية

- واجب الالتزامات الأساسية/ القانونية
- العناية الواجبة
- متطلبات التعاقد
- مذكرات التفاهم (MoUs)

- حجوزات السفر
- متطلبات التأشيرات
- مجموعة أدوات الصحة والسلامة للسفر في المكتب (صناديق الإسعافات الأولية، هواتف الأقمار الصناعية)

- مخاطر الأمن السيبراني
- الأمن الرقمي
- الامتثال للائحة العامة لحماية البيانات (GDPR)

- الاتصالات الداخلية
- البيانات الخارجية/ الصحفية
- اتصالات الأزمات

- صناديق الطوارئ
- سلف نقدية

- ضباط ارتباط الأسرة
- استمارات أقارب الدرجة الأولى
- استمارات إثبات الحياة

- إدارة الجهات الخارجية المعنية

- إدارة ميزانية المشروع

- مواقع الموظفين
- إجراءات التسجيل

العمل كالمعتاد

الأزمات هي حوادث لا يمكن إدارتها ضمن الإجراءات والعمليات الروتينية. لذا، من المهم أن تأخذ المنظمات في اعتبارها عند تصميم خطط إدارة الأزمات و/أو خطط استمرارية الأعمال مدى قدرتها على مواصلة تلبية متطلبات الأعمال العادية والمستمرة بينما يكون القادة الرئيسيون مشغولين بالاستجابة لحادث كبير. تتطلب المرونة التنظيمية الفعالة من جميع قيادات الوظائف، بما في ذلك الأمن، التأكد من وجود الموارد الكافية والمهارات والقدرات اللازمة للحفاظ على وظائفها وعملياتها الأساسية، والقدرة على الاستمرار في تقديم الخدمات أثناء الأزمة أو بعدها.

موارد مفيدة

- GISF دليل تدريب إدارة الأزمات للمنظمات غير الحكومية
- GISF إدارة الأزمات الناتجة عن الحوادث الحرجة
- دليل المدافعين في الخطوط الأمامية

مكتب تنسيق الشؤون الإنسانية للأمم المتحدة/ماتيو ميناسي

هايتي

يقوم العاملون في المجال الإنساني بتنسيق استجاباتهم في أعقاب الزلزال. تحتاج المنظمات إلى وضع احتمالية وقوع أزمات كبرى في الاعتبار عند وضع خططها لتحديد كيفية الاستجابة لها ومواصلة أداء وظائفها الطبيعية.

الفقرة 6: رصد وتقييم ومساءلة إدارة المخاطر الأمنية (MEAL) (SRM) والتعلم من

6.1 لماذا يعتبر الرصد والتقييم والمساءلة والتعلم مهمة – المفاهيم الأساسية

إن مفتاح نجاح أي استراتيجية لإدارة المخاطر الأمنية هو إنشاء عمليات لمراقبة وتقييم فعاليتها، وفي نهاية المطاف تأثيرها. يتطلب تنفيذ استراتيجية شاملة لإدارة المخاطر الأمنية (SRM) التقييم المستمر والتكيف. ومن ثم، فإن وجود نظام شامل للرصد والتقييم والمساءلة والتعلم سيساعد على ضمان الجودة والتحسين المستمر في العملية وكفاءتها ومخرجاتها. يسمح نظام الرصد والتقييم والمساءلة والتعلم المتكامل أيضًا للمنظمة بمراقبة مدى نجاح استراتيجية إدارة المخاطر الأمنية في تمكين أو دعم تحقيق الأهداف التنظيمية الأوسع نطاقًا.

التعاريف الرئيسية:

- **نظرية التغيير:** توضيح شامل لكيفية وسبب توقع حدوث التغيير المرغوب في سياق معين. إنها تصور المسارات لتحقيق كل نتيجة. يتم ذلك من خلال تحديد النتائج المرغوبة على المدى الطويل أولاً، ثم العمل على تحديد جميع الشروط (النتائج الفرعية) التي يجب أن تكون متاحة (وكيف ترتبط هذه الشروط ببعضها البعض بشكل سببي) حتى تتحقق النتائج.
- **الإطار المنطقي (Logframe):** الإطار المنطقي هو جدول أو مصفوفة تسرد أنشطة البرنامج، والمخرجات قصيرة المدى، والنتائج متوسطة المدى، والأهداف طويلة المدى. فهو يبين منطق الكيفية التي ستؤدي بها الأنشطة إلى المخرجات، والتي بدورها تؤدي إلى النتائج، وفي نهاية المطاف إلى الهدف. يتضمن المؤشرات التي سيتم استخدامها لقياس التقدم، ومصدر البيانات، والافتراضات اللازمة لنجاح المشروع.
- **خطة الرصد والتقييم والمساءلة والتعلم (MEAL):** وثيقة ملخص توضح كيفية تنفيذ خطط الرصد والتقييم، بما في ذلك قائمة بالعناصر التي يجب قياسها ولماذا، والأنشطة الرئيسية، والميزانيات، والمسؤوليات، والمواعيد النهائية.

يتطلب تحديد كيفية مراقبة وتقييم أنظمة إدارة المخاطر الأمنية (SRM) وتحديد متطلبات التقرير للأشخاص المسؤولين وتفصيل كيفية تبادل الدروس المستفادة خبرة في تقنيات وممارسات المراقبة والتقييم. لذلك، يُوصى بشدة بأن يعمل القادة الاستراتيجيون في إدارة المخاطر الأمنية (SRM) بشكل وثيق مع المتخصصين في الرصد والتقييم والمساءلة والتعلم (MEAL) في منظمتهم لتطوير العملية التي ستعمل بشكل أفضل بالنسبة لهم.

نصيحة هامة: ثمانية أسباب تجعل من الضروري أن تتضمن استراتيجيتك لإدارة المخاطر الأمنية (SRM) خطة للرصد والتقييم والمساءلة والتعلم (MEAL)

1. تمكين أنظمة وسياسات وإجراءات أقوى وأكثر سهولة في الاستخدام.
2. تواكب مدى نجاحك في تحقيق أهدافك الاستراتيجية والنتائج المرغوبة.
3. تضمن إنفاق الأموال والموارد بكفاءة وفعالية.
4. توفر بيانات دقيقة يمكن استخدامها في الاتصالات الخارجية والداخلية، وطلبات التمويل، وإعداد التقارير للمانحين أو مجلس الإدارة.
5. يمكن أن تساهم في تخطيط استمرارية الأعمال وإدارة الأزمات لتحديد مجالات الفجوات أو التهديدات.
6. يمكنك من اتباع نهج ديناميكي وقابل للتكيف في التنفيذ العملي لاستراتيجيات السلامة والأمن.
7. تمنح الموظفين والعملاء وأصحاب المصلحة الرئيسيين صوتًا.
8. تعمل على تحسين الدافع والتركيز لدى الأشخاص الذين ينفذون استراتيجية السلامة والأمن الخاصة بك.

6.2 تطوير خطة الرصد والتقييم والمساءلة والتعلم (MEAL)

ستمكنك خطة الرصد والتقييم والمساءلة والتعلم من التواصل بشأن نهجك وإثبات كيفية تحقيق أهدافك، بما في ذلك من هو المسؤول وما هي التمويلات/الموارد المطلوبة. يساعد ذلك في إظهار المساءلة والتعلم، ويتيح لك في النهاية تعزيز مصداقيتك بينما تعزز فهمًا مشتركًا لأهدافك النهائية. (أنظر المادة 12: مثال لخطة الرصد والتقييم والمسائلة والتعلم).

نصيحة هامة: إنشاء نظرية فعالة للتغيير وخطة رصد وتقييم ومسائلة وتعلم MEAL

- ✓ ابدأ مع وضع النهاية في الاعتبار: حدد أهدافك طويلة المدى.
- ✓ كن محددًا وواقعيًا عند تحديد المؤشرات، وتأكد من أنها SMART (محددة، قابلة للقياس، قابلة للتحقيق، ذات صلة ومحددة زمنياً).
- ✓ قم بتعيين "نقاط مسار" تحدد النتائج قصيرة ومتوسطة وطويلة المدى.
- ✓ اشراك أصحاب المصلحة (أنظر القسم 6.3) لضمان مشاركتهم وتعليقاتهم ومدخلاتهم في العملية - فهم من سيحتاجون إلى إنجاح العملية.
- ✓ ضع أهدافك في سياقها الصحيح. قد تختلف كيفية حدوث التغيير لفريق يعمل في بلد عالي المخاطر مع نظام قمعي ذو حزب واحد، مقارنة بفريق يعمل في بيئة منخفضة المخاطر في ديمقراطية متعددة الأحزاب. تخصيص المؤشرات الخاصة بك وفقًا للسياق الذي يتم استخدامها فيه.
- ✓ مراجعة وتعديل نموذج نظرية التغيير الخاص بك لتعكس الدروس المستفادة بشأن ما ينجح، بالإضافة إلى التغييرات في استراتيجيتك أو بيئة التشغيل الخاصة بك.

6.3 الرصد الروتيني لتقدم إدارة المخاطر الأمنية (SRM)

اختيار مؤشرات إدارة المخاطر الأمنية SRM

يمكن أن تكون المؤشرات كمية، مثل عدد الحوادث الأمنية المبلغ عنها، أو التدريبات الأمنية المقدمة، أو الموظفين المدربين. أو يمكن أن تكون أكثر نوعية، مثل مخاوف الناس، أو ردود أفعالهم، أو تجاربهم. طالما يمكنك التقاط البيانات واستخدامها لتوضيح الرحلة، فإنك تنجح في إظهار التأثير.

يجب أن يكون كل مؤشر:

- مرتبطة بشكل مباشر بالإخراج أو النتيجة أو الهدف المذكور في نظرية التغيير.
- شيء يمكنك قياسه بدقة باستخدام أساليب نوعية أو كمية أو مختلطة، والموارد المتاحة لديك.

