



IT AUDIT/IS



مقدمه

- آشنایی با ریسک ها و کنترل های فناوری اطلاعات
- توانایی طرح ریزی و اجرای حسابرسی فناوری اطلاعات

مخاطبان دوره:

این دوره برای تمامی افراد ذیل جذاب می باشد.
این افراد شامل موارد ذیل هستند:

- مدیران ارشد
- تحلیل گران
- مدیران فناوری اطلاعات
- مدیران طرح و برنامه
- مدیران حسابرسی داخلی

مدت زمان دوره:

3 روز (24 ساعت)

سرفصل های دوره:

1-Introduction

- 1.1. Trainers
- 1.2. Purpose of this course and applicability
- 1.3. Audience

امروزه فناوری اطلاعات یکی از توانمندسازهای کلیدی برای سازمان ها به شمار می آید و ارائه اکثر خدمات و اغلب محصولات بدون استفاده از این فناوری قابل تصور نیست. این فناوری گرچه فرصت های بیشماری برای صنایع به همراه دارد، لیکن تهدیدها و آسیب پذیری هایی را نیز ممکن است متوجه آنان نموده است. مدیریت موثر این تهدیدها مستلزم طراحی و اجرای موثر فرآیند مدیریت ریسک فناوری اطلاعات است. از سوی دیگر باید اطمینان حاصل شود که سرمایه گذاری های صورت گرفته در حوزه فناوری اطلاعات به نحو موثر برای سازمان ها اثربخشی به همراه داشته است. براین اساس حسابرسی فناوری اطلاعات یکی از ابعاد کلیدی حسابرسی داخلی است که اثربخشی فرآیندهای مدیریت ریسک فناوری اطلاعات را بررسی نموده، کارایی و اثربخشی و میزان تطابق فناوری اطلاعات با قوانین و مقررات را تضمین خواهد نمود.

اهداف دوره

- آشنایی با مفاهیم حسابرسی فناوری اطلاعات
- شناخت چارچوب های کلیدی برای حسابرسی فناوری اطلاعات

IT AUDIT/IS Foundation

5.3.3. Implementing an Awareness and Training Program

5.4. Post-Implementation

5.4.1. Monitoring Compliance

5.4.2. Evaluation and Feedback

5.5. Managing Change

5.6. Program Success Indicators

5.7. Incident Management

6-Performance Measures and SLA (internal / vendor)

6.1. Metric Types

6.2. Metrics Development and Implementation Approach

6.3. Metrics Program Implementation

7-Information Technology Contingency Planning

7.1. Step 1: Develop Contingency Planning Policy Statement

7.2. Step 2: Conduct Business Impact Analysis

7.3. Step 3: Identify Preventive Controls

7.4. Step 4: Develop Recovery Strategies

7.5. Step 5: Develop IT Contingency Plan

7.6. Step 6: Plan Testing, Training, and Exercises

7.7. Step 7: Plan Maintenance

8-Risk Management

8.1. Risk Assessment

8.1.1. Step 1 – System Characterization

8.1.2. Step 2 – Threat Identification

8.1.3. Step 3 – Vulnerability Identification

8.1.4. Step 4 – Risk Analysis

8.1.4.1. Control Analysis

8.1.4.2. Likelihood Determination

8.1.4.3. Impact Analysis

8.1.4.4. Risk Determination

8.1.5. Step 5 – Control Recommendations

8.1.6. Step 6 – Results Documentation

8.2. Risk Mitigation

8.3. Evaluation and Assessment

9-Security Violations

10-Incident Response

10.1. Preparation

10.1.1.

