



CISM

Certified Information Security Manager



اهداف دوره:

مقدمه

- establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations.
- identify and manage information security risks to achieve business objectives.
- create a program to implement the information security strategy.
- implement an information security program.
- oversee and direct information security activities to execute the information security program.
- plan, develop, and manage capabilities to detect, respond to, and recover from information security incidents.

CISM (Certified Information Security Manager) با هدف توسعه و مدیریت inforsec تمرکز بر دانش مدیریت ریسک به عنوان پایه و اساس امنیت اطلاعات تمرکز دارد. 4 محور اصلی "حاکمیت فناوری اطلاعات" و "مدیریت ریسک" و "تدوین برنامه امنیت اطلاعات" و "مدیریت حوادث امنیت اطلاعات" از جمله مباحثی اصلی هستند که در CISM مورد بحث و ارائه قرار می گیرند. این مفهوم توسط انجمن جهانی ISACA آمریکا مورد ارائه قرار گرفته است تا کمک نماید انگیزه های مربوطه به امنیت اطلاعات از نقطه نظر کسب و کار نیز درک شده و صرفاً توجه به امنیت از جنبه نقطه نظرات فنی و امور مرتبط با زیر ساخت نبوده است.

CISM

Certified

Information Security Manager

تیم مدیریتی IT House از سال ۱۳۸۷ به صورت جدی به منظور ارائه خدمات مشاوره ای و آموزشی در حوزه ی چارچوب های مدیریتی فناوری اطلاعات پا به عرصه ی ظهور گذاشت. این گروه در ابتدا تحت نام های تجاری دیگری همچون NIS ICT شروع به فعالیت نموده که در سال ۱۳۹۸ به منظور ارائه ی خدمات جدید و متفاوت برند IT House را ایجاد نموده اند. IT House با اتکا به توانمندی نیروهای متخصص داخلی و همچنین حمایت شبکه ای گسترده از شرکای بین المللی، همچون گذشته آمادگی دارد سبد کاملی از خدمات مورد نیاز سازمان ها را در حوزه های استاندارد ها و چارچوب های مدیریت فناوری اطلاعات و امنیت اطلاعات، ارائه نماید. حوزه های اصلی فعالیت این شرکت چارچوب ها و استانداردها و به روش های مدیریتی فناوری اطلاعات از جمله و نه محدود به موارد مندرج در دیاگرام های ذیل است که در هر یک از چارچوب های درج شده خدمات مرتبط با:

- آموزش
 - مشاوره
 - نرم افزار
 - ممیزی و صدور گواهی نامه
 - ارزیابی
- بسته به نوع محصول، ارائه می شود.

مخاطبان دوره

- مدیران فناوری اطلاعات
- مدیران و کارشناسان امنیت اطلاعات
- حسابرسان فناوری اطلاعات

مدت زمان دوره

5 روز (40 ساعت) - حضوری
30 ساعت آنلاین

سرفصل های دوره

- Information Security Governance — Resources That Help
- Information Security Governance — Constraints That Hurt
- Information Security Governance — The Action Plan
- Information Security Governance — Metrics and Monitoring
- Information Security Governance — What Success Looks Like
- Information Risk Management — Overview
- Information Risk Management — The Goal
- Information Risk Management — The Strategy
- Information Risk Management — Who Does What
- Information Risk Management — Resources That Help
- Information Risk Management — Constraints That Hurt
- Information Risk Management — The Action Plan
- Information Risk Management — Metrics, Monitoring, and Reporting
- Information Risk Management — What Success Looks Like
- Information Security Program Development and Management — Overview
- Information Security Program Development and Management — The Goal
- Information Security Program Development and Management — The Strategy
- Information Security Program Development and Management — Who Does What
- Information Security Program Development and Management — Resources That Help
- Information Security Program Development and Management — Constraints That Hurt
- Information Security Program Development and Management — The Action Plan
- Information Security Program Development and Management — Metrics and Monitoring
- Information Security Program Development and Management — What Success Looks Like
- Information Security Incident Management — Overview
- Information Security Incident Management — The Goal
- Information Security Incident Management — The Strategy
- Security Concepts
- Governance, Goals, Strategies, Policies, Standards, and Procedures
- Strategy
- Risk Appetite, Tolerance, and Capacity
- Analysis of Risk
- Controlling Threats and Risk
- Controls and Countermeasures
- ALE, RTO, RPO, SDO, MTO, MTD, and AIW
- BCP, DRP, and BIA
- Business Continuity and Disaster Recovery
- Testing Incident Response, Business Continuity Plans, and Disaster Recovery Plans
- Roles, Responsibilities, RACI, and Skills
- Due Diligence and Due Care
- Security Principles
- KGIs, KPIs, KRIs, and CSFs
- Technologies
- Standards and Frameworks
- Culture
- Metrics
- Current State, Desired State, and the Gap in Between
- Information Security Infrastructure and Architecture
- Cloud Computing
- Metrics Development
- Business Model for Information Security (BMIS)
- Information Security Governance — Overview
- Information Security Governance — The Goal
- Information Security Governance — The Strategy
- Information Security Governance — Who Does What

پیش نیازهای دوره

پیش نیاز ضروری برای این دوره ی آموزشی وجود ندارد، اشنایی اولیه با مفاهیم امنیت اطلاعات مورد نیاز می باشد.

درباره ی مدرک

به شرکت کنندگان در این دوره ی آموزشی گواهی حضور از سوی موسسه ITHOUSE اعطا خواهد شد.

- Information Security Incident Management — Who Does What
- Information Security Incident Management — Resources That Help
- Information Security Incident Management — Constraints That Hurt
- Information Security Incident Management — The Action Plan
- Information Security Incident Management — Metrics and Monitoring
- Information Security Incident Management — What Success Looks Like



تماس با IT HOUSE

آدرس:

تهران، سهروردی شمالی، کوچه تهمت، پلاک 6 واحد 7

تلفن:

+ 98 (0) 21 88731466

فکس:

+ 98 (0) 21 86031447

وبسایت:

www.it-house.me

ایمیل:

info@it-house.me