اختيار نقاط بيانات SRM

هذه بعض الأمثلة على نقاط بيانات إدارة المخاطر الأمنية المحددة التي يمكن أن تغذي المؤشرات المخصصة التي يمكن استخدامها لتسليط الضوء على التغيير، سواء كان إيجابيا أو سلبيا:

- الحوادث المبلغ عنها.
- المخاوف أو الحوادث الوشيكة المبلغ عنها.
- قياس المشاركة أو استخدام قنوات إعداد التقارير.
- تعليقات السلامة والأمن المأخوذة من تقارير البرنامج.
- تقارير التعليقات من الاستجوابات الفردية ومقابلات الخروج أو النماذج.
- استطلاعات الإدراك التي تقيس الوعي.
- فهم سياسات وإجراءات إدارة المخاطر الأمنية والالتزام بها.
- الحضور للتدريب (الداخلي والخارجي).
- محاضر ووقائع اجتماعات إدارة المخاطر الأمنية أو اجتماعات نقاط الاتصال الأمنية.
- سجلات السفر الدولية.
- مطالبات التأمين.
- الإنفاق الميزاني والفعلي على موارد إدارة المخاطر الاستراتيجية.
- المقارنة بالمعايير الخارجية.
- التدقيق الداخلي المتعلق بـ:
  - استكمال ومراجعة مستندات إدارة المخاطر الأمنية (خطط السلامة والأمن، تقييمات المخاطر، خطط إدارة الحوادث، الإحاطات الأمنية، وإجراءات السلامة والأمن أثناء السفر).
  - فحوصات أو سجلات سلامة وأمن المكتب.
  - فحوصات أو سجلات سلامة السيارة.
  - سجلات حركة الموظفين الوطنيين.

6.4 التقييم

إن القدرة على قياس التغير الاجتماعي والثقافي بطريقة محسوبة وملموسة، يمكن أن تكون أداة أساسية لتوصيل قيمة وفعالية الاستثمار في إدارة المخاطر الأمنية. لا توجد طريقة أو نهج واحد يستخدم لقياس الأثر أو تقييمه أحد الأساليب هو استخدام نموذج نظرية التغيير (ToC)، الذي يرسم الروابط بين مدخلاتك وأنشطتك ومخرجاتك وكيفية تحقيق هذه النتائج والتأثير المطلوب.

نماذج نظرية التغيير الأكثر فعالية هي نماذج بسيطة وتركز على:

- المشكلة التي يسعى إطار عمل إدارة المخاطر الأمنية SRM الخاص بك إلى حلها (على سبيل المثال، نقص الوعي والمشاركة في إدارة المخاطر الأمنية SRM، وزيادة التهديدات التي يتعرض لها الموظفون).
- التأثير الذي تحاول إحداثه (على سبيل المثال، إنشاء بيئة آمنة وسليمة لكل من يعمل لصالح مؤسستك أو نيابة عنها)
- الشروط المطلوبة لتحقيق هذه النتائج (أنظر الأداة 10: مخطط ToC بسيط).

6.5 المسائلة

إن المشاركة التنظيمية هي شرط أساسي لبناء ثقافة إدارة المخاطر الأمنية بنجاح. لذلك، من الضروري إشراك القادة الكبار وأعضاء مجلس الأمناء والزملاء في ما تتعلمه من الرصد والتقييم والمساءلة والتعلم، بالإضافة إلى الشفافية في المساءلة إذا لم يتم تحقيق الأهداف. على سبيل المثال، يمكن أن يضمن تضمين إدارة المخاطر الأمنية كجزء من مؤشرات الأداء الرئيسية لمجلس الإدارة في التقارير الربعية تكامل إدارة المخاطر الأمنية بشكل جيد من خلال ربطها بوضوح بنجاح المنظمة.

يجب أن تكون أنظمة التدقيق والامتثال المناسبة متاحة على جميع مستويات المنظمة مع وجود نتائج واضحة وإجراءات عقابية في حالة عدم الالتزام. يجب أن تُحدد خطوط المسؤولية الواضحة، بالإضافة إلى الإجراءات المحددة للامتثال، داخل الإطار المنطقي لضمان المسؤولية الكاملة.

أمثلة من القطاع:

"كانت منظمتنا تمتلك نظامًا مكتوبًا جيدًا وعملية واضحة لإدارة المخاطر الأمنية، ومع ذلك، لم يتم مراقبتها أو مراجعتها بشكل صحيح أبدًا. "كانت السياسات تُرسل، ولكن لم يكن هناك أي متابعة، أو عواقب إذا لم يتم استكمال تقييم المخاطر أو خطة إدارة الحوادث. لم يكن هناك منتدى أو آلية قائمة لمراجعة تنفيذ السياسة أو المشاركة فيها أو التحقق منها. كان من المفترض فقط أنه بمجرد إرسال سياسة ما، سيكون من المتوقع أن يقوم الموظفون بتنفيذها - مع القليل من الدعم من كبار القادة الاستراتيجيين أو متابعة التقدم أو التأثير."

من مشارك في المقابلات الاستقصائية الرئيسية (KII)، مدير العمليات في إحدى المنظمات غير الحكومية

6.6 التعلم

تُعد استراتيجيات إدارة المخاطر الأمنية الأكثر نجاحاً هي التي تتيح مراجعة دائمة، وتكيفاً مستمراً، وتعديلات منتظمة، مع إتاحة فرص للتفكير الجماعي والتعلم، سواء من خلال أساليب منظمة أو غير رسمية.

رأي الخبراء

نحن لا نجمع البيانات لمجرد الجمع فقط. نحن نجمع فقط البيانات التي سنستخدمها كجزء من مناقشاتنا حول التأمل والمراجعة.

(مشارك في المقابلات الفردية، قائد استراتيجي في منظمة غير حكومية)

من الممارسات الجيدة أن نشارك الدروس المستفادة على كافة المستويات، سواء كانت إيجابية أو سلبية، لأن هذا من شأنه أن يعزز المساءلة والشفافية ويشجع على اتباع نهج أكثر تشاركية.

رأي الخبراء

يجتمع [منسقو الأمن] لدينا بشكل منتظم لمناقشة قضايا الأمن والسلم ذات الاهتمام مع مديريهم في البلدان، الذين يقومون بعد ذلك باستخلاص المعلومات الرئيسية لنشرها على فريق الموظفين الأوسع في جلسات تضم جميع الموظفين

(مشارك في المقابلات المعمقة، مسؤول استراتيجي في إدارة المخاطر الأمنية لمنظمة غير حكومية)

يجب أن تكون عملية التعلم متبادلة في كلا الاتجاهين. يشمل ذلك عملية تغذية استباقية لدعم مشاركة معلومات إدارة المخاطر الأمنية (SRM) من القادة الاستراتيجيين (أي استيعاب التعلم الجديد) إلى بقية المنظمة. كما أنها تتضمن أيضًا عملية تغذية راجعة تشاركية، والتي تستفيد من ما تم تعلمه وتضع إجراءات واضحة بناءً على هذه الدروس.

من خلال دعم التعلم عبر المؤسسة بهذه الطريقة، من الممكن بناء ثقافة إدارة المخاطر الأمنية التي تصبح مجزية ومكتفية ذاتيًا. من خلال هذه العملية، تستطيع المنظمات بناء الانفتاح على التغيير الذي يدعم في نهاية المطاف التجديد الاستراتيجي.

نصيحة هامة: آليات التعلم الجيد

- رسم خريطة لتدفق المعرفة. من لديه حق الوصول إلى أي معلومات؟ من الذي لا يستطيع الوصول إلى المعلومات المفيدة؟ من هم حُرّاس المعرفة؟ كيف يمكنك بسهولة مشاركة تلك المعرفة داخليًا وخارجيًا؟
- أشرك فريق القيادة العليا لديك في هذه العملية. استعرض أصولك وأبرز إمكاناتك غير المستغلة.
- فكر في نقاط القوة في مؤسستك وأبرز المجالات التي تحتاج إلى تحسين.
- تحسين فترات التغيير. يمكن أن تكون التغييرات التنظيمية الكبيرة مرهقة، ولكنها قد توفر أيضًا فرصًا لوضع الأسس لطرق عمل جديدة.
- ابحث عن طرق بسيطة للحصول على المعرفة. تنظيم جلسات مشاركة للفريق وكافة الموظفين، مع مراعاة الجمهور المستهدف لكل معلومة لتعظيم أثرها.
- إنشاء الموارد في أماكن يسهل الوصول إليها وإحالة الأشخاص إليها في كل فرصة.

ويلسدون، ن. معهد أبحاث العمل التطوعي، "اتباع نهج التعلم الاستراتيجي للتقييم"

6.7 طرق جمع البيانات

عند تطوير خطة الرصد والتقييم، تحتاج المنظمة أولاً إلى تحديد ما تريد مراقبته. ينتقل التركيز بعد ذلك إلى اختيار طريقة/طرق جمع البيانات الخاصة بك. هناك مجموعة متنوعة من الأدوات والمنهجيات الكمية والنوعية للاختيار من بينها. يمكن استخدام العديد من هذه الأدوات معًا أو مجتمعة، بناءً على ميزانية مؤسستك وأهدافها ووقتها. على الرغم من تغيّر الأساليب، إلا أن ذلك يتيح لفرق إدارة المخاطر الأمنية فرصة منتظمة وشاملة لمراجعة فعالية استراتيجياتها بشكل مستمر. هذا لا يضمن فقط إنفاق الأموال واستثمار الموارد بشكل مؤثر، بل يتيح أيضًا إجراء التعديلات والتكيفات وتلقي الملاحظات حول النهج الاستراتيجي.

يرد أدناه ملخص لأدوات جمع البيانات النموذجية.

نوع الأداة	المزايا	العيوب
المراقبة الروتينية	يوفر بيانات محدثة ويتيح اتخاذ إجراءات تصحيحية.	
استبيان	يسمح بجمع البيانات من عدد كبير من الأشخاص. مرونة عالية: يمكن إجراء الاستطلاعات عبر الإنترنت أو عن طريق الهاتف أو شخصياً، وجمع كل من الاستجابات الكمية والنوعية.	قد يكون من الصعب تحديد مدى العلاقة السببية بين عنصرين أو أكثر.
مقابلات	تسمح بإجراء مناقشة أكثر عمقًا لموضوع ما. تتيح المقابلات غير المنظمة أو شبه المنظمة الفرصة لتكييف المحادثات مع الاحتياجات والسماح بالمرونة في إجابات المشاركين. مفيد للمواضيع الحساسة.	يمكن أن تكون عرضة لتحيز المُحاور (حيث يمكن لمعتقدات أو مواقف المُحاور أن تشكل إجابات المُستفتى) أو تحيز الرغبة الاجتماعية (حيث يقدم المُستفتى الإجابات التي يعتقد أن المُحاور يريدها). مكلفة من حيث الوقت والموارد. صعوبة إنتاج بيانات قابلة للقياس الكمي.
مجموعات التركيز	مناسب للحصول على فهم أكثر عمقًا لقضية أو منظور ومشاركة الملاحظات والدروس المستفادة.	مستهلكة للوقت في التنفيذ والتحليل. لا يجوز للمشاركين ذوي الشخصيات الأقل سيطرة مشاركة آرائهم.

