# خلاصه مشخصات دوره ها یا پودمان های آموزشی

| | |
|---|---|
| ۱- **عنوان دوره:** مدیریت امنیت اطلاعات | ۲- **کد دوره:** ۷۰۸۹ |

۳- **اهداف رفتاری دوره (توانایی شرکت‌کنندگان پس از شرکت در دوره) :**

پایه‌گذاری، پیاده‌سازی، بهره‌برداری، نظارت، پاربینی، نگهداری و بهبود امنیت اطلاعات

| | |
|---|---|
| ۴- **مدت آموزش به ساعت:** ۲۰ساعت نظری: ۲۰ ساعت عملی: ۰ ساعت | ۵- نوع آموزش: الزامی ☐ اختیاری ☐ اقتضایی ☐ |
| ۶- **گروه آموزشی:** | ۷- **حیطه/رشته:** |

۸- **سطح دوره:** ☐ مهارتی ☐ تخصصی ☒ تخصصی - پژوهشی

۹- **سرفصل‌های آموزش :**

۱- تشریح الزامات، مستندسازی و پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS)

۱-۱- معرفی اصول، مفاهیم و الزامات سیستم مدیریت امنیت اطلاعات

۱-۲- مستندات و سوابق سیستم مدیریت امنیت اطلاعات

۱-۳- آشنایی با مفهوم فرآیند و دیدگاه فرآیندگرا و چرخه PDCA

۱-۴- معرفی و تشریح فازهای پروژه پیاده‌سازی ISMS

۱-۵- نحوه آنالیز شکاف (Gap Analysis) سازمان کارفرما و شناخت اولیه

۱-۶- تعیین و تدوین دامنه سیستم مدیریت امنیت اطلاعات

۱-۷- تهیه و تدوین خط‌مشی امنیت اطلاعات

۱-۸- انتخاب متدولوژی شناسایی و مدیریت مخاطرات امنیت اطلاعات

۱-۹- مدیریت حوادث امنیتی و مدیریت تداوم کسب‌وکار (BCM)

