مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

CISM

Certified Information Security Manager

مدت(ساعت): ۳۰ | **پیش نیاز:** مبانی امنیت | **اعتبار دهنده:** ISACA

معرفی دوره :

با توجه به محتوای دوره که مطابق با دوره رسمی اعتباردهنده می باشد گذراندن آن برای کلیه مدیران ارشد امنیت اطلاعات لازم و حیاتی می باشد.

در برخی سازمانها با توجه به ساختار سازمانی امنیت نیاز است مدیر ارشد امنیت اطلاعات علاوه بر دانش مدیریت امنیت اطلاعات ،دانش فنی در حوزه امنیت اطلاعات را نیز در حد بالایی داشته باشد که لازم است بنا به میزان نزدیکی ایشان به حوزه فنی، دوره های مدیریتی- فنی مربوطه نظیر CISSP یا SANS 414 MGT بگذرانند . در هر صورت گذراندن دوره CISM برای کلیه مدیران ارشد امنیت اطلاعات واجب و ضروری است.

امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
  - مجوز از اداره کل نظام مدیریت امنیت اطلاعات (نما)
  - سازمان مدیریت و برنامه ریزی کشور (معاونت توسعه مدیریت و سرمایه انسانی رئیس جمهوری سابق)
  - شورای عالی انفورماتیک
  - قابلیت ترجمه وتایید قوه قضاییه وامور خارجه
- بهره گیری از لابراتوارسخت افزاری ونرم افزاری مجهز
- بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه‌های ملی

اهداف دوره :

- ارزیابی و مدیریت ریسک کلان
- ارزیابی استراتژیک امنیت سازمان
- تربیت مدیر ارشد امنیت اطلاعات
- مدیریت حادثه و بحرانهای امنیت اطلاعات
- تعیین و پیاده سازی ساختار سازمانی امنیت
- تعیین اهداف امنیتی کلان سازمان و تهیه نقشه راه
- فرهنگ سازی حکمرانی امنیت اطلاعات در سازمانها
- آشنایی با برنامه های تداوم کسب و کار و بازسازی پس از فاجعه
- ساختارمند نمودن دانش های امنیتی قبلی در حوزه مدیریت امنیت اطلاعات
- استاندارد و همگن نمودن دانش مدیریت امنیت اطلاعات مدیران امنیت اطلاعات در کشور

مخاطبان دوره :

- مدیران ارشد، مدیران و کارشناسان امنیت، شبکه و فناوری اطلاعات
- مدیران حراست سازمانها و ارگانها

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، ۸ فاکس: ۸۸۰۶۵۲۲۲

Course Outline :	محتوای دوره :

Information Security Governance

- Business Goals and Objectives
- Roles and Responsibilities of senior management
- Roles and Responsibilities in Information security
- Business model for information security
- Information security Governance metrics
- Developing an Information Security Metrics
- Information security strategy objective
- Determine current state of security
- Strategy Resources
- Enterprise information security Architecture
- Compliance Enforcement
- Business Impact Assessment
- Strategy constraints
- Action plan to Implement strategy

Information Risk Management

- Risk management strategy
- Effective Information security risk Analysis
- Information security risk management
- Information resources validation
- Recovery time objectives
- Security control baselines

Information Security Program Development and Management

- Information Security Program Concept and Objectives
- Scope and charter of an Information Security Program
- Information Security management framework
- Defining an information security program Road Map
- Information security Infrastructure and architecture
- Security program management and administrative activities
- Security program services and operational activates
- Information liaison responsibility
- Due Diligence
- Controls and counter measures
- Security Program Metrics and Monitoring

Incident Management and Response

- Incident management Procedures ,organization, Resources
- Incident management Objectives
- Incident management metrics and Indicators
- Current state of Incident response capabilities
- Developing an Incident response plan
- Business continuity and disaster recovery Procedures
- Testing Incident Response plan
- Post incident Activities and investigation

Accredited by CARRIER DIGIT Computer Software LLC
EC-Council
تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، ۸ فاکس: ۸۸۰۶۵۲۲۲