مستمر

نوع الأداة	المزايا	العيوب
دراسات الحالة	مناسب للحصول على تقدير متعمق لموضوع محدد، مثل مجموعة أو فرد أو برنامج.	من الصعب تعميم الملاحظات أو النتائج. هناك خطر التحيز، حيث من المرجح أن يسعى الباحثون لاستخدام دراسات الحالة التي تؤكد افتراضاتهم بدلاً من تقديم أدلة موضوعية على القضية.
تدفقات وجها لوجه	يسمح بجمع المعلومات في بيئة أكثر طبيعية، مما قد يؤدي إلى الحصول على نتائج أكثر دقة.	يمكن أن تمنع التدقيقات المخططة المشاركين من التصرف بشكل طبيعي. تفشل الدراسات الرصدية السرية في إتاحة الفرصة للمشاركين للموافقة على المشاركة.
سجلات الأمان/ قاعدة بيانات الحوادث	يتتبع المخاوف المتعلقة بالسلامة والأمن، وحالات القرب، والحوادث بطريقة موحدة، مما يجعله مناسبًا للغاية لأغراض الإبلاغ الرسمية.	يجب أن يكون من السهل الوصول إليه لجميع الموظفين. يتطلب ثقافة إعداد تقارير جيدة - حيث يُنظر إلى التقارير بشكل إيجابي.
مؤشرات الأداء الرئيسية/ الأساسية (KPIs/ CPIs)	يمكن أن تكون نوعية أو كمية. التركيز على أهداف/مجالات محددة للمنظمة. يعزز المساءلة.	ينبغي دمجه مع أساليب أخرى حتى لا يُنظر إليه على أنه آلية عقابية بحتة.
التدقيق السنوي (داخلي أو من طرف ثالث)	يوفر تحليلًا شاملاً للمعرفة والسلوك والممارسة المتعلقة بإدارة المخاطر الأمنية (SRM) في سياق معين، ويمكنه تقييم العمليات مقابل المعايير التشغيلية الدنيا للأمن.	يمكن أن يكون مكلفًا ويتطلب موارد إضافية.

موارد مفيدة

- تحليل القدرات التشاركية ونقاط الضعف لدى منظمة أوكسفام: دليل الممارس
- البنك الدولي: المراقبة والتقييم؛ بعض الأدوات والأساليب والنهج
- معهد التنمية الخارجية: دعم الإدارة التكيفية
- INTRAC: المراقبة والتقييم العالمية
- بوند المملكة المتحدة: اختيار طرق التقييم المناسبة

منظمة العفو الدولية

اوكرانيا

يقوم محقق الأسلحة في منظمة العفو الدولية بإجراء تحقيق ميداني. بما أن السلامة والأمن هما من مجالات العمل الوقائية، فقد يكون من الصعب قياس النجاح. لذلك، من المهم بشكل خاص أن يكون لدينا خطة قوية للرصد والتقييم والمسائلة والتعلم

أداة إدارة المخاطر الأمنية (SRM)

الأداة 1
تطوير الاتجاهات الاستراتيجية الخاصة بك - مثال

التوجه الاستراتيجي 1: النهج التنظيمي لإدارة المخاطر الأمنية				
المخارج: جميع أصحاب المصلحة على دراية بالنهج التنظيمي للمخاطر وأين تكمن حدود المخاطر.				
الرقم	**الهدف**	**من المسؤول**	**التاريخ المستهدف**	**مقياس النجاح**
1.1	تحديد موقف المخاطرة والحدود	الفرق التنفيذية	25 فبراير	* تم تطوير بيان موقف المخاطرة وتم توزيعه على جميع الموظفين. * تم إكمال مصفوفة عتبة المخاطر وإبلاغها إلى جميع القادة الاستراتيجيين.
1.2	تأكيد نهج استراتيجية إدارة المخاطر الأمنية	مدير إدارة المخاطر الأمنية العالمية ولجنة إدارة المخاطر	26 ديسمبر	* تحليل سياقي لجميع العمليات والأنشطة التي تم إنجازها في الدولة. * تتفق فرق البرنامج وإدارة المخاطر الأمنية على نهج القبول والحماية والردع في كل سياق/برنامج تشغيلي. *المناهج المتضمنة في التدريب الداخلي.
التوجه الاستراتيجي 2: رفع الوعي				
المخارج: يتم توعية جميع أصحاب المصلحة وقبولهم لأدوارهم ومسؤولياتهم في الحد من المخاطر التي تهدد الأشخاص والمعلومات والأصول المادية.				
الرقم	**الهدف**	**من المسؤول**	**التاريخ المستهدف**	**مقياس النجاح**
2.1	تعزيز فهم إدارة المخاطر الأمنية على المستويات الاستراتيجية والتشغيلية والوظيفية من خلال برنامج توعية داخلي منظم.	قسم إدارة المخاطر الأمنية	26 ديسمبر	* تم تطوير برنامج التوعية الداخلية لإدارة المخاطر الأمنية وتم توزيعه على جميع الموظفين. * مراجعة كل ستة أشهر لممارسات إدارة المخاطر التي يتبعها أصحاب المصلحة المختلفون (على سبيل المثال الإبلاغ عن الحوادث، وتطوير تقييمات المخاطر/أدوات إدارة المخاطر).

2.2	توفير التدريب على السلامة والأمن الداخلي والخارجي (حسب مصفوفة التدريب).	مدير إدارة المخاطر الأمنية العالمية ولجنة إدارة المخاطر	26 ديسمبر	* المراجعة السنوية لمستوى المشاركة في التدريب على السلامة والأمن. * مراجعة ربع سنوية لمستوى الرضا عن التدريب المقدم.
2.3	هيكل الحوكمة المعمول به فيما يتعلق بإدارة المخاطر الأمنية.	الفرق التنفيذية	25 فبراير	*الاتفاق على هيكل حوكمة واضح وتوزيع الأدوار والمسؤوليات على كل مستوى. * تأكيد عملية توظيف الموظفين. * إبلاغ هيكل الحوكمة إلى جميع الموظفين.

التوجه الاستراتيجي 3: التركيز الثقافي على السلامة والأمن

المخارج: إن ثقافة المنظمة ونهجها في التعامل مع البرامج وتحقيق الأهداف التنظيمية مدعومة بوعي جيد بالسلامة والأمن. تشكل إدارة المخاطر الأمنية جزءًا أساسيًا من عملية التخطيط.

الرقم	الهدف	من المسؤول	التاريخ المستهدف	مقياس النجاح
3.1	تم تضمين إدارة المخاطر الأمنية في مراحل التخطيط للأنشطة التشغيلية.	قسم إدارة المخاطر الأمنية	26 ديسمبر	* تظهر إدارة المخاطر الأمنية بانتظام في بنود جدول الأعمال والمحاضر. * تتضمن عمليات التخطيط مشاركة/تسجيل الخروج من إدارة المخاطر الأمنية (SRM).
3.2	تحديد 10 "قواعد ذهبية" يفهمها جميع الموظفين جيدًا.	مدير إدارة المخاطر الأمنية العالمية ولجنة إدارة المخاطر	26 ديسمبر	* التدقيق الداخلي للتأكد من وعي الموظفين بالقواعد الذهبية – 80٪ حد أدنى من الوعي. * القواعد الذهبية معروضة بشكل واضح على الموقع الإلكتروني، والمكاتب الداخلية، ومكاتب الموظفين الوطنية.
3.3	تشكيل لجنة إدارة المخاطر وتفعيلها.	COO	25 فبراير	* تأكيد أعضاء المجموعة من جميع الوظائف. * عقد اجتماعات ربع سنوية، وتدوين محاضرها ومشاركتها مع فريق القيادة التنفيذية.

التوجه الاستراتيجي 4: إعداد التقارير والتفكير والمراجعة				
المخارج: يتم توعية جميع أصحاب المصلحة بضرورة الإبلاغ عن المخاوف والحوادث التي كادت تقع، وهم على ثقة من أن كبار القادة سوف يراجعونها ويتخذون الإجراءات اللازمة بشأنها بانتظام.				
الرقم	**الهدف**	**من المسؤول**	**التاريخ المستهدف**	**مقياس النجاح**
4.1	تطوير آلية تغذية راجعة لإدارة المخاطر الأمنية للإبلاغ عن الحوادث، والاقتراب من الحوادث، والمخاوف.	مدير إدارة المخاطر الأمنية العالمية ولجنة إدارة المخاطر	26 ديسمبر	تم تطوير آليات التغذية الراجعة واستخدامها بانتظام من قبل جميع الموظفين. * يتم تحديث سجل جميع الحوادث والحوادث الوشيكة والمخاوف بانتظام.
4.2	مراجعة الحوادث والحوادث الوشيكة والمخاوف والتفكير فيها.	مدير إدارة المخاطر الأمنية العالمية ولجنة إدارة المخاطر	26 ديسمبر	* تسجيل الإجراءات مع تحديد أصحاب الإجراءات بشكل واضح وتقارير التقدم في مكانها. * استكمال المراجعة نصف الشهرية للحوادث الخطيرة وتحليل الاتجاهات ومشاركتها مع القادة التنفيذيين.
التوجه الاستراتيجي 5: أفضل الممارسات				
المخارج: المنظمة محدثة وتتبع إرشادات أفضل الممارسات وتشارك وتتعاون مع الآخرين في هذا القطاع.				
الرقم	**الهدف**	**من المسؤول**	**التاريخ المستهدف**	**مقياس النجاح**
5.1	التفاعل والتواصل والتعاون داخل القطاعات وفيما بينها.	مدير إدارة المخاطر الأمنية العالمية ولجنة/ مجموعة العمل لإدارة المخاطر	25 ديسمبر	* العضوية في المنتديات والمجموعات ذات الصلة بإدارة المخاطر الأمنية ضمن القطاع، مثل GISF. * إقامة علاقات مع متخصصي إدارة المخاطر الأمنية خارج القطاع. تسجيلات دخول ربع سنوية/نصف سنوية، يتم تسجيلها ومشاركتها مع لجنة المخاطر.
5.2	مراجعة معايير منتظمة.	مدير إدارة المخاطر الأمنية العالمية ولجنة إدارة المخاطر	25 ديسمبر	* المراجعة الخارجية لممارسات واجب الرعاية المتعلقة بمعايير المنظمة الدولية للمعايير والتي أجريت باستخدام مزود خارجي. * إجراء مراجعة داخلية للمعايير المرجعية لأفضل الممارسات كل 18 شهرًا. * مشاركة نتائج عمليات التدقيق/المراجعات مع القيادة التنفيذية وإبلاغها إلى عدد أكبر من الموظفين مع نقاط عمل المتابعة.