1.4. Internal Audit in the Organizational Structure

1.5. Auditors' Authorities

1.6. A sample best practice:

2-Information Systems Governance

2.1. Information Systems Governance Components

2.1.1. Information Systems Strategic Planning

2.1.2. Information Systems Governance Structures

2.1.3. Key Governance Roles and Responsibilities

2.1.4. Information Systems Committees

2.1.5. Information Systems Policy and Guidance

2.1.6. Documentation

2.1.7. Ongoing Monitoring

2.2. Information Systems Governance Challenges and Keys to Success

3-Portfolios, Projects, and Operations

4-System Development Life Cycle

4.1. Initiation Phase

4.2. Development/Acquisition Phase

4.3. Implementation Phase

4.4. Operations/Maintenance Phase

4.5. Disposal Phase

4.6. Security Activities within the SDLC

5-Awareness and Training

5.1. Awareness and Training Policy

5.2. Components: Awareness, Training, Education, and Certification

5.2.1. Awareness

5.2.2. Training

5.2.3. Education

5.2.4. Certification

5.3. Designing, Developing, and Implementing an Awareness and Training Program

5.3.1. Designing an Awareness and Training Program

5.3.2. Developing an Awareness and Training Program

تیم مدیریتی IT House از سال ۱۳۸۷ به صورت جدی به منظور ارائه خدمات مشاوره‌ای و آموزشی در حوزه‌ی چارچوب‌های مدیریتی فناوری اطلاعات پا به عرصه‌ی ظهور گذاشت. این گروه در ابتدا تحت نام‌های تجاری دیگری همچون NIS ICT شروع به فعالیت نموده که در سال ۱۳۹۸ به منظور ارائه خدمات جدید و متفاوت برند IT House را ایجاد نموده‌اند. با اتکا به توانمندی نیروهای متخصص داخلی و هم‌منظور حمایت شبکه‌ای گسترده از شرکای بین‌المللی، همچون گذشته آمادگی دارد سبد کاملی از خدمات مورد نیاز سازمان‌ها را در حوزه‌های استانداردها و چارچوب‌های مدیریت فناوری اطلاعات و امنیت اطلاعات، ارائه نماید. حوزه‌های اصلی فعالیت این شرکت چارچوب‌ها و استانداردها و به‌روش‌های مدیریتی فناوری اطلاعات از جمله و نه محدود به موارد مندرج در دیاگرام‌های ذیل است که در هر یک از چارچوب‌های درج شده خدمات مرتبط با:

- آموزش
 - مشاوره
 - نرم‌افزار
 - ممیزی و صدور گواهینامه
 - ارزیابی
- بسته به نوع محصول، ارائه می‌شود.

- 16.1.2. Credentials Propagation
- 16.1.3. Levels of Access
 - 16.1.3.1. View of Pages
 - 16.1.3.2. View/ Edit/ Delete of Categories
 - 16.1.3.3. View/ Edit/ Delete of Sub-Categories
- 16.1.4. Requesting Access
- 16.1.5. Access Review
- 16.1.6. Access Revoke
- 16.2. Code Hardening
- 16.3. Maintenance
 - 16.3.1. Versioning
 - 16.3.2. Patch
 - 16.3.3. User Friendly Design

17-Operating Systems controls

- 17.1. Access Management
 - 17.1.1. Responsibilities of Access Grantors
 - 17.1.2. Credentials Propagation
 - 17.1.3. Levels of Access
 - 17.1.3.1. Level
 - 17.1.3.1.1. Intranet
 - 17.1.3.1.1.1. Domains
 - 17.1.3.1.1.2. Work groups
 - 17.1.3.1.2. Internet
 - 17.1.3.1.3. USB/ CD
 - 17.1.3.1.4. Outgoing Emails
 - 17.1.3.1.5. High Level Access
 - 17.1.3.1.5.1. Local Admin
 - 17.1.3.1.5.2. Domain Admin/ Enterprise Admin
 - 17.1.3.2. Privilege
 - 17.1.3.2.1. Read
 - 17.1.3.2.2. Edit/ Update
 - 17.1.3.2.3. Delete
 - 17.1.4. Password Policy
 - 17.1.5. Remote Access
 - 17.1.6. Requesting Access
 - 17.1.7. Access Review
 - 17.1.8. Access Revoke
- 17.2. Antivirus
 - 17.2.1. In house Systems
 - 17.2.2. Temp Systems
 - 17.2.3. Vendor Systems
 - 17.2.4. gysts Systems
- 17.3. Authorized Applications
- 17.4. Patch Management
- 17.5. Audit Trails

- 10.1.2. Preparing for Incident Response
- 10.1.3. Preparing to Collect Incident Data
- 10.1.4. Preventing Incidents
- 10.2. Detection and Analysis
- 10.3. Containment, Eradication, and Recovery
- 10.4. Post-Incident Activity
- 10.5. Knowledge Management
- 10.6. SLA and Monitoring

11-Change Management

- 11.1. Change Initiation
- 11.2. Change CAB approval
- 11.3. Change Plan
- 11.4. Change Impact Analysis
- 11.5. Change Resources
- 11.6. Change Role back Plan
- 11.7. Emergency Change
- 11.8. Change Finalization
- 11.9. Retrospective Change

12-Configuration Management

- 12.1. CMDB
- 12.2. Baseline
- 12.3. Configuration Changes
- 12.4. Configuration Management Process

