عنوان دوره: مدیریت ریسک امنیت اطلاعات مبتنی بر استاندارد

ISO/IEC 27005

INTERNATIONAL STANDARD

ISO/IEC 27005

Fourth edition
2022-10

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

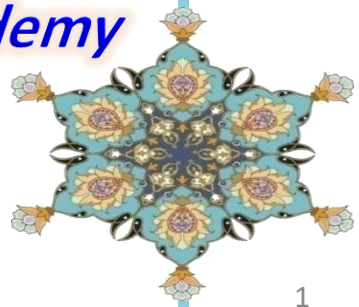
Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information

ISO IEC

Reference number
ISO/IEC 27005:2022(E)

ISO/IEC 27005:2022: Information security, cyber security and privacy protection -Guidance on managing information security risks

By: Zoozanaqeh Educational and Research Academy



کلیات دوره مدیریت ریسک مبتنی بر استاندارد ISO/IEC 27005:

سرفصل‌ها

مستندات دوره:

- فایل آموزشی دوره
- ISO/IEC 27005: 2022
- ISO/IEC 31000:2018
- IEC 31010: 2019
- سایر استانداردها و منابع مرتبط

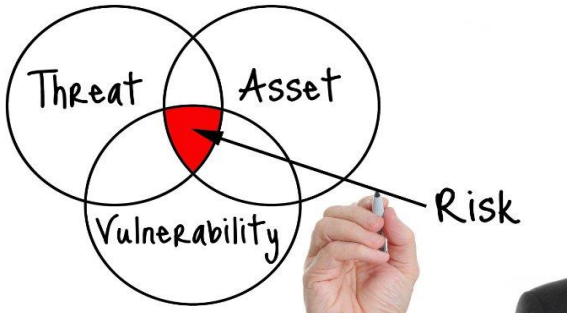
ارزیابی دوره:

- حضور فعال در دوره
- مشارکت در فعالیت‌های تیمی
- انجام تکلیف کلاسی
- آزمون نهایی

شناسایی ریسک

- رویدادی رخ دهد که منجر به خسارت، نابودی یا افشاء داده ها یا منابع دیگر شود .
- احتمال اینکه یک تهدید از یک آسیب پذیری بهره برداری کرده و منجر به ایجاد خسارت در یک دارایی گردد.

Information security risks are usually associated with a negative effect of uncertainty on information security objectives.



Information security risks can be associated with the potential that threats (3.1.9) will exploit vulnerabilities (3.1.10) of an information asset or group of information assets and thereby cause harm to an organization.

شناسایی ریسک امنیت اطلاعات

1. شناسایی دارایی‌های موجود در دامنه (طبقه‌بندی و ارزش‌گذاری)
2. شناسایی تهدیدات علیه دارایی‌ها
3. شناسایی آسیب‌پذیری‌های متناظر با تهدید و دارایی
4. شناسایی ریسک (آسیب‌ها)
5. تعیین مالکان ریسک