مقتبس من نموذج بقلم درابر، ر. (2014)، كيفية كتابة خطة أمنية استراتيجية
https://www.linkedin.com/pulse/how-write-strategic-security-rick-draper/

الأداة 2
كيفية ترشيد استراتيجية إدارة المخاطر الأمنية الخاصة بك

الرؤية	حدد رؤيتك. حدد إطارًا زمنيًا محددًا عمليًا للمنظمة واسأل نفسك: أين تود أن ترى إدارة المخاطر الأمنية داخل مؤسستك بعد خمس سنوات؟ من هو جمهورك المستهدف؟ كيف تريد أن يرى الآخرون إدارة المخاطر الأمنية SRM؟ كيف ستحقق هدفك؟ **تذكر:** • استخدم لغة بسيطة يمكن أن يفهمها الأشخاص من جميع الخلفيات. • يجب أن تكون رؤيتك جذابة وملهمة لإشراك الناس. • لديها سياق واسع. • ينبغي أن تكتب في زمن الحاضر.
القياسات/تحليل البيانات	لإثبات بيان الرؤية، من المهم أن تكون هناك مبررات. يمكن أن تتضمن هذه الأرقام والمقاييس التي ستحدد في النهاية ما إذا كانت استراتيجية إدارة المخاطر الأمنية قد حققت تأثيرًا، كما هو مخطط له (أنظر الفقرة 6). **ينبغي لقادة إدارة المخاطر الأمنية أن يسألوا أنفسهم:** • ما هو اسم المقياس وماذا سيعرض عن المنظمة؟ • ما نوع البيانات التي يجب إنتاجها من المقياس وأين يمكن العثور على البيانات؟ • ما هو نوع الرسم البياني أو المرئي الذي سيعرض البيانات بشكل أفضل؟ • ما هي طرق تفسير القياس؟
تحليل نقاط القوة والضعف والفرص والتهديدات	SWOT تعني نقاط القوة والضعف والفرص والتهديدات. تحليل SWOT هو أداة تخطيط فعالة أخرى، حيث يقترح الأعضاء ويقومون بإدراج وتقييم نقاط القوة والضعف والفرص والتهديدات لمنظمتهم. إن إجراء تحليل SWOT يعد أداة فعالة للغاية لتقييم وتحليل الحالة الحالية لإدارة المخاطر الأمنية داخل مؤسستك. قد يكون من المفيد استخدام تحليل SWOT لمراجعة نهجك تجاه إدارة المخاطر الأمنية إلى جانب استراتيجية المنظمة بأكملها لمعرفة نقاط القوة والضعف والفرص والتهديدات التي قد تطرأ على مواءمة استراتيجية إدارة المخاطر الأمنية. (أنظر الأداة 4، نموذج تحليل SWOT).
تحليل PESTLE	يستخدم هذا التحليل لتحديد التهديدات ونقاط الضعف أثناء إجراء تحليل SWOT. الخطوة الأولى أثناء إجراء تحليل PESTLE هي فهم جميع العوامل الخارجية التي قد تؤثر على عمل منظمتك. في التحليل يتم تقييم العوامل التالية: سياسية، اقتصادية، اجتماعية، تكنولوجية، قانونية، بيئية.

مخططات التقارب والترابط	نتيجة لتحليل SWOT، غالبا ما يكون هناك العديد من المشاريع الداخلية والاستراتيجية التي قد يكون من الضروري القيام بها. يُعد مخطط التقارب مفيدًا لتضييق نطاق عدد كبير من العناصر إلى فئات أكثر تنظيمًا وتشابهًا لجعلها أكثر قابلية للإدارة. يتم إنشاء مخطط التقارب من خلال جعل فريق القيادة يكتب جميع المبادرات أو المشاريع المحتملة التي تم تحديدها من خلال تحليل نقاط القوة والضعف والفرص والتهديدات على ملاحظات لاصقة. يجب على الفريق بعد ذلك تصنيف هذه الملاحظات ضمن مواضيع محددة، قبل تخصيص المشاريع لوظيفة أو وظائف محددة. يساعد هذا في تبسيط وتحديد الروابط بين الوظائف، بالإضافة إلى تعيين مالكي الإجراءات بطريقة منطقية.
تحليل المحفظة	تحديد الاستراتيجيات المختلفة التي تم استخدامها لتحقيق أهداف إدارة المخاطر الأمنية في الماضي. ثم تصنفها إلى "نجوم" (حيث كانت التنفيذات ناجحة للغاية)، و"أساس" (حيث تشكل قاعدة لإطلاق أهداف إدارة المخاطر الأمنية)، و"علامة استفهام" (استراتيجيات جديدة/غير مجربة) و"أوز ميتة" (استراتيجيات تم تجربتها وفشلت). يمكن أن يساعد هذا في التركيز على الأساليب التي تحتاج إلى التركيز عليها وتلك التي يجب إلغاؤها أو مراجعتها.

الأداة 3
نموذج تخطيط إدارة المخاطر الأمنية).

الغرض التوجيهي	لماذا نقوم بتنفيذ إدارة المخاطر الأمنية SRM؟ ما الذي نهدف إلى تحقيقه؟ ما هي الفوائد التي نأمل أن نراها؟
العناصر الأكثر أهمية في عملية إدارة المخاطر الأمنية بالنسبة لمنظمتنا	ما هي عناصر إطار إدارة المخاطر الأمنية الأكثر أهمية لتحقيق أهدافنا؟
النهج المتبع في تكييف مبادئ إدارة المخاطر الأمنية مع ثقافتنا واحتياجاتنا التنظيمية	كيف يمكننا دمج إدارة المخاطر الأمنية في عملياتنا الحالية بشكل أكثر فعالية؟ هل سنشكل مجلسًا جديدًا للمخاطر أم سنستخدم منتدى موجودًا لمناقشة المخاطر؟ كيف سنقوم بتدريب أصحاب المخاطر؟ كيف سنقوم بتضمين إدارة المخاطر الأمنية في الميزانية والتخطيط الاستراتيجي؟ كيف سنتعامل مع مجلس إدارتنا؟
خطة لزيادة قيمة إدارة المخاطر الأمنية بشكل تدريجي لمنظمتنا	كيف ومتى سنقوم بتوسيع نطاق إدارة المخاطر الأمنية لزيادة القيمة التي تقدمها لمنظمتنا؟

الأداة 4
نموذج تحليل نقاط القوة والضعف والفرص والتهديدات

نقاط القوة	نقاط الضعف
ما الذي نقوم به بشكل جيد ضمن إطار/نهج إدارة المخاطر الأمنية الحالي لدينا؟ ما هي الموارد أو القدرات الداخلية التي نمتلكها/التي يمكننا الاستفادة منها؟ على سبيل المثال، وجود ثقافة جيدة حول إدارة المخاطر الأمنية، وموظفين ذوي خبرة في إدارة المخاطر الأمنية، وأدوات قوية لتقييم المخاطر، وبرنامج قوي للتعلم والتطوير.	ما هي مجالات إطار إدارة المخاطر الأمنية الحالي لدينا والتي تحتاج إلى تحسين؟ ما هي الموارد أو التدريب الذي نفتقر إليه؟ على سبيل المثال، التدريب غير الكافي على إدارة الأزمات، والافتقار إلى الفهم والمشاركة في إدارة الأزمات، والتكنولوجيا القديمة، والبنية التحتية الضعيفة.
الفرص	**التهديدات**
ما هي الفرص المتاحة التي يمكن لإدارة المخاطر الأمنية SRM استغلالها أو الاستفادة منها؟ هل هناك أماكن حيث يمكن أن تساعد إدارة المخاطر الأمنية في تحقيق أهداف المنظمة بأكملها/تلبية الأهداف الاستراتيجية؟ على سبيل المثال، التقنيات الناشئة والشراكات الجديدة وفرص التواصل.	ما الذي قد يهدد فعاليتنا في تنفيذ إدارة المخاطر الأمنية في جميع مناحي المنظمة؟ على سبيل المثال، الاحتفاظ بالموظفين، وانتهاكات الأمن السيبراني، ومجالات العمل في السياقات عالية المخاطر، وإرهاق الموظفين.

الأداة 5
مثال على بيانات موقف المخاطر

المثال 1

في السعي لتحقيق ..... ‘الأهداف الاستراتيجية *[تحديد]* .....
.....، من المحتم أن الأنشطة التشغيلية *[تضمين أمثلة]* .....
..... أن تعرض فريق العمل لبعض التهديدات. تسعى المنظمة إلى تقليل مستوى المخاطر المرتبطة بهذه التهديدات من خلال إدارة المخاطر الأمنية القوية.

سيتم اعتبار المخاطر مفرطة عندما يكون احتمال وقوع حادث خطير أكثر احتمالا من الإمكان، مع الأخذ في الاعتبار تدابير التخفيف من المخاطر المطبقة.

الحادث الخطير هو الحادث الذي من شأنه أن يسبب ما يلي:

- أحد أعضاء الفريق أو الموظفين المرتبطين به الذين يعانون من أذى جسدي أو نفسي خطير؛ أو
- تعرض مالية المنظمة أو سمعتها لأضرار جسيمة.

..... تعمل في بعض البيئات الأكثر صعوبة والنائية. عندما تكون الاحتياجات البرمجية عالية، ..... قد يتم قبول مستوى أعلى من المخاطر. وفي مثل هذه الحالات، يصبح التركيز بشكل أكبر على إدارة المخاطر الأمنية أمرا ضروريا.

.....'إن موقف المنظمة من المخاطرة سوف يأخذ دائمًا في الاعتبار أهداف البرنامج، وأهمية ما يجب تحقيقه، والقدرة على إدارة التهديدات، فضلاً عن تأثير العوامل الاستراتيجية الأخرى (مثل العلاقات الرئيسية ومصالح الجهات المانحة). سوف يقرر أصحاب المخاطر على أساس كل حالة على حدة ما إذا كانت أهداف البرنامج المحددة والنتائج المقصودة تبرر قبول مستوى المخاطر المقدر.

