

عنوان دوره:

فارسی: مدیریت راهبردی امنیت اطلاعات  
انگلیسی: Information Security Strategic Management

درباره دوره:

گسترش روز افزون تهدیدات و افزایش حملات سایبری به سازمان‌ها در سال‌های اخیر، بیانگر آن است که شیوه‌های دفاع فعلی در برابر این تهدیدات دیگر جوابگو نیست و سازمان‌ها نیازمند بکارگیری تدابیر اصولی‌تری در این حوزه هستند. امروزه یکی از مهمترین راهکارها در خصوص مدیریت امنیت اطلاعات و پاسخگویی مناسب به تهدیدات سایبری، استفاده از الگوهای راهبردی امنیت اطلاعات است.

در این دوره آموزشی، مخاطبان ضمن آشنایی با الزامات، نیازمندی‌ها، استانداردها و به‌روش‌های راهبردی امنیت اطلاعات در سازمان می‌توانند امنیت اطلاعات را در سازمان‌های خویش، مدیریت و راهبری کنند.

اهداف دوره:

- 1- آشنایی با الزامات و نیازمندی‌های راهبردی امنیت اطلاعات در سازمان‌های ایرانی
- 2- آشنایی با استانداردها و به‌روش‌های مدیریت راهبردی امنیت اطلاعات
- 3- آشنایی با روش‌ها و متدولوژی‌های مدیریت مخاطرات امنیت اطلاعات
- 4- آشنایی با نحوه تدوین برنامه‌های مدیریت تداوم کسب و کار و بازیابی از فاجعه
- 5- آشنایی با نحوه انتخاب کنترل‌های امنیت اطلاعات برای سازمان
- 6- آشنایی با چگونگی اندازه‌گیری اثربخشی کنترل‌های امنیتی بکار گرفته شده

مخاطبان دوره:

- ✓ مدیران، راهبران و کارشناسان فناوری اطلاعات و امنیت
- ✓ مشاوران امنیت اطلاعات

مدت زمان دوره:

16 ساعت (2 روز)

محتویات دوره:

### 1- روز اول

- آشنایی با اصول و مفاهیم راهبردی امنیت اطلاعات
  - اصطلاحها و تعاریف مهم امنیت اطلاعات
  - مثلث سه گانه امنیت اطلاعات و نحوه ارتباط اجزای آن با یکدیگر
  - مثلث عملکرد، راحتی استفاده و امنیت و اصول رعایت آن در سازمانها
  - اصول امنیت اطلاعات
  - چرخه تداوم امنیت در سازمان
  - مفاهیم امنیت راهبردی و راهبری امنیت
  - دارایی و دارایی‌های اطلاعاتی در راهبری امنیت
  - روش‌های شناسایی دارایی‌ها
  - به‌روشها و بهترین درس آموزه‌های امنیت اطلاعات
- آشنایی با الزامات و نیازمندی‌های امنیت اطلاعات
  - الزامات کلیدی امنیت اطلاعات
  - اصول مدیریت امنیت اطلاعات
  - نیازمندی‌های امنیت اطلاعات بهینه
  - آسیب‌پذیری‌ها و تهدیدات امنیتی
  - چالش‌های فراهم‌آوری امنیت اطلاعات در سازمانها
- آشنایی با فرایندهای ارزیابی و مدیریت مخاطرات امنیت اطلاعات
  - متدولوژی‌های مدیریت دارایی‌ها
  - شیوه‌های ارزش‌دهی به دارایی‌ها
  - شیوه ارزش‌گذاری دارایی‌های با روابط متقابل
  - متدولوژی‌های ارزیابی مخاطرات امنیت اطلاعات
  - استانداردهای مطرح در حوزه ارزیابی مخاطرات امنیت اطلاعات
  - آسیب‌پذیری‌ها و نحوه بررسی و اولویت‌بندی آنها
  - سازوکارهای تبیین آنالیز ضربه (Impact Analysis) و پیامدهای تهدیدات