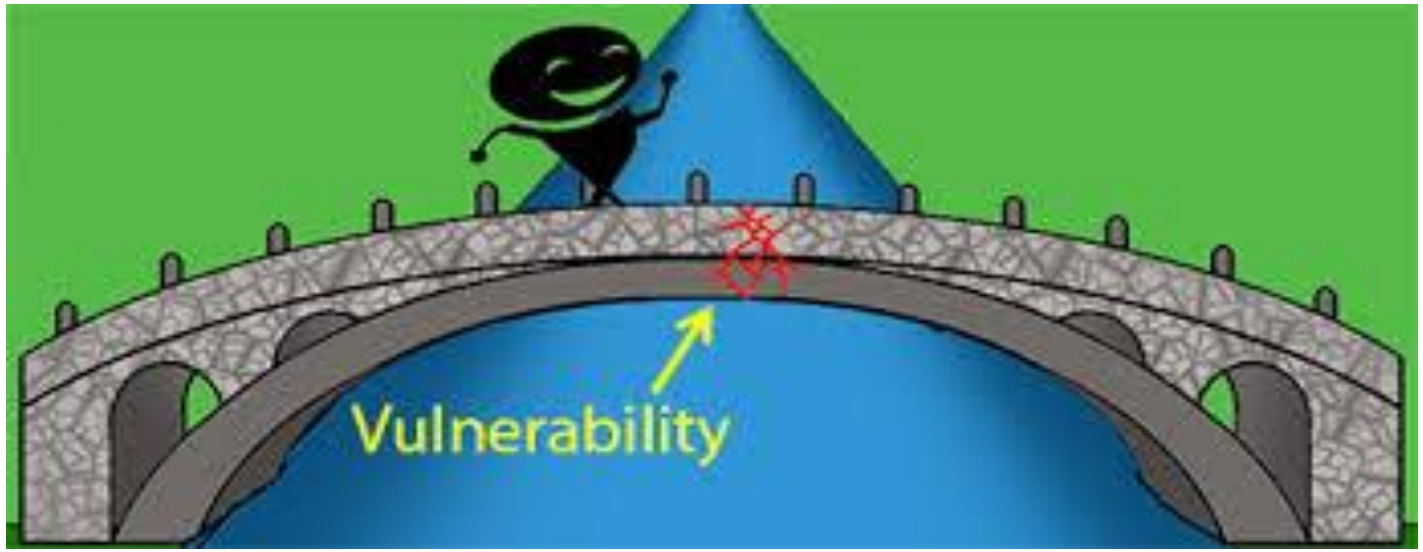
نمونه‌ای از ارزش گذاری دارایی

ردیف	معیار شدت اثر	ارزش دارایی		
		۱	۲	۳
۱	میزان تأثیر دارایی از نظر مالی بر سازمان	کمتر از ۵۰ میلیون ریال	بین ۵۰ تا ۱۰۰ میلیون ریال	بیش از ۱۰۰ میلیون ریال
۲	میزان تأثیر دارایی بر عملیات Online سازمان	ایجاد وقفه در فعالیت های سازمان تا ۱۵ دقیقه	ایجاد وقفه در فعالیت های سازمان تا یک ساعت	ایجاد وقفه در فعالیت های سازمان بیش از یک ساعت
۳	تأثیر دارایی بر وجهه و اعتبار سازمان	داخل شرکت	صنف	ملی/ بین المللی
۴	از دست دادن درآمد مشتری (ماهانه)	کمتر از ۱۰میلیون ریال	بین ۱۰ تا ۱۰۰ میلیون ریال	۱۰۰ یا بیش از ۱۰۰ میلیون ریال
۵	رضایت مشتری (تعداد شکایات هر هفته)	کمتر از ۵	۱۰	بیش از ۱۰
۶	درز اطلاعات محرمانه و تجربیات شرکت به بیرون	داخل سازمان	بیرون سازمان	رقبا
۷	میزان تأثیر دارایی بر عملیات کاری روتین	۱ نفر	در واحد	در کل سازمان

شناسایی آسیب‌پذیری‌ها

آسیب‌پذیری

ضعف دارایی یا حفره امنیتی در دارایی (یا محیط پیرامون آن) که زمینه خسارت به سازمان را فراهم می‌کند.



کار عملی تیمی:

شناسایی ریسک‌های امنیت اطلاعات

دامنه فرضی برای مدیریت ریسک درنظر بگیرید. دارایی‌ها، تهدیدات، آسیب‌پذیری‌ها و مالکان ریسک را شناسایی کنید.

تدوین طرح مقابله با ریسک امنیتی(RTP)

- انتخاب گزینه مناسب برای مقابله با ریسک،
- تعیین کنترل‌های مورد نیاز
- روش پیاده‌سازی کنترل امنیتی،
- اولویت‌بندی پیاده‌سازی کنترل،
- مسوولیت اجرای کنترل،
- برنامه زمانی اجرای کنترل،
- ساز و کار سنجش اثربخشی کنترل.

دارایی	تهدید	کنترل های موجود	کنترل های پیشنهادی	مسئول اجرا	زمان شروع	مهلت انجام	منابع		
							مالی	انسانی	تجهیزت

برای درخواست برگزاری دوره آنلاین یا حضوری و یا دریافت فایل کامل دوره با آکادمی ذوزنقه تماس بگیرید.

راه های ارتباطی:

www.Zoozanaqeh.com

Zoozanaqeh@gmail.com