۲- ممیزی سیستم مدیریت امنیت اطلاعات

۲-۱- معرفی واژگان و تعاریف ممیزی

۲-۲- آشنایی با فرآیند ممیزی داخلی امنیت اطلاعات

۲-۳- ممیزی بهبود مستمر

۲-۴- نکات قابل‌توجه در فرآیند اخذ گواهینامه سیستم مدیریت امنیت اطلاعات

۳- مدیریت ریسک امنیت اطلاعات

۳-۱- آشنایی با مفهوم ریسک، آسیب‌پذیری، آسیب و مدیریت ریسک امنیت اطلاعات

۳-۲- اهداف و مزایای مدیریت مخاطرات در سازمان

۳-۳- بررسی انواع متدولوژی‌ها و ابزارهای ارزیابی مخاطرات

۳-۴- فرآیند مدیریت مخاطرات امنیت اطلاعات

۳-۵- نحوه تدوین طرح برطرف سازی مخاطرات- Risk Treatment Plan

۳-۶- بررسی محدودیت کاهش مخاطرات

۳-۷- آشنایی با مفهوم بازگشت سرمایه امنیتی و ROSI

۳-۸- نقش‌ها و مسئولیت‌های سازمان در فرآیند مدیریت مخاطرات

۴- مدل بلوغ مدیریت امنیت اطلاعات

۴-۱- مفهوم بلوغ مدیریت امنیت اطلاعات

۴-۲- آشنایی با فرآیندها و معیارهای امنیت اطلاعات

۴-۳- سطوح بلوغ امنیت اطلاعات

۴-۴- شناسایی شاخص‌های سنجش میزان بلوغ امنیت اطلاعات

۴-۵- افراد و مسئولیت‌های اندازه‌گیری بلوغ امنیت اطلاعات

۴-۶- مدل فرآیندی بلوغ مدیریت امنیت اطلاعات

۴-۷- متد مدیریت ریسک ISM۳

۴-۸- نقش مدیریت استراتژیک، تاکتیکی و عملیاتی در ارتقاء بلوغ امنیت اطلاعات

۵- اندازه‌گیری اثربخشی امنیت اطلاعات

۵-۱- تعریف و اهداف اندازه‌گیری امنیت اطلاعات

۵-۲- مزایای اندازه‌گیری اثربخشی امنیت در سازمان

۵-۳- ورودی‌ها و خروجی‌های اندازه‌گیری در چرخه سیستم مدیریت امنیت اطلاعات PDCA

۵-۴- گام‌های فرآیند اندازه‌گیری امنیت

۵-۵- افراد و بخش‌های درگیر در اندازه‌گیری امنیت و مسئولیت آن‌ها

۵-۶- مدل اندازه‌گیری امنیت اطلاعات

۵-۷- انواع معیارها و مشخصه‌های اندازه‌گیری

۸-۵- ارزیابی و بهبود برنامه اندازه‌گیری امنیت اطلاعات

۶- تشریح الزامات مدیریت حوادث امنیت اطلاعات و سازمان‌دهی تیم پاسخگویی به رخدادهای امنیتی رایانه (CERT)

۶-۱- آشنایی با مفاهیم و واژگان مرتبط با حوادث امنیت اطلاعات

۶-۲- مثال‌هایی از حوادث امنیت اطلاعات

۶-۳ فازها و مراحل مدیریت حوادث امنیت اطلاعات طبق استاندارد ISO/IEC۲۷۰۳۵

۶-۴- مراحل راه‌اندازی CERT/CSIRT

۶-۵- افراد و وظایف تیم پاسخگویی به حوادث امنیتی و رایانه‌ای

۶-۶- چرخه عمر رسیدگی به حادثه

۶-۷- فعالیت‌های فاز طراحی و آماده‌سازی واکنش به رخدادها و حوادث امنیتی و رایانه‌ای

۶-۸- فعالیت‌های فاز شناسایی و گزارش دهی حوادث امنیتی و رایانه‌ای

۶-۹- فعالیت‌های فاز ارزیابی و تصمیم‌گیری حوادث امنیتی و رایانه‌ای

۶-۱۰- فعالیت‌های فاز پاسخگویی به حوادث امنیتی و رایانه‌ای

۷- آشنایی با مفاهیم مرکز عملیات امنیت (SOC)

۷-۱- آشنایی با مفاهیم مرکز عملیات امنیت – SOC

۷-۲- انواع مرکز عملیات امنیت

۷-۳- جایگاه مرکز عملیات امنیت و کارکردهای مورد انتظار

۷-۴- اجزاء اصلی و فرعی یک مرکز عملیات امنیت

۷-۵- فرآیندهای مؤثر در مرکز عملیات امنیت

۷-۶- نحوه راه‌اندازی مرکز عملیات امنیت و فعالیت‌ها و اقدامات مربوطه

۷-۷- مزایای پیاده سازی یک مرکز عملیات امنیت مؤثر

۷-۸- ابزارهای کاربردی در مرکز عملیات امنیت

۷-۹- راهبری مرز عملیات امنیت

۷-۱۰- مدل‌های پیاده‌سازی مرکز عملیات امنیت

۷-۱۱- بررسی چند نمونه کاربردی

۱۰- **شیوه اجرا و ارایه آموزش:**

- حضوری: ☐کلاس درس ☐کارگاه آموزشی ☐ سمینار ☐ بحث گروهی ☐ مطالعه موردی سایر.....
- غیرحضوری: ☐ مکاتبه ای ☐ الکترونیکی سایر.....

۱۱- **شیوه ارزشیابی:**

☐کتبی ☐ شفاهی ☐ عملی
سایر.....

۱۲- **مجریان آموزش:**

۱۳- **منابع پیشنهادی آموزشی:**

کتاب های آموزشی (CISSP professional Certified Information Systems Security