- شیوه‌های دستیابی به احتمال وقوع تهدیدات
  - روش‌های ارزیابی و تعیین مخاطره برای هر دارایی
  - روش‌های اولویت‌بندی مخاطرات
  - روش‌های شناسایی و بررسی آسیب‌پذیری‌های دارایی‌ها
  - روش‌های شناسایی و بررسی تهدیدات دارایی‌ها
  - استراتژی‌های مطرح در مدیریت مخاطرات
  - روش تعیین معیار و سطح قابل قبول مخاطرات
  - روش‌های اتخاذ کنترل‌های امنیتی
  - بهترین تجربه‌های جهانی در حوزه مدیریت مخاطرات
  - بررسی جایگاه افراد، فرایندها و فناوری‌ها در راهبرد امنیت اطلاعات سازمان
  - چگونگی تعریف نقش‌ها و مسئولیت‌های راهبردی امنیت اطلاعات در سازمان
    - نقش‌ها و مسئولیت‌های راهبردی امنیت اطلاعات
    - چگونگی تعریف این نقش‌ها و مسئولیت‌ها
  - اصول راهبری و مدیریت امنیت اطلاعات در سازمان‌های ایرانی
    - اصول راهبردی امنیت اطلاعات در حوزه راهبری فناوری اطلاعات و امنیت
    - جایگاه مدیریت امنیت راهبردی در سازمان
    - نقش امنیت راهبردی در فراهم‌آوری دفاع فعال در سازمان
    - حوزه‌های مورد توجه در امنیت راهبردی
    - رویکردهای امنیت راهبردی
    - مزایای امنیت راهبردی
    - مشکلات و چالش‌های امنیت راهبردی
  - راهکارهای مدیریت راهبردی امنیت اطلاعات در سازمان
    - مدیریت عملیات
    - مدیریت ظرفیت
    - مدیریت تغییرات
    - مدیریت ارتباطات
    - مدیریت دسترسی
    - مدیریت دارایی‌ها
    - مدیریت منابع انسانی
    - مدیریت امنیت اطلاعات
    - مدیریت خدمات شخص سوم
  - نکات قابل توجه در راهبردهای مدیریتی امنیت فیزیکی و محیطی سیستم‌های اطلاعاتی
    - ✓ تمرین روز اول:
1. شناسایی الزامات و نیازمندی‌های کلیدی امنیت اطلاعات در سازمان خودتان

## 2. مدیریت مخاطرات امنیتی نیازمندی‌های تمرین اول

### 2- روز دوم

- معرفی استانداردها و به‌روش‌های موجود در حوزه مدیریت راهبردی امنیت اطلاعات
- راهبردهای طراحی و پیاده‌سازی کنترل‌های امنیتی در سازمان
  - راهبردهای کنشی امنیت اطلاعات
  - راهبردهای واکنشی امنیت اطلاعات
  - راهبردهای مبتنی بر بلوغ امنیت اطلاعات سازمانی
  - راهبردهای مبتنی بر استانداردهای امنیتی
  - راهبردهای معرفی شده در چارچوب‌های امنیتی
  - راهبردهای مبتنی بر بهترین شیوه‌های اجرایی
- چگونگی تطبیق و بررسی انطباق کنترل‌های امنیتی پیاده‌سازی شده در سازمان با استانداردهای امنیت اطلاعات
- اصول مستندسازی در امنیت اطلاعات راهبردی
  - مستندات الزامی امنیت اطلاعات
  - استانداردهای مستندسازی امنیت اطلاعات
  - نکات قابل توجه در مستندسازی امنیتی
  - روش‌های نسخه‌گذاری مستندات امنیتی
  - اصول به روز رسانی مستندات امنیتی
- اصول تدوین برنامه پاسخدهی به حوادث امنیت اطلاعات
  - انواع روش‌های پاسخدهی به حوادث امنیتی
  - نحوه تدوین طرح پاسخدهی به حوادث امنیتی
  - نحوه تعیین اقدامات لازم در خصوص پاسخگویی فوری به حوادث امنیتی
  - نحوه تعیین اقدامات لازم در خصوص پاسخگویی ثانویه به حوادث امنیتی
  - نحوه تعیین اقدامات لازم در خصوص پاسخگویی‌ها با موقعیت‌های ویژه
  - نحوه تعیین طرح محدودسازی اثرات نامطلوب حوادث امنیتی
  - چگونگی طراحی زیرساخت‌های سازمانی مطلوب و مورد نیاز برای پاسخگویی به رویدادهای امنیتی
  - نحوه تعیین متدولوژی مناسب جهت روز آمد کردن اطلاعات رویدادهای امنیتی
  - نحوه تعیین روش تحلیل امور قانونی امنیت اطلاعات
- اصول تدوین برنامه‌های تداوم کسب و کار و بازیابی از فاجعه
  - استانداردها و بهترین شیوه‌های اجرایی تداوم کسب و کار و بازیابی از فاجعه
  - اصول مهم در تدوین برنامه‌های کسب و کار و بازیابی از فاجعه در سازمان

- چگونگی تدوین برنامه‌های مدیریت تداوم کسب و کار و بازیابی از فاجعه در سازمان
  - معرفی روش‌های اندازه‌گیری کارایی برنامه‌های تداوم کسب و کار و بازیابی از فاجعه
  - اصول تدوین خطمشی‌ها، دستورالعمل‌ها و روش‌های اجرایی امنیت اطلاعات در سازمان
    - چگونگی تدوین خطمشی‌ها، دستورالعمل‌ها و روش‌های اجرایی امنیت اطلاعات
    - بررسی تفاوت هر یک از این اسناد با یکدیگر
    - چگونگی سنجش اثربخشی این اسناد
    - نحوه بازنگری این اسناد
    - معرفی منابع و وبگاه‌های اسناد از قبل تدوین شده
  - اصول طراحی و اجرای برنامه‌های آموزشی و آگاهی‌رسانی امنیتی
    - ✓ تمرین روز دوم
1. تدوین یک خطمشی امنیتی برای سازمان خودتان، در حوزه مشخص شده

#### ویژگی‌های دوره :

✓ امکان صدور گواهینامه معتبر حضور در دوره آموزشی