المثال 2

..... تدرك أن المنظمة تعمل في بيئات حيث لا يمكن القضاء على المخاطر بشكل كامل. ومع ذلك، لا بد من اتخاذ كافة التدابير العملية لخفض مستويات المخاطر قدر الإمكان.

يعتبر المستوى المتبقي من المخاطر الذي يظل قائما بعد اتخاذ مثل هذه التدابير مقبولا فقط إذا كان مبررا بالتأثير الإنساني للعملية.

عندما يتم القضاء على المخاطر غير الضرورية، ويُعتبر النشاط يستحق المتابعة، يجب أن يكون أعضاء الموظفين مستعدين لقبول مستوى المخاطر المتبقية.

أمثلة مقدمة من طرف سلامة المواقع الدولية

الأداة 6
إنشاء نهج تنظيمي لإدارة المخاطر

تحمل المخاطر

تحمل المخاطر هو المستويات المقبولة من التباين في موقف المنظمة من المخاطر بناءً على ظروف محددة. (إنظر القسم 1.5). يقع هذا ضمن عتبة المخاطر التنظيمية (أي مقدار المخاطرة التي يمكن للمنظمة أن تتحملها بالفعل قبل أن تتأثر قدرتها على تحقيق مهمتها بشكل خطير).

تحديد نهجك في التعامل مع المخاطر:

- وضع معايير واضحة للفرق للعمل ضمنها.
- السماح بالمعالجة المنهجية للمخاطر.
- الحماية من الانهيار التنظيمي.

العملية:

1. **تعريف السياق:** قدم شرحًا موجزًا عن كيفية ارتباط مخاطر إدارة المخاطر الأمنية (SRM) بالاستراتيجية العامة للمنظمة وكيف يمكن أن تؤثر عليها، استنادًا إلى مهمتها وأهدافها وغاياتها والسياق التشغيلي. هل هناك أي عوامل خارجية يجب أخذها بعين الاعتبار؟
2. **تحديد الحدود:** حدد بوضوح ما هي المواقف التي لا تقبل المخاطر على الإطلاق، وما هي المواقف التي تتطلب الحذر، ولماذا يمكن أن يكون هناك في بعض الظروف مستوى أعلى من تقبل المخاطر (مثل متطلبات المانحين أو المواقع ذات المخاطر العالية).
3. **تعيين المؤشرات:** حدد مؤشرات المخاطر الرئيسية التي ستُستخدم لتقييم ما إذا كانت المنظمة تعمل ضمن حدود المخاطر، أو بجوارها منها، أو خارجها. ستساعد هذه المؤشرات أيضًا في تحديد مسار العمل المتعلق بإدارة المخاطر المختلفة.

لتتأكد من أن موقفك من المخاطرة متناسب، استخدم سجل المخاطر التنظيمية الخاص بك لإبلاغك بالتهديدات الرئيسية التي تواجهك. يمكن القيام بذلك لكل وظيفة في المنظمة. تقييم تأثير واحتمالية حدوث هذه التهديدات. يمكنك استخدام التعريفات المعمول بها أو إنشاء تعريفاتك الخاصة. يظهر أدناه مثال على ذلك.

الاحتمالية

النتيجة	الأجل	التعريف
1	منخفض جدا	من غير المرجح جدًا أن يحدث التهديد.
2	منخفض	من غير المرجح أن يحدث التهديد.
3	متوسط	التهديد ممكن.
4	عالي	من المرجح أن يحدث التهديد.
5	عالي جدا	من المرجح جدًا أن يحدث التهديد.

التأثير

النتيجة	الأجل	التعريف
1	منخفض جدا	إصابات أو آثار صحية غير مهمة، خسارة مالية غير مهمة (<1000 جنيه إسترليني)، انقطاع غير مهم في الأعمال (لا يوجد أيام عمل ضائعة)، لا يوجد تعرض سلبي للسمعة، تأثيرات قابلة للعكس تمامًا.
2	منخفض	إصابات أو آثار صحية طفيفة، خسارة مالية ضئيلة (<5000 جنيه إسترليني)، انقطاع الأعمال ضئيل (<1 يوم عمل ضائع)، تعرض سمعة سلبية ضئيل، تأثيرات قابلة للعكس في الغالب.
3	متوسط	إصابات أو آثار صحية متوسطة، خسارة مالية متوسطة (<10000 جنيه إسترليني)، انقطاع متوسط في الأعمال (1-2 يوم عمل ضائع)، تعرض سلبي متوسط للسمعة، الحاجة إلى مساعدة خارجية لاحتواء المخاطر، تأثيرات قابلة للعكس جزئيًا.
4	عالي	العجز الدائم أو الاستشفاء المتعدد، والآثار الصحية الكبرى، والخسارة المالية الكبرى (10000-50000 جنيه إسترليني)، وانقطاع الأعمال الكبرى (3-6 أيام عمل ضائعة)، والتعرض لسمعة سلبية كبيرة، والمساعدة الخارجية المطلوبة لاحتواء المخاطر، وبعض التأثيرات القابلة للعكس.
5	عالي جدا	الوفيات، والإعاقات الدائمة المتعددة أو الاستشفاء، والخسائر المالية الكبيرة (<50،000 جنيه إسترليني)، وانقطاع الأعمال بشكل كبير (>6 أيام عمل ضائعة)، والتعرضات السلبية الكبرى للسمعة، والمساعدة الخارجية المطلوبة لاحتواء المخاطر، والتأثيرات الكبيرة.

ارسم هذه العناصر على مصفوفة المخاطر وراقبها باستمرار:

		تأثير التهديدات				
		منخفض جدا	منخفض	متوسط	عالي	عالي جدا
احتمالية التهديد	منخفض جدا	1	2	3	4	5
	منخفض	2	4	6	8	10
	متوسط	3	6	9	12	15
	عالي	4	8	12	16	20
	عالي جدا	5	10	15	20	25

تعتبر المساحات الخضراء ضمن المخاطر التنظيمية. يمكن إدارتها ضمن الآليات الطبيعية.

تقع المناطق الكهرمانية في أعلى مستويات موقف المخاطرة التنظيمية ولكنها ضمن حدود تحمل المخاطر. ينبغي الإبلاغ عن هذه الأمور من أجل الوعي بها، وقد تكون هناك حاجة إلى خطط للمراجعة/الطوارئ.

المناطق الحمراء هي مناطق تقع خارج حدود المخاطر التنظيمية. ينبغي الإبلاغ عن هذه المخالفات، مع ضرورة اتخاذ إجراءات فورية لتحسين الضوابط.

المصدر: سلامة المواقع الدولية

الأداة 7
مثال على الشروط المرجعية للجنة إدارة المخاطر

الغرض من الاجتماع

تعمل لجنة إدارة المخاطر على ضمان قيام المنظمة غير الحكومية بتحديد المخاطر التي تهدد موظفيها وإدارتها بشكل استباقي. وهي تضمن أن تعمل المنظمة غير الحكومية بشكل مستمر على الحفاظ على موقف المنظمة الأمني وتحسينه، ومعالجة المشكلات والمخاطر التي تم تحديدها عند الضرورة.

تشمل مسؤوليات وواجبات المجموعة ما يلي:

- ملكية إطار عمل واستراتيجيات إدارة المخاطر الأمنية.
- الموافقة على جميع طلبات الرحلات ذات مستوى التهديد العالي والعالي جدًا.
- إجراء المراجعات بعد وقوع الحادث والأزمات.
- إدارة الامتثال لإطار إدارة المخاطر الأمنية.
- الاتفاق على أنشطة وأولويات إدارة المخاطر الأمنية.
- ضمان إدارة المخاطر الأمنية المناسبة وتمويل الأزمات.
- الموافقة على الاتصالات الأمنية والرسائل الموجهة إلى الموظفين.

توفر المجموعة لجميع الوظائف الفرصة لإثارة المشكلات من داخل فرقهم. وهي تضمن أن الحلول للمخاطر التي تم تحديدها تشمل احتياجات المنظمة.

الحضور

الدور	دور اللجنة
	رئيس / عضو اللجنة
	نائب الرئيس / عضو اللجنة
	عضو اللجنة
	عضو اللجنة
	عضو اللجنة

الجدولة

أ. سيتم جدولة اجتماع اللجنة الإدارية العليا كاجتماع شهري.

ب. يجوز لرئيس اللجنة أو لأي عضو من أعضائها ترتيب اجتماع طارئ إذا استدعت الظروف عقد مثل هذا الاجتماع.

ج. سيتم تأكيد مكان الاجتماع من قبل الرئيس على أساس كل حدث.

د. مدة الاجتماع محددة في 90 دقيقة.

المذكرة

عنصر	ورقة مرجعية	مقدمة من طرف	الإجراءات
المذكرة		الرئيس	
الحوادث منذ آخر RMC	تقارير الحوادث / تقرير الدروس المستفادة	رئيس / عضو اللجنة	تحديث قاعدة بيانات الحوادث العالمية و/ أو سجل المخاطر إذا لزم الأمر
تحديث حول الإجراءات المتخذة من الاجتماع الأخير للجنة إدارة المخاطر الأمنية.	محاضر الاجتماع	رئيس / عضو اللجنة	
الإنجازات أو القضايا أو المخاطر الرئيسية في إدارة المخاطر الأمنية		رئيس / عضو اللجنة	
مراجعة نماذج الرحلات عالية الخطورة (إذا لزم الأمر)		عضو اللجنة	
الاجتماع اللاحق		الرئيس	
أي أعمال أخرى		الرئيس	

الأجل

أ. يقدم الرئيس تقاريره إلى الرئيس التنفيذي / مجلس الإدارة عند الضرورة.

ب. كل عضو في اللجنة يحمل صوتًا.

ج. يجب حضور ثلاثة أعضاء على الأقل من اللجنة حتى يكتمل النصاب القانوني للاجتماع.

د. الحضور الشخصي ليس إلزاميا ولكن يفضل. الحضور عن طريق مؤتمر الفيديو أو الصوت مقبول.

ه. في حالة غياب أعضاء اللجنة، يجوز للنواب المخولين الحضور.

و. سيتم السماح للحاضرين بتقديم توصيات ضمن سياق وحدود مجالات معرفتهم.

