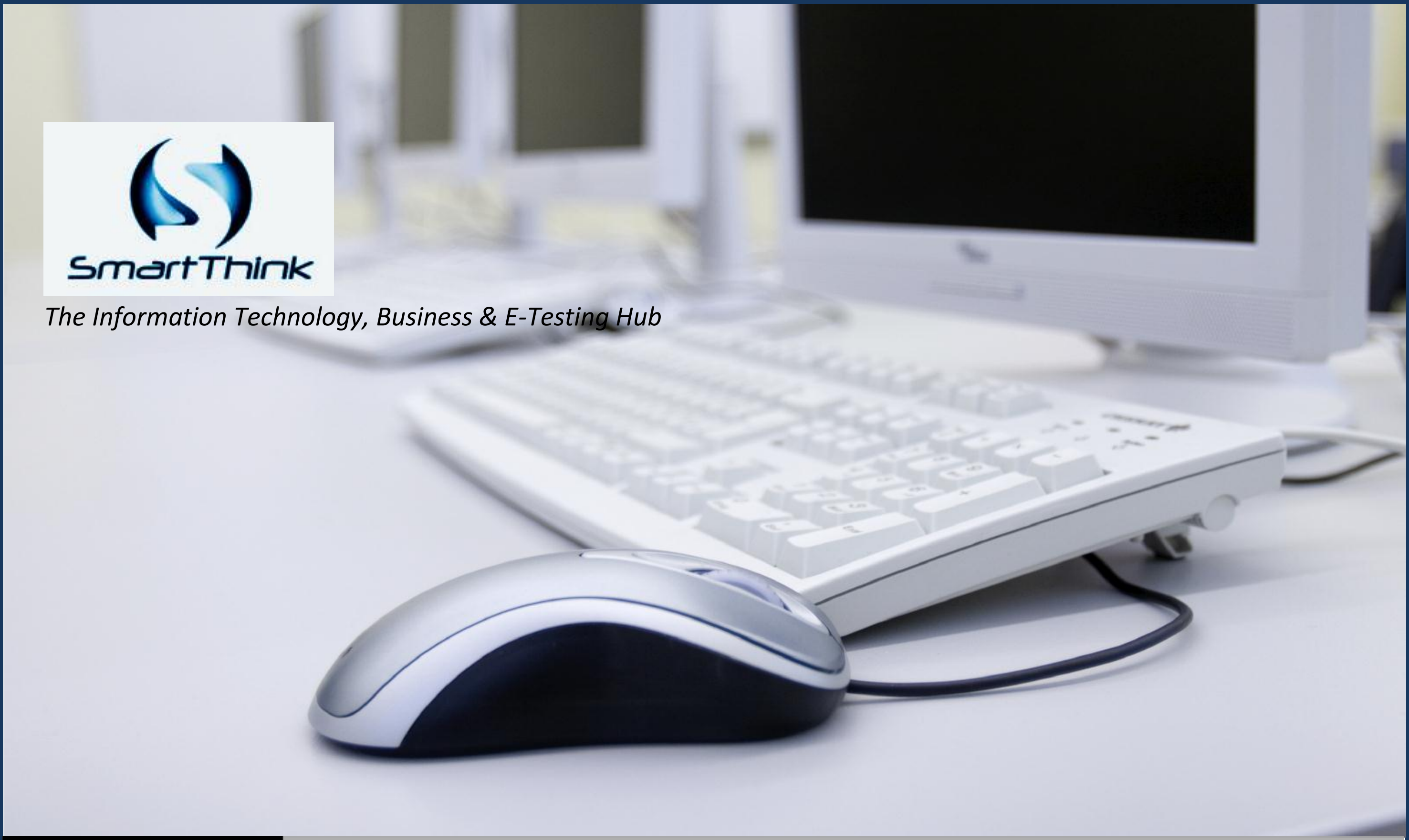

SmartThink

The Information Technology, Business & E-Testing Hub

SMARTTHINK
LIMITED

TRAINING BROCHURE

SMARTTHINK LTD
T: 917-341-3283
E: infous@smartthink.co.uk

INTRODUCTION

The IT field, specially the IT Security field has been recession free. You can check that on your own, we do not have to tell you that, however it is very easy to get in this field. IT Security Analyst/Auditor with a 1 year experience makes on average **$85,000** per year, and you verify and confirm this information on many job posting boards such as **Monster.com, Dice.com** and so on.