13-Procurement and Asset Management

14-Business Continuity Management

15-Network

- 15.1. Design
 - 15.1.1. Boundaries of the Organization Digital Structure
 - 15.1.1.1. Physical Boundaries and Security
 - 15.1.1.2. Firewall
 - 15.1.1.3. IDS/ IPS
 - 15.2. IP Ranges
 - 15.3. Access
 - 15.4. Log / Audit Trail
 - 15.5. Settings
 - 15.6. Server Room
 - 15.7. Spare Management

16-Application

- 16.1. Access Management
 - 16.1.1. Responsibilities of Access Grantors

- 20.2. Mandate
- 20.3. Auditing Process Background
- 20.4. Objectives
- 20.5. Risks and Control Criteria
- 20.6. Scope
- 20.7. Scope Exceptions
- 20.8. Review Approach
- 20.9. Reporting
- 20.10. Key Audit Team Contacts

21-Opening Meeting

- 21.1. Scope
- 21.2. Initial Documents
- 21.3. Auditee Contact People

22-Audit Plan

- 22.1. Risks
- 22.2. Best Practices
- 22.3. Actual Business Practices
- 22.4. Adequacy Check
- 22.5. Audit Test
- 22.6. Test Result
- 22.7. Residual Risk

23-Execution of testing

- 23.1. Communication
- 23.2. Info Request/ Gathering
- 23.3. Evidences
- 23.4. Analysis
 - 23.4.1. Intervals of Information
 - 23.4.2. Info generators vs Info users
 - 23.4.3. Analysis Tools
- 23.5. Involvement of Managers
- 23.6. Test Result Documentation
 - 23.6.1. Completeness and accuracy
 - 23.6.2. Referencing and Evidence

24-Report

- 24.1. Drafting
- 24.2. Management Exit Meeting
 - 24.2.1. Describing
 - 24.2.2. Action Plan
 - 24.2.3. Scheduling
- 24.3. Higher Manager (CEO) Exit Meeting
 - 24.3.1. Describing Major Items
 - 24.3.2. Review and Confirmation of Action Plan
 - 24.3.3. Review and Confirmation of Scheduling
- 24.4. Report Finalization
- 24.5. Reporting to Board of Directors

25-Follow Up

- 17.5.1. Generation
- 17.5.2. Access
- 17.5.3. Retention
- 17.5.4. Review
- 17.6. Backup
 - 17.6.1. Generation
 - 17.6.1.1. Actual OS
 - 17.6.1.2. Virtual OS
 - 17.6.2. Test/ Restore
 - 17.6.3. Access
 - 17.6.4. Retention
 - 17.6.5. Redundancy
- 17.7. Services
- 17.8. File Sharing
 - 17.8.1. Folders
 - 17.8.2. SharePoint

18-Database Controls

- 18.1. Access Management
 - 18.1.1. Responsibilities of Access Grantors
 - 18.1.2. Credentials Propagation
 - 18.1.3. Levels of Access
 - 18.1.3.1. Login / Account/ Database
 - 18.1.3.2. Privilege
 - 18.1.3.2.1. Read
 - 18.1.3.2.2. Edit/ Update
 - 18.1.3.2.3. Delete
 - 18.1.4. Password Policy
 - 18.1.5. Requesting Access
 - 18.1.6. Access Review
 - 18.1.7. Access Revoke
- 18.2. Database in the Domain
- 18.3. Patch Management
- 18.4. Audit Trails
 - 18.4.1. Generation
 - 18.4.2. Access
 - 18.4.3. Retention
 - 18.4.4. Review
- 18.5. Backup
 - 18.5.1. Generation
 - 18.5.1.1. Actual OS
 - 18.5.1.2. Virtual OS
 - 18.5.2. Test/ Restore
 - 18.5.3. Access
 - 18.5.4. Retention
 - 18.5.5. Redundancy

19-Sources of Data/ Raw Data

20-APM

- 20.1. RACI

پیش نیازهای دوره

آشنایی اولیه با مفاهیم ممیزی مبتنی بر استاندارد
ISO 19011 و همچنین حاکمیت شرکتی و فناوری
اطلاعات مبتنی بر چارچوب های COBIT & COSO
نیاز می باشد.

تعداد شرکت کنندگان

6 الی 20 نفر

درباره ی مدرک

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

تماس با IT HOUSE

آدرس:

تهران، سهروردی شمالی، کوچه تهمتن، ساختمان مهرگان،
پلاک 6 واحد 7

تلفن:

+ 98 (0) 21 88731466

فکس:

+ 98 (0) 21 186031447

وبسایت:

www.it-house.me

ایمیل:

info@it-house.me