ز. في حالة غياب كل من الرئيس ونائب الرئيس، يجب إعادة جدولة الاجتماع.

ح. سيتم اتخاذ القرارات بالإجماع بين أعضاء اللجنة وسيتم تسجيلها.

ط. ويجوز للأطراف المدعوة تقديم عرض إلى اللجنة إذا تم اتخاذ مثل هذا القرار في اجتماع سابق.

المسؤوليات والصلاحياتتوفير منتدى سري لتحديد القضايا/المخاطر التي تهدد المنظمة أو الإجراءات الإدارية التي قد تؤثر على أمن المنظمة.

أ. التأكد من أن مجموعة العمل هي مجموعة عمل وتظهر تحسنًا مستمرًا في السلامة والأمن.

ب. التحكم في إطار عمل إدارة المخاطر الأمنية في المنظمة واستراتيجياتها، بما في ذلك التوقيع على البروتوكولات والأدوات.

ج. الموافقة على جميع طلبات الرحلات ذات مستوى التهديد العالي والعالي جدًا.

د. إجراء المراجعات بعد وقوع الحادث والأزمات.

ه. إدارة الامتثال لإطار إدارة المخاطر الأمنية.

و. الاتفاق على أنشطة وأولويات إدارة المخاطر الأمنية.

ز. ضمان إدارة المخاطر الأمنية المناسبة وتمويل الأزمات.

ح. الموافقة على الاتصالات الأمنية والرسائل الموجهة إلى الموظفين.

ط. عندما قد تؤدي المخاطر الرقمية والقانونية إلى تفاقم التهديد الذي يتعرض له الموظفون أو الأشخاص الخاضعون لتعليمات المنظمة، فيجب أخذ ذلك في الاعتبار في استراتيجيات إدارة المخاطر وتدابير الحد من المخاطر.

ي. مراجعة وإقرار التغييرات على الشروط المرجعية لإطار إدارة المخاطر الأمنية.

أمثلة مقدمة من طرف سلامة المواقع الدولية

مكتب تنسيق الشؤون الإنسانية/جويل أوبولنسيا

سويسرا

ينبغي للجنة إدارة المخاطر أن تهدف إلى الاجتماع مرة واحدة شهريًا.

الأداة 8
نموذج خطة التعلم والتطوير

الهدف التنظيمي	المعرفة والمهارات المطلوبة	من سيشارك؟

مقتبس من NCVO، مهارات القطاع الثالث؛ تحليل احتياجات التدريب

	أنشطة/طرق التعلم والتطوير	كيف سيتم تقييم ذلك؟	التكلفة	التاريخ

الأداة 9
مثال على مصفوفة التدريب الاستراتيجي

يمكن تعديل هذه الأداة أو توسيعها على المستوى التشغيلي لتعكس احتياجات الموظفين المحددة/ تاريخ الانتهاء/مستوى المهارة في كل مجال.

الوصف	اسم المزود (داخلي/خارجي)
إطار الأمن	
إنشاء الإجراءات (على سبيل المثال، خطط الأمن والسلامة القطرية، والمخاطر القطرية، والسجلات، وخطط إدارة الحوادث)	
تقييم المخاطر	
التدريب على الأمن الشخصي الميداني / التوعية الأمنية	
التدريب على السلامة والأمن أثناء السفر	
ورشة عمل إدارة الأزمات	
الاسعافات الاولية	
المرونة وإدارة الإجهاد	
دورة تدريبية في إدارة المخاطر الأمنية	
أهمية واجب الرعاية	
الإبلاغ عن الحوادث الأمنية	
الأمن السيبراني	
التدريب على النزاهة ومكافحة الفساد	
التدريب على مكافحة الرشوة والفساد	
المراقبة	

- الأولوية
- خلال 12 شهرا
- غير مطلوب

أمثلة مقدمة من طرف سلامة المواقع الدولية

	القادة الاستراتيجيون	المديرين الإقليميين	المدراء القطريون	نقاط محورية للأمن	كل الموظفين

الأداة 10
نموذج نظرية التغيير

الوضع: ما هو سياق أو سبب هذا التغيير؟

الأهداف: كيف سيبدو "النجاح"؟

المدخلات والأنشطة	المخارج	آلية التغيير	المخارج	التأثير
مدخلات ما هي النفقات المالية والموظفين والموارد الأخرى المطلوبة؟	ما هي النتائج الملموسة أو المنتجات أو الدروس أو عمليات التفتيش أو التحسينات التي سيتم إنتاجها؟	ما هي الإجراءات اللازمة لتحقيق التغيير (التغييرات)؟ هل تقوم بإزالة الاحتكاكات وتغيير السلوك وما إلى ذلك؟	**على المدى القصير** ما هي الفوائد والنتائج الأوسع نطاقا، سواء المتقدمة أو المتأخرة؟	ما هي التأثيرات وكيف تتناسب مع أولويات الوزارات والحكومات؟
الأنشطة ما الذي سيتم تقديمه، مثل التدريب أو التوجيه؟			**على المدى البعيد** ما هي التغييرات المستدامة والدائمة، وما هي المقاييس التي سيتم استخدامها لقياس هذه التغييرات؟	

تقييم الأدلة: ما هي قوة قاعدة الأدلة الحالية لهذا التغيير؟

الافتراضات: ما هو المفترض كجزء من الخطة؟

العواقب غير المقصودة المحتملة: هل هناك أي نتائج أخرى يمكن أن تنتج عن هذا المشروع؟

مقتبس من مثال قدمته وزارة الخارجية وشؤون الكومنولث والتنمية في المملكة المتحدة

الأداة 11
نموذج الإطار المنطقي

	ملخص المشروع	المؤشر كيف يتم احتسابه؟	مصدر البيانات كيف يتم قياسها؟	المخاطر/الافتراضات
الهدف				
المخارج				
المخارج				
النشاط				

المصدر: Tools4Dev

الأداة 12
نموذج تخطيط الرصد والتقييم والمسائلة والتعلم

المؤشر	أنشطة رصد وتقييم ومسائلة وتعلم مخصصة	من هو المنخرطون فيها	من المسؤول	أهم المعالم
الثقافة التنظيمية فيما يتعلق بالمشاركة في إدارة المخاطر الأمنية وفهمها	استطلاع الرأي عبر الإنترنت المرسل إلى جميع الموظفين	اتصالات تكنولوجيا المعلومات، الموارد البشرية، إدارة المخاطر الأمنية	الاتصالات وإدارة المخاطر الأمنية	**Q1** تم الانتهاء من النظام عبر الإنترنت **Q2** الاستبيان جاهز **Q3** نتائج الاستبيان
المشاركة مع إعداد التقارير آلية إدارة المخاطر الأمنية	سجل الحوادث/الحوادث الوشيكة/ المخاوف (الوصول عبر تطبيق الهاتف المحمول) مع الإجراءات والمالكين المرتبطين	الموارد البشرية، إدارة المخاطر الأمنية، تكتولوجيا المعلومات، المالية، الشؤون القانونية والبرامج	إدارة المخاطر الأمنية وتكنولوجيا المعلومات	**Q1** تم إعداد نظام **Q2** تدريب القدرات **Q3** النظام قيد التش **Q4** النتائج والتحليل
المشاركة في قضايا/مخاوف إدارة المخاطر الأمنية والتواصل بشأنها	إعداد سجل عبر الإنترنت لجميع الاجتماعات وجداول الأعمال والمحاضر المتعلقة بإدارة المخاطر الأمنية	تكنولوجيا المعلومات وإدارة المخاطر الأمنية	إدارة المخاطر الأمنية	**Q1** إعداد الأنظمة **Q2** تدريب القدرات **Q3** التجميع والتفكي
الفحص المادي لموارد إدارة المخاطر والمعدات والتدابير المعمول بها	تصميم هيكل التدقيق الداخلي وتنفيذه	إدارة المخاطر الأمنية، تكتولوجيا المعلومات، الشؤون القانونية والبرامج	إدارة المخاطر الأمنية والبرامج	**Q1** نظام التدقيق ا **Q2** تدريب القدرات على مستوى الموظ **Q3:** التجميع والتفك
المشاركة في قضايا/مخاوف إدارة المخاطر الأمنية والتواصل بشأنها	قم بتعديل قوالب تقارير البرنامج لتشمل قسم تعليقات إدارة المخاطر الأمنية SRM المرتبط بسجل الحوادث / الحوادث الوشيكة / المخاوف	إدارة المخاطر الأمنية، تكتولوجيا المعلومات، البرامج	البرامج وإدارة المخاطر الأمنية	**Q1** التعديلات المن **Q2** بناء القدران م **Q3** إطلاق **Q4** التجميع والتفكي
بناء القدرات فيما يتعلق بإدارة المخاطر الأمنية	تم تطوير مصفوفة التدريب وسجل التدريب وتعبئتهما ودمجهما	الموارد البشرية، إدارة المخاطر الأمنية، تكتولوجيا المعلومات، المالية	الموارد البشرية وإدارة المخاطر الأمنية	**Q1** استكمال تحليل المصفوفة وإعداد ال **Q2** بدء برنامج الت **Q3** النظام قيد التش **Q4** النتائج والتحليل