SMARTTHINK LTD is proud to provide IT Audit/ Security courses at their Laurel, Maryland site located at 8568 Laureldale Drive, Laurel MD 20724.

These courses will be taught by a group of IT security professionals with over 17 years of Experience in IT Audit, IT Security Compliance, IT Governance and Information Assurance in the private and public sectors. The courses are run every Saturday for 12 Saturdays, two hours per session.

Class size will be small, therefore promoting extensive interaction between instructors and students. Each participant or student will have the chance to ask as many questions as they wish and have the opportunity to interact with other students and get all the attention of the instructors. We have a tract record of students getting plenty of interview and jobs. Some of the past student will be coming through to share their experience and testimonies

We will assist with resume writing, Job search, interview preparation and other after training assistance. We will also be providing professional reference and guidance (Help you while on the job).

There is a short description of the course and please feel free to call if you have any question.

We will discuss payment and payment options on a one on one basis; we are flexible but will not bend our rules to accommodate non-Payment. We could be reached at 917-341-3283 or infous@smartthink.co.uk for additional information and registration. The seats are limited.

FISMA –A&A SOX 404 8568 LAURELDALE DRIVE, LAUREL, MD 20724

These courses provide detailed information on the NIST-FISMA A & A (C&A) documentation package, and NIST 800 security controls and SOX 404 as stated below:

A

1. **FISMA & NIST**

   - Definition
   - Applicable Laws And Regulations
   - Roles And Responsibilities
   - The NIST 800-37/ 800-39 Process
   - Introduction To Security Controls
   - Security Control Assessment
   - NIST Special Publications / NIST Baseline Security Controls.
   - Website to visit: NIST.GOV, DISA.GOV, NSA.GOV, ISACA.org, IIA.org, PCAOB.org, CIS.org, etc.

2. **A&A (C&A)**

   These are the main items to be reviewed and discussed during these sessions.
   The SA&A (C&A) Artifacts: FIPS 199, E-AUTHENTICATION, PTA, PIA, SORN, RISK ASSESMENT (RA), SYSTEM SECURITY PLAN (SSP), CONTIGENCY PLAN (DRP), CONTIGENCY PLAN TEST, ST&E, SAR, POAM, ANNUAL SELF ASSESMENT (800-53A), ATO, MOU, ISA

   - Introduction
   - C&A Documentation

- Accreditation Decisions
- Phases
- Certification Phase Activities
- Accreditation Phase Activities
- Continuous Monitoring Phase Activities
- C&A Documentation Package
- Key policies: OMB A-130, FISMA, OMB A-123, Federal Information Processing
- Standards (Example FIPS 199)
- NIST Special Publications
- NIST SA&A (C&A) Process Overview
- Roles and Responsibilities
- SA&A (C&A) Prerequisites
- Accreditation Boundaries
- System Categorization/Security Controls Selection
- System Security Plan
- Initial Risk Assessment
- Initiation Phase Activities
- System Security Plan (SSP)
- Risk Assessment Report
- Security Assessment (ST&E) Report
- Plan of Action and Milestones (POA&M) and FISMA reporting
- Transmittal and Decision Letters

Other Documents:

- Supporting Documentation
- Security Controls (NIST SP 800-53)
- Assessment Methods (NIST SP 800-53a) Security Testing Tools
- SA&A (C&A) Package

B. <u>SARBANES AND OXLEY</u>

- The Law
- Introduction To IT Audit
- IT Audit Framework: COSO/COBIT
- Key Controls IT Audit Controls
- IT General Computer Control
- Application Control
- SOX Phase
- SOX Documentation

