Projacs
an egis company
بروجاكس للتدريب والتطوير
Projacs Training and Development

Information Security Risk Management

إدارة أمن وسلامة تكنولوجيا المعلومات

24 – 28 August 2020

Kuala Lumpur / Malaysia

A Member of:
PROJACS ACADEMY

ProjacsAcademy.com

Introduction

An overview of activities, methods, methodologies, and procedures related to establishing sound information security policies

The purpose of the course is to provide the attendees with an overview of the field of Information Security from a management perspective. Students will be exposed to the spectrum of security activities, methods, methodologies, and procedures. Coverage will include inspection and protection of information assets, the management of risk, the detection of and reaction to threats to information assets, and an overview of the Information Security Planning and staffing functions.

Objectives

At the end of the course the attendees will be able to:

1. Identify and prioritize information assets
2. Identify and prioritize threats to information assets
3. Define an information security strategy and architecture
4. Define risk management and its role in the organization
5. Plan for and respond to intruders in an information system
6. Present a disaster recovery plan for recovery of information assets after an incident
7. Apply project management principles to an information security program.

Who Should Attend?

IT managers and directors, IT staff, IT security team.

Course Outlines

DAY 1:

- Pre-exam assessment
- Information security concepts
- Align Information Security Strategy with Corporate Governance
- Identify Legal and Regulatory Requirements
- Justify Investment in Information Security
- Obtain Senior Management Commitment to Information Security
- Define Roles and Responsibilities for Information Security
- Establish Reporting and Communication Channels

DAY 2:

- Implement an Information Risk Assessment Process
- Determine Information Asset Classification and Ownership
- Conduct Ongoing Threat and Vulnerability Evaluations
- Identify and Evaluate Risk Mitigation Strategies
- Integrate Risk Management into Business Life Cycle Processes
- Report Changes in Information Risk

DAY 3:

- Information Security plan
- Security Technologies and Controls
- Coordinate Information Security Programs with Business Assurance Functions
- Estimate required resources
- Develop Information Security Architectures and policies
- Information Security Policies documentation

DAY 4:

- Manage Information Security Resources
- Enforce Information Security During Systems Development
- Maintain Information Security Within an Organization
- What is Information Security Advice and Guidance?
- What is Information Security Awareness and Training?
- Resolve Noncompliance Issues

DAY 5:

- Information Security Incident Response strategy
- Escalation Process
- Information security communication plan
- How to Manage Responses to Information Security Incidents
- Information Security Incident Investigation
- Post-exam assessment

Training Method

- Pre-assessment
- Live group instruction
- Use of real-world examples, case studies and exercises
- Interactive participation and discussion
- Power point presentation, LCD and flip chart
- Group activities and tests
- slides and handouts
- Post-assessment

Program Support

This program is supported by interactive discussions, role-play, case studies and highlight the techniques available to the participants.

Schedule

The course agenda will be as follows:

- Technical Session 08.30-10.00 am
- Coffee Break 10.00-10.15 am
- Technical Session 10.15-12.15 noon
- Coffee Break 12.15-12.45 pm
- Technical Session 12.45-02.30 pm
- Course Ends 02.30 pm

Course Fees*

- **3,250 USD**
  **VAT is Excluded If Applicable*

مقدمة

الغرض من هذه الدورة هو تزويد المشاركين بنظرة عامة عن مجال أمن المعلومات من منظور الإدارة. سوف يتعرض الطلاب لطيف من الأنشطة الأمنية والأساليب والمنهجيات، والإجراءات. وستشمل التغطية التفتيش وحماية أصول المعلومات، وإدارة المخاطر، والكشف عن التهديدات التي يتعرض لها أصول المعلومات، ونظرة عامة عن التخطيط لأمن المعلومات ووظائف الموظفين.

الاهداف

في نهاية الدورة الحضور سوف يكون قادرا على:

- تحديد ووضع أولويات أصول المعلومات
- تحديد ووضع أولويات التهديدات التي يتعرض لها أصول المعلومات
- تحديد استراتيجية أمن المعلومات
- تعريف إدارة المخاطر ودورها في المؤسسه
- التخطيط و الرد على المتسللين في نظام المعلومات
- تقديم خطة التعافي من الكوارث لاسترداد أصول المعلومات
- تطبيق مبادئ إدارة المشاريع لبرنامج أمن المعلومات.

الحضور

مديري تكنولوجيا المعلومات ومديري وموظفي تكنولوجيا المعلومات، الفريق الأمني

المحاور

اليوم الأول
- تقييم ما قبل الامتحان
- مفاهيم أمن المعلومات
- محاذاة استراتيجية أمن المعلومات مع حوكمة الشركات
- تحديد المتطلبات القانونية والتنظيمية
- ضبط الاستثمار في أمن المعلومات
- الحصول على التزام الإدارة العليا لأمن المعلومات
- تحديد الأدوار والمسؤوليات لأمن المعلومات
- إنشاء قنوات للتقارير والاتصالات

اليوم الثانى
- تنفيذ عملية تقييم المخاطر
- تحديد معلومات تصنيف الأصول والملكية
- تقييمات التهديد المستمر والضعف
- تحديد وتقييم استراتيجيات تخفيف المخاطر
- إدراج إدارة المخاطر في عمليات المؤسسه
- اعداد تقارير التغير فى مخاطر المعلومات

اليوم الثالث
- خطة أمن المعلومات
- تقنيات الأمن والتحكم
- تنسيق برامج أمن المعلومات مع وظائف ضمان و توكيد أعمال المؤسسه
- تقدير الموارد المطلوبة
- تطوير البنى وسياسات أمن المعلومات
- وثائق سياسات أمن المعلومات

اليوم الرابع
- إدارة موارد أمن المعلومات
- فرض أمن المعلومات خلال تطوير النظم
- الحفاظ على أمن المعلومات داخل المنظمة
- ما هي الارشادات الخاصه بأمن المعلومات ؟
- الوعي والتدريب بأمن المعلومات
- قضايا عدم التطابق

اليوم الخامس

- استراتيجية التعامل مع حوادث أمن المعلومات
- دور الادارات العليا فى خطه امن المعلومات
- خطة اتصالات أمن المعلومات
- التحقيق في حوادث أمن المعلومات
- امتحان نهايه الدورة