

واژه‌های فاوا

// پیامد (consequence):

تبعات رویداد اثر گذار بر اهداف عینی حاصل را گویند هر رویداد می‌تواند به مجموعه‌ای از تبعات منجر شود که ممکن است معین یا نامعین باشند و در بستر امنیت اطلاعات به طور معمول معنای منفی دارند. تبعات را می‌توان به صورت کمی یا کیفی بیان کرد. تبعات اولیه ممکن است به صورت زنجیره‌ای دامن گسترش شوند.

// واپایش (control):

محدود کردن مخاطره را گویند که در امنیت اطلاعات شامل هر فرایند، خط‌مشی، روال، رهنمود، عملکرد یا ساختار سازمانی می‌شود که می‌توانند ماهیت اداری، فنی، مدیریتی یا حقوقی داشته باشند و مخاطرات امنیت اطلاعات را محدود کنند. واپایش ممکن است همیشه محدودکنندگی مورد نظر یا فرضی را نداشته باشد و مترادفی برای محافظت یا اقدام متقابل نیز هست.

// بستری بیرونی (external context):

محیط بیرونی که سازمان در آن در پی تحقق اهداف خود است و می‌تواند شامل موارد زیر باشد:

- محیط فرهنگی، اجتماعی، سیاسی، حقوقی، مقرراتی، مالی، فنی، اقتصادی، طبیعی و رقابتی که می‌توانند بین المللی، ملی، منطقه‌ای یا محلی باشند

- روندها و محرک‌های کلیدی اثر گذار بر اهداف عینی سازمان
- روابط با ذینفعان بیرونی و برداشت‌ها و ارزش‌های مربوطه

// بستری درونی (internal context):

محیط درونی که سازمان در آن در پی تحقق اهداف خود است و می‌تواند شامل موارد زیر باشد:

- حاکمیت، ساختار سازمانی، نقش‌ها و مسئولیت‌پذیری‌ها
- خط‌مشی‌ها، اهداف و راهبردها

- قابلیت‌ها از لحاظ منابع و دانش (مثل سرمایه، زمان، کارکنان، فرایندها، سامانه‌ها و فناوری‌ها)

- سامانه‌های اطلاعات، گردش‌های اطلاعات و فرایندهای تصمیم‌گیری (رسمی یا غیررسمی)

- روابط با ذینفعان درونی و برداشت‌ها و ارزش‌های مربوطه
- فرهنگ سازمان

- استانداردها، رهنمودها و حالت‌های اتخاذی توسط سازمان
- شکل و گستره‌ی روابط پیمانی

// مخاطره (risk):

اثر عدم قطعیت بر اهداف که می‌تواند انحراف مثبت یا منفی باشد. اهداف نیز وجوه مختلفی دارند (مثل اهداف مالی، بهداشتی، ایمنی، امنیت اطلاعات و اهداف زیست‌محیطی) و در ترازهای مختلف (مثل راهبردی، سازمانی، پروژه‌ای، فرآورده و فرایند) قابل اعمال است. اغلب با ارجاع به رویدادهای بالقوه و پیامدها یا آمیزه‌ای از این دو، مشخصات مخاطره را تعیین می‌کنند. مخاطره امنیت اطلاعات را اغلب بر حسب آمیزه‌ای از پیامدهای رویداد امنیت اطلاعات و احتمال رخداد مربوطه بیان می‌کنند. عدم قطعیت به معنای نارسایی درک یا شناخت رویداد، پیامد یا احتمال آن است. مخاطره امنیت اطلاعات با قابلیت تهدیدهایی رابطه دارد که از آسیب‌پذیری‌های

اطلاعات بهره‌برداری می‌کنند.

// تراز مخاطره (level of risk):

دامنه مخاطره که بر حسب آمیزه پیامدها و احتمال‌شان بیان می‌شود.

// مخاطره باقی‌مانده (residual risk):

مخاطره باقی‌مانده پس از برطرف‌سازی مخاطره که می‌تواند شامل مخاطرات شناخته نشده باشد. مخاطره باقی‌مانده به مخاطره مانده نیز معروف است.

// ارزیابی مخاطره (risk assessment):

فرآیند کلی شناسایی، تحلیل و ارزیابی مخاطره

// ارتباطات و رایزنی مخاطره

(risk communication and consultation):

فرایندهایی مستمر و مکرر که سازمان‌ها برای فراهم‌سازی، تشریح یا به دست آوردن اطلاعات و تعامل با ذینفعان راجع به مدیریت مخاطره انجام می‌دهند. این اطلاعات می‌تواند به وجود، ماهیت، شکل، احتمال، اهمیت، ارزیابی، قابلیت پذیرش و برطرف‌سازی مخاطره ارتباط داشته باشد. رایزنی فرایند دوسویه ارتباط آگاهانه بین سازمان و ذینفعان آن پیش از تصمیم‌گیری راجع به موضوعی یا تعیین مسیر آن است و بر اثر نفوذ داشتن نه اعمال قدرت بر تصمیمات اثر می‌گذارد.

// معیارهای مخاطره (risk criteria):

شرایط مرجع که اهمیت مخاطره توسط آن‌ها ارزیابی می‌شود. معیارهای مخاطره مبتنی بر اهداف سازمانی و بستری بیرونی و درونی است. معیارهای مخاطره از استانداردها، قوانین، خط‌مشی‌ها و سایر الزامات قابل استخراج است.

// سنجش مخاطره (risk evaluation):

فرآیند مقایسه نتایج تحلیل مخاطره با معیارهای مخاطره به منظور تعیین این که مخاطره و یا دامنه آن قابل قبول یا تحمل هست یا خیر. سنجش مخاطره به تصمیم‌گیری راجع به برطرف‌سازی مخاطره کمک می‌کند.

// شناسایی مخاطره (risk identification):

فرایند یافتن، تشخیص و تشریح مخاطرات را گویند. شناسایی منابع مخاطره، رویدادهای، علل آن‌ها و پیامدهای بالقوه‌شان جزو شناسایی مخاطره است. شناسایی مخاطره می‌تواند شامل داده‌های تاریخی، تحلیل نظری، نظرات کارشناسی و اطلاعات‌مند و نیازهای ذینفعان می‌شود.

// مدیریت مخاطره (risk management):

فعالیت‌های هماهنگ جهت هدایت و کنترل سازمان نسبت به مخاطره یادآوری در این استاندارد در کل از واژه فرایند برای مدیریت مخاطره به کار می‌رود و مولفه‌های درونی آن را فعالیت می‌نامند.

// برطرف‌سازی مخاطره (risk treatment):

فرایند محدود کردن مخاطره را گویند که شامل موارد زیر می‌شود:
- پرهیز از مخاطره با آغاز نکردن یا ادامه ندادن فعالیتی که مخاطره‌افزا است.

- تن دادن به مخاطره یا افزودن مخاطره به منظور استفاده از فرصت

- حذف منبع مخاطره

- تغییر دادن احتمال

- تغییر دادن پیامدها

- تشریح مخاطره با طرف یا طرف‌های دیگر و مهار مخاطره از طریق انتخاب آگاهانه

برطرف‌سازی مخاطره می‌تواند مخاطرات جدیدی پدید آورد یا مخاطرات موجود را محدود کند.