أمثلة مقدمة من طرف سلامة المواقع الدولية

	المدة المتوقعة	التكلفة
ي تصميم السؤال وتم تطوير ت ز للإكمال ي تم تحليلها وتقديمها	**Q1-Q3**	**وقت الموظفين:** خمسة أيام لتطوير نظام الإستبيان وتكنولوجيا المعلومات وإجراء ضمان الجودة 30 دقيقة لكل عضو من أعضاء الموظفين لإكمال الاستبيان ثلاثة أيام لتحليل النتائج وتقديمها **التكلفة المالية:** 250 جنيهًا إسترلينيًا لعضوية نظام الاستبيان الإلكتروني
التسجيل وإطلاقه ت لجميع الموظفين شغيل. ل الأولي والإجراءات	**Q1-Q2 التطوير والإعداد** جاري التنفيذ: المراجعة والتفكير ربع السنوي	**وقت الموظفين:** 30 يومًا للتطوير والتنفيذ تدريب لمدة ساعة لجميع الموظفين **التكلفة المالية:** 3000-5000 جنيه إسترليني للنظام القائم على التطبيق 1000 جنيه إسترليني للتدريب الخارجي
الداخلية ت، وتأكيد المذكرات ير والمراجعة المستمرة	**Q1-Q2 التطوير والإعداد** جاري التنفيذ: المراجعة والتفكير ربع السنوي	**وقت الموظفين:** يومين للإعداد تدريب لمدة ساعة على القدرات لموظفي إدارة المخاطر الأمنية الرئيسيين **التكلفة المالية:** 0 جنيه استرليني
لداخلي وإعداد العملية ت لجميع قادة التدقيق ونشرها فين بالكامل كير والمراجعة المستمرة	**Q1-Q2 التطوير والإعداد** جاري التنفيذ: المراجعة والتفكير ربع السنوي	**وقت الموظفين:** 15 يومًا من الإعداد تدريب لمدة ثلاث ساعات لكل مسؤول تدقيق، وتدريب لمدة ساعة لجميع الموظفين **التكلفة المالية:** تعديلات وتطوير نظام تكنولوجيا المعلومات بقيمة 1000 جنيه إسترليني
جزة ع قادة البرنامج ير والمراجعة المستمرة	**Q1-Q2 التطوير والإعداد** جاري التنفيذ: المراجعة والتفكير ربع السنوي	**وقت الموظفين:** 10 أيام للتطوير والمراجعة تدريب لمدة ثلاث ساعات لكل قائد برنامج **التكلفة المالية:** 0 جنيه استرليني
ي الاحتياجات التدريبية. تطوير سجل تدريب شغيل. ل الأولي والإجراءات	**Q1-Q2 التطوير والإعداد** جاري التنفيذ: المراجعة والتفكير ربع السنوي	**وقت الموظفين:** ثمانية أيام للتطوير والتنفيذ تعتمد الاحتياجات التدريبية المستمرة على تحليل الاحتياجات التدريبية **التكلفة المالية:** الاعتماد على مقدمي التدريب

مراجع

عامة

بريكنريدج، إم.-جيه، وززورنو، إم، ودوكي-ديز، إم، وفيربانكس، إيه، وهارفي، بي، وستودارد، إيه (2023). تقرير أمن عمال الإغاثة 2023. التدريب الأمني في القطاع الإنساني: قضايا العدالة والفعالية. النتائج الإنسانية.
https://www.humanitarianoutcomes.org/AWSR_2023

هيرمان، إي.، وأوبرهولزر، إس. (2020). "إدارة المخاطر الأمنية وتجنب المخاطر في القطاع الإنساني." تقييم عمليات صنع القرار في المنظمات غير الحكومية الإنسانية المحلية والدولية. جنيف: ICVA. https://www.icvanetwork.org/uploads/2021/07/Security_Risk_Management_May2020-1.pdf

شبكة الممارسات الإنسانية (2010). (HPN). مراجعة الممارسات الجيدة: إدارة الأمن التشغيلي في البيئات العنيفة. العدد 8 (طبعة جديدة). معهد التنمية الخارجية.
https://odihpn.org/wp-content/uploads/2010/11/GPR_8_revised2.pdf

الفقرة 1

تشابل، م، (2023): 'الرغبة في المخاطرة مقابل تحمل المخاطر؛ ما الفرق بينهما؟ الهدف التقني https://www.techtarget.com/searchcio/feature/Risk-appetite-vs-risk-tolerance-How-are-they-different

داتامينر، (2022)، "فهم وتخطيط مشهد المخاطر في الشركات". https://www.dataminr.com/resources/ebook/understand-and-plan-for-the-corporate-risk-landscape

دونوفان، ل. (2022)، "ما هي الرغبة في المخاطرة وكيف يمكنك تنفيذها؟"، شبكة قيادة المخاطر. https://www.riskleadershipnetwork.com/insights/what-is-risk-appetite-and-how-do-you-implement-it

درابر، ر (2014)، "كيفية كتابة خطة إدارة المخاطر الأمنية الاستراتيجية"، لينكد إن https://www.linkedin.com/pulse/how-write-strategic-security-rick-draper/

خووشي، س، (2017)، "التخطيط الاستراتيجي للمنظمات غير الحكومية: دليل لفهم أسس التخطيط الاستراتيجي لينكدإن. https://www.linkedin.com/pulse/strategic-planning-ngos-guide-understand-basics-samina-khushi/

سيمبسون، ك. ورانداال، آي (2020). 'تصميم الأنظمة: "مقدمة، واسافيري." https://u05.88f.myftpupload.com/wp-content/uploads/2020/10/Wasafiri-SystemCraft-2020-Small.pdf

مجموعة توجيهية بشأن الأهمية الحاسمة لبرامج الأمم المتحدة (2016)، إطار الأهمية الحاسمة لبرامج منظومة الأمم المتحدة، CEB/2016/HLCM/23.
https://programmecriticality.org/Static/index.html

USAID 2022. بيان الرغبة في المخاطرة للوكالة الأمريكية للتنمية الدولية: مرجع إلزامي للفصل 596 من قانون ADS.
https://www.usaid.gov/sites/default/files/2022-12/596mad.pdf

الفقرة 2

مقالة "أدوات التفكير": "مصفوفة RACI" "تنظيم المساءلات لتحقيق أقصى قدر من الكفاءة والنتائج". https://www.mindtools.com/agn584l/the-raci-matrix

فون مولتكه، ن. (2024)، "نموذج RACI والدليل النهائي لعام 2024 لمصفوفة RACI"، أكاديمية الابتكار. https://www.aihr.com/blog/raci-template/

الفقرة 3

IEC 31010:2019: إدارة الأزمات تقنيات تقييم المخاطر.
https://www.iso.org/standard/72140.html

قام المركز السويسري للكفاءة في التعاون الدولي (CINFO) وGISF بتطوير أداة شاملة للتقييم الذاتي لواجب الرعاية. https://dutyofcare.cinfo.ch/index.html

3.2 البرنامج/العمليات

دليل عمل المدافعين في الخطوط الأمامية حول الأمن.
https://www.frontlinedefenders.org/en/workbook-security

أداة الأمن GISF، 2. تحليل القبول.
https://www.gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/

منتدى الأمن العالمي المشترك بين الوكالات. (2021) تحقيق العمليات الآمنة من خلال القبول: التحديات والفرص لإدارة المخاطر الأمنية. منتدى الأمن العالمي المشترك بين الوكالات (GISF). https://www.gisf.ngo/wp-content/uploads/2021/12/Achieving_Safe_Operations_through_Acceptance_challenges_and_opportunities_for_security_risk_management.pdf

لاريسا فاست، ل.، فينوكين سي.، فريمان ف.، أونيل م.، رولي إي.، (2011) مجموعة أدوات القبول، منظمة إنقاذ الطفولة. https://acceptanceresearch.files.wordpress.com/2012/01/acceptance-toolkit-final-for-print-with-notes.pdf

"مورّو، إ. (2023) "الوصول الإنساني وإدارة الأمن: اعتبارات لأمان الموظفين' مدونة GISF https://www.gisf.ngo/blogs/humanitarian-access-security-management-considerations-for-security-staff/

ستودارد، أ.، كزوارنو، م.، وهامسيك، إل. (2019). المنظمات غير الحكومية والمخاطر: إدارة حالة عدم اليقين في الشراكات المحلية والدولية (تقرير عالمي). النتائج الإنسانية.
https://www.humanitarianoutcomes.org/publications/ngos-risk2-partnerships

3.3 المالية

منتدى الأمن العالمي المشترك بين الوكالات (GISF). (2013). تكلفة إدارة المخاطر الأمنية للمنظمات غير الحكومية. https://www.gisf.ngo/resource/the-cost-of-srm-for-ngos/

سويني، أ. (2019)، "تأمين سلامة العاملين في مجال الإغاثة من خلال الميزانية الفعالة"، الاستجابة للأزمات، أكتوبر 2019 | المجلد: 14 | المسألة 4 https://www.gisf.ngo/wp-content/uploads/2019/11/Securing-Aid-Worker-Safety-Through-Effective-Budgeting.pdf

3.4 الاتصالات

فولكس، أ، (2022)، حملة تضليل ضد اللجنة الدولية للصليب الأحمر في أوكرانيا، BBC News. https://www.bbc.com/news/world-europe-60921567

GISF ومؤسسة Cornerstone OnDemand، (2019)، مجموعة أدوات إدارة المخاطر الأمنية: الاستراتيجيات. https://gisf.ngo/wp-content/uploads/2020/03/Planning-security-risk-management-strategies-and-systems.pdf

إنترنيوز، (2019)، إدارة المعلومات المضللة في سياق إنساني. https://internews.org/wp-content/uploads/2021/02/Rumor_Tracking_Mods_3_How-to-Guide.pdf

ليلاند، جيه، وتيلر، إس، وبهاتاشاريا، ب. (2023). المعلومات المضللة في البرامج الإنسانية: الدروس المستفادة من تجربة الاستماع التي تقدمها منظمة أطباء بلا حدود مجلة الشؤون الإنسانية، 5(2).