A&A (C&A) / FISMA AND SARBANES OXLEY 404 TRAINING OVERVIEW

Compliance Solutions:

GLBA
HIPAA
PCI
SOX
SEC
FFEIC

OMB
FISMA DITSCAP
SB 1386
ISO 17799
DIACAP

A- CERTIFICATION AND ACCREDITATION (C&A) FISMA-DITSCAP-DIACAP:

OMB Circular A-130, Appendix III, requires that agencies conduct certification and accreditation SA&A (C&A)

OF Information Systems. SA&A (C&A) provides a form of quality control and challenges an agency to implement the MOS effective security controls possible in an information system. This process ensures that all aspects of security are addressed throughout the life cycle of the system. Armed with the most complete, accurate, and trustworthy information possible on the security status of a system, an agency official can make risk-based decisions on whether to authorize operation of a system within the agency. DOD Directives, DISA STIGS, NSA Guides, NITS 800 Special Publications.

Could be able to manage and/or conduct a complete certification or prepare and assess individual documents in the FINA certification package that is ultimately presented to the Certifying Agent r for approval.

Developing a security test and evaluation (ST&E) plan and test procedures Conducting an ST&E

Analyzing and reporting test results Conducting a vulnerability assessment Conducting a risk assessment

Developing a System Security Plan (SSP)

Developing a Continuity of Operations and Disaster Recovery Plan Developing a Change Management Plan
Developing the certification and accreditation package

B- INFORMATION ASSURANCE:

Will be able to successfully delivered security services and solutions to both private and public sectors. Our hands-on most critical and valuable information assurance assets security. Some of our typical hands-on security solutions include:

- Security Assessments and Audits
- FISMA Compliance and Audits
- Security Policy Development
- Security Awareness Training
- Infrastructure Security
- Incident Response

C – SARBANES OXLEY (SOX 404) COSO – COBIT FRAMEWORKS:

IT Audit Background No Pre-requisite

From the CEO and CFO to management and other key employees, many now have new roles to play as a result of SOX. This course is designed to benefit all personnel in any organization who want to learn more about internal controls and this landmark legislation. This program will arm you with the knowledge needed to understand the importance of SOX and help you better understand your role in complying with internal control requirements.

This course can be specifically tailored toward a specific audience by emphasizing certain topics and customized exercises of specific interest. Class size may vary but small numbers are encouraged.

A - Using the concepts presented, participants gain the knowledge and skills needed to:

- Compare current internal control practices to COSO's Internal Control - Integrated Framework
- Identify opportunities to enhance existing internal controls when appropriate
- Understand your role in meeting SOX internal control requirements

B- History and Background behind Sarbanes-Oxley: How recent corporate scandals have changed the way companies must behave:

- Significant Aspects of Sarbanes-Oxley: Background and Benchmarking
- Top-Down Risk Assessment -- Entity-Level Controls-- Key Controls -- Testing Approaches and Practices Monitoring and Reporting

C- PCAOB Public Accounting Oversight Board AS5/External Audit Relationships

Sarbanes-Oxley and Enterprise Risk Management and Governance Internal Audit Role

Sustaining Sarbanes-Oxley Relationship between sections 302 and 404 (Focusing more on SOX 404)

D - Understanding and Applying the COSO Internal Control - Integrated Framework:

- Control Environment: The foundation for all other elements of internal controls that sets the tone of the organization, including ethical values and competence of the company's leaders and employees. Includes:
  1. Code Of Conduct And Ethics
  2. Fraud Prevention
  3. Whistleblower Policy

- Internal Control Design and Scoping including:
  1. Significant accounts
  2. Mapping
  3. Documentation

- Risk Assessment: The identification and analysis of relevant risks that can hinder the achievement of business objectives
- Control Activities: Specific activities designed to mitigate identified risks
- Information and Communication: Information pathways between management and employees.
- Monitoring: The evaluation and assessment of internal controls including:
  1. Management Monitoring/Testing
  2. Deficiency Evaluation And Remediation
  3. External Auditor's Testing And Reporting