أوه، س.، أدكينز، ت. (2018)، مجموعة أدوات التضليل، InterAction. https://www.interaction.org/wp-content/uploads/2019/02/InterAction_DisinformationToolkit.pdf

3.5 تكنولوجيا المعلومات

ريليفويب، "الهجمات الإلكترونية: تهديد حقيقي للمنظمات غير الحكومية وغير الربحية"، 2022.
https://reliefweb.int/report/world/cyberattacks-real-threat-ngos-and-nonprofits

أمن سهل الوصول من : GISF (2020) الوحدة 4 الأمن الرقمي. https://gisf.ngo/wp-content/uploads/2020/11/GISF_Security-to-Go_Module-4_Oct20.pdf

اللجنة الدولية للصليب الأحمر، (2024)، هجوم إلكتروني على اللجنة الدولية للصليب الأحمر: ماذا نعرف. https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

كومار م. (2017)، الأمن الرقمي للعاملين في مجال الإغاثة من مجتمع LGBTQ+: الوعي والاستجابة. https://www.gisf.ngo/resource/digital-security-of-lgbtqi-aid-workers-awareness-and-response/

ستين ك.، كوين س.، ويت ج.، غاردنر ر. ك.، (2020) دمج الأمن السيبراني وإدارة المخاطر المؤسسية، المعهد الوطني للمعايير. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf

3.6 الموارد البشرية

آرثر، ت. وموتارد، ل. (2022). نحو إدارة شاملة للمخاطر الأمنية: تأثير "العرق" والانتماء العرقي والجنسية على أمن العاملين في مجال الإغاثة. منتدى الأمن العالمي المشترك بين الوكالات (GISF). https://gisf.ngo/wp-content/uploads/2022/05/Towards-Inclusive-Security-the-impact-of-race-ethnicity-and-nationality-on-aid-workers-security.pdf

سلسلة بودكاست الأمن الشامل GISF الحلقة 1: تقديم نهج يركز على الشخص. https://gisf.ngo/resource/inclusive-security-e1-introducing-a-person-centered-approach/

GISF، (2018)، إدارة أمن العاملين في مجال الإغاثة من ذوي الملفات الشخصية المتنوعة https://gisf.ngo/resource/managing-the-security-of-aid-workers-with-diverse-profiles/

GISF (2017)، مجموعة أدوات الأمان المتنقلة: الوحدة 12 إدارة الأفراد، سي ويليامسون. https://gisf.ngo/resource/people-management-security-to-go-module/

جولد هيل، أو (2019)، رئيس خدمات الصحة العقلية في فلسطين يقول إن اضطراب ما بعد الصدمة هو مفهوم غربي، مجلة كوارتز. https://qz.com/1521806/palestines-head-of-mental-health-services-says-ptsd-is-a-western-concept

جوزي، هـ (2020)، إزالة الاستعمار من الصدمة مع فرانز فانون، مطبعة جامعة أكسفورد. https://academic.oup.com/ips/article-abstract/15/1/102/5868933?redirectedFrom=fulltext

شركة ماكينزي آند كومباني: (2023). ما هي السلامة النفسية؟ شركة ماكينزي آند كومباني. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-psychological-safety

بيرسود، س. (2014أ). الجنس والأمن: المبادئ التوجيهية لدمج النوع الاجتماعي في إدارة المخاطر الأمنية. GISF. https://www.gisf.ngo/resource/ gender-and-security/

3.7 الشؤون القانونية

GISF، (2012)، الوكالات الدولية العاملة مع الشركاء المحليين، ورقة إحاطة GISF. https://gisf.ngo/resource/international-agencies-working-with-local-partners/

تقرير معياري عالمي لواجب الرعاية من ISOS، 2015 https://www.internationalsos.co.id/duty-of-care

ميركلباخ، م. وكيمب، إي. (2011). هل يمكن مقاضاتك؟ المسؤولية القانونية للمنظمات الدولية العاملة في مجال المساعدات الإنسانية تجاه موظفيها. مبادرة إدارة الأمن. https://www.gisf.ngo/resource/ can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/

ميركلباخ، م. وكيمب، إي. (2016). واجب الرعاية: مراجعة لحكم قضية دينيس ضد المجلس النرويجي للاجئين وتداعياته. GISF. https://gisf.ngo/ resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/

3.8 الحماية

ندوة عبر الإنترنت لـGISF | تقاطع الأمن والحماية | تسجيل. https://gisf.ngo/resource/gisf-webinar-intersection-of-security-and-safeguarding-recording/

مولين ك.، (2021)، إطلاق مجموعة أدوات الحماية المرئية القائمة على المجتمع https://www.interaction.org/blog/launching-the-safeguarding-community-visual-toolkit/

مركز دعم الموارد والحماية (RSH). https:/ safeguardingsupporthub.org/

ملاحظة إرشادية حول كيفية تنفيذ دورة الحماية https://www.gisf.ngo/resource/how-to-note-on-implementing-the-safeguarding-cycle/

الأساسيات. https://safeguardingsupporthub.org/essentials

مسرد مصطلحات PSEA.
https://safeguardingsupporthub.org/psea-glossary-clear-global

مقدمة حول الحماية – RSH جنوب السودان. https://safeguardingsupporthub.org/sites/default/files/essentials/Essentials_What%20is%20safeguarding/Essentials_Introduction%20to%20safeguarding%20South%20Sudan.pdf

3.9 السفر

ISO 31030: إدارة مخاطر السفر. https://www.iso.org/standard/54204.html

الفقرة 4

GISF (2022)، دليل التعاون الأمني للمنظمات غير الحكومية, Global المنتدى العالمي للأمن المشترك بين الوكالات.
https://www.gisf.ngo/long-read/ngo-security-collaboration-guide/

منتدى الأمن العالمي المشترك بين الوكالات. (2021) الشراكات وإدارة المخاطر الأمنية: دليل عمل مشترك للمنظمات الإغاثية المحلية والدولية. منتدى الأمن العالمي المشترك بين الوكالات (GISF). https://www.gisf.ngo/wp-content/uploads/2021/06/GISF_Partner-Joint-Action-Guide_EN_download_Aug211.pdf

منتدى الأمن العالمي المشترك بين الوكالات. (2020) الشراكات وإدارة المخاطر الأمنية: من وجهة نظر الشريك المحلي. منتدى الأمن العالمي المشترك بين الوكالات (GISF).
https://www.gisf.ngo/resource/partnerships-and-security-risk-management-from-the-local-partners-perspective/

ISO 31000:2018 إدارة المخاطر. https://www.iso.org/standard/65694.html

إدارة الأمم المتحدة للسلامة والأمن. (2015). SLT إنقاذ الأرواح سوياً إطار عمل لتحسين الترتيبات الأمنية بين المنظمات غير الحكومية الدولية/المنظمات الدولية والأمم المتحدة.
https://www.gisf.ngo/wp-content/uploads/2020/02/2225-UNDSS-2015-Saving-Lives-Together-Framework.pdf

ويليامز س، (2020)، إدارة المخاطر الأمنية التعاونية: حالة من أجل التنمية المحلية، مقالة في منتدى GISF.
https://www.gisf.ngo/collaborative-security-risk-management-a-case-for-local-development/

الفقرة 5

بوث ب. (2010)، إدارة الأزمات والحوادث الحرجة، GISF
https://www.gisf.ngo/resource/crisis-management-of-critical-incidents/

المنتدى الأمني العالمي المشترك بين الوكالات و المجلس الاستشاري للأمن الخارجي. (2023) دليل ممارسة إدارة الأزمات للمنظمات غير الحكومية: دليل لتطوير وتيسير التمارين الفعالة. المنتدى الأمني العالمي المشترك بين الوكالات (GISF) والمجلس الاستشاري للأمن الخارجي (OSAC). https://www.gisf.ngo/resource/ngo-crisis-management-exercise-manual-a-guide-to-developing-and-facilitating-effective-exercises/

كونال كيه، إيدير بي، مجتمع لينكد إن، (2023)، كيف يمكنك تعزيز ثقافة الوعي بالمخاطر والمساءلة عبر الوظائف والمستويات المختلفة؟
https://www.linkedin.com/advice/0/how-do-you-foster-culture-risk-awareness

لوسيدشارت، (2023)، أفضل الاستراتيجيات لإدارة الفرق متعددة الوظائف.
https://www.lucidchart.com/blog/managing-cross-functional-teams

ميلر، ر. (2018)، الفرق متعددة الوظائف المؤثرة على جهود أمن المعلومات، لينكدإن.
https://www.linkedin.com/pulse/cross-functional-teams-impacting-information-security-richard-miller/?trk=public_profile_article_view

ناجيلي-بيازا ل. (2018)، إنشاء فريق متعدد الوظائف لمكافحة مشكلات أمن البيانات، جمعية إدارة الموارد البشرية (SHRM)
https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/cross-functional-team-to-combat-data-security-issues.aspx

وايت جيه، جوفيا بي، سنجر جيه، جوزياس إم، الاتجاهات الناشئة والدروس المبكرة في إدارة الأزمات ومرونة الأعمال، استخبارات إدارة الأزمات والاستشارات المتعلقة بالمخاطر.

http://www.s-rminform.com/srm-insights/crisis-management-business-resilience

الفقرة 6

بنيامين م. (2023)، فوائد المراقبة والتقييم في الوقت الفعلي، لينكد إن. https://www.linkedin.com/pulse/benefits-real-time-monitoring-evaluation-migolo-benjamin/

البيانات من أجل التنمية (2021)، طرق يمكنك من خلالها دمج التكنولوجيا في المراقبة والتقييم. https://datafordev.com/ways-you-can-integrate-technology-in-monitoring-and-evaluation/

اللجنة الدولية للإنقاذ (2021)، سلسلة النتائج، الإطار المنطقي ومصطلحات نظرية التغيير. https://rescue.app.box.com/s/e8sj6rep7hghs8j2yern8crxauavs6o8/file/775591027183

جادكاري م. (2023)، ما هو الرصد والتقييم والتعلم (MEL)؟، ريزونانس جلوبال. https://www.resonanceglobal.com/blog/what-is-monitoring-evaluation-and-learning-mel

باسانين ت.، بارنيت آي، (2019)، دعم الإدارة التكيفية، معهد التنمية الخارجية. https://cdn.odi.org/media/documents/odi-ml-adaptivemanagement-wp569-jan20.pdf

التحالف الدولي للتنمية في اسكتلندا، (2023)، دليل الرصد والتقييم والتعلم. https://intdevalliance.scot/wp-content/uploads/2023/08/MEL_Support_Package_4th_June.pdf

البنك الدولي، (2004)، الرصد والتقييم؛ بعض الأدوات والأساليب والمناهج. https://cnxus.org/wp-content/uploads/2022/04/WB_ME20ENG.pdf

مجموعة أدوات الرصد والتقييم: مجموعة أدوات تمهيدية للمبتدئين، المقال: ما هو الرصد والتقييم؟ https://thetoolkit.me/what-is-me/

تورنبول م.، تورفيل إي.، (2012) القدرة التشاركية وتحليل نقاط الضعف: دليل الممارس، منظمة أوكسفام البريطانية https://policy-practice.oxfam.org/resources/participatory-capacity-and-vulnerability-analysis-a-practitioners-guide-232411/

ويلسدون، ن. معهد أبحاث العمل التطوعي، "اتباع نهج التعلم الاستراتيجي للتقييم". https://www.ivar.org.uk/blog/taking-a-strategic-learning-approach-to-evaluation/

مكتب تنسيق الشؤون الإنسانية/باسمينة جيردا

نيجيريا

متطوع من منظمة أطباء بلا حدود يساعد في عيادة لدعم الأشخاص النازحين من منازلهم.

gisf

منتدى الأمن العالمي المشترك بين الوكالات

أبحاث وبرامج GISF
الهاتف: 5032 7274 20(0) 44+
البريد الالكتروني: research@gisf.ngo

www.gisf.ngo