IntelleSecure
Information Security & Compliance
www.intellesecure.com

Governance, Risk & Compliance

- *Certified Information Systems Auditor (CISA)*
- *Certified in Risk and Information Systems Control (CRISC)*
- *Control Objectives for Information and related Technologies (COBIT)*
- *Sarbanes-Oxley Act (SOX)*
- *Attestation Standards (SAS70 - SAE16 - ISAE 3402)*
- *Payment Card Industry Data Security Standard (PCI DSS)*
- *Health Insurance Portability and Accountability Act (HIPAA)*
- *Information Technology Infrastructure Library (ITIL)*
- *Information Technology Service Management System (ISO 20000)*
- *Information Security Management System (ISO 27001)*
- *Business Continuity Management System (ISO 22301)*
- *Enterprise Risk Management (ISO 31000)*

IntelleSecure
Information Security & Compliance
www.intellesecure.com

CISA

Home

Certified Information Systems Auditor

CISA is considered the de facto standard for those interested in IS Audit as a career. CISA is to audit what a CPA or CA is to accounting. For professionals in the banking and financial industry, a CISA would add tremendous value to their resume.

ISACA (**I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation) specifies **5 job practice areas:**

- ***The Process of Auditing Information Systems***
- ***Governance and Management of IT***
- ***Information Systems Acquisition, Development, and Implementation***
- ***Information Systems Operations, Maintenance and Support***
- ***Protection of Information Assets***

Our workshop covers the 5 job practice areas specified by ISACA for CISA by explaining the various IS audit, control or security concepts with relevant examples to help participants understand the requirements from an exam perspective. A mock exam on completion helps participants prepare for the CISA exam from **ISACA**.

Prerequisite

- Five (5) years of professional IS auditing, control or security work experience with at least two (2) years of specific domain expertise on any two (2) job practice areas of CISA.
- Waiver of one (1) year if you have financial or operational auditing experience or three (3) years of college education or two (2) years as full time university instructor in computer science, accounting or IS auditing.

IntelleSecure
Information Security & Compliance
www.intellesecure.com

CISA …

Home

Suggested study material would be

- CISA Review Manual from ISACA
- CISA Prep Guide by John B Kramer

Workshop Duration: 3 days
Schedule: Training Calendar

Certification Process & Maintenance

- Minimum 20 contact hours of **CPE** (**C**ontinuing **P**rofessional **E**ducation)
- Minimum 120 contact hours of CPE during a fixed three (3) year period
- US$ 40 towards **AMF** (**A**nnual **M**aintenance **F**ee)

Examination	**CISA**
Certifying Body	ISACA (**I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation)
Exam Fee	US$ 635
Exam Duration	4 hours
Exam Type	Offline paper based (conducted twice a year in June and December)
Exam Questions	200 multiple choice
Exam Pass Score	450 (Scaled score of 450 points on a 200-800 point scale)

IntelleSecure
Information Security & Compliance
www.intellesecure.com

CRISC

Home

Certified in Risk and Information Systems Control

CRISC is considered one of the leading industry certifications which helps senior management professionals understand enterprise risk, and provides them with the technical knowledge to design, implement, monitor and maintain appropriate IS controls to mitigate such risk.

ISACA (**I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation) specifies **5 job practice areas:**

- ***Risk Identification, Assessment & Evaluation***
- ***Risk Response***
- ***Risk Monitoring***
- ***Information Systems Control Design & Implementation***
- ***IS Control Monitoring & Maintenance***

Our workshop covers the 5 job practice areas specified by ISACA for CRISC by explaining the various business risks and and appropriate IS controls with relevant examples to help participants understand the requirements from an exam perspective. A mock exam on completion helps participants prepare for the CRISC exam from **ISACA**.

Prerequisite

- Minimum of at least three (3) years of cumulative work experience performing the tasks of a CRISC professional across at least three (3) CRISC job practice areas is required for certification.
- There are no substitutions or experience waivers.

IntelleSecure
Information Security & Compliance
www.intellesecure.com

CRISC …

Home

Suggested study material would be

- CRISC Review Manual from ISACA
- CRISC Certification Study Guide by William Manning

Workshop Duration: 3 days
Schedule: Training Calendar

Certification Process & Maintenance

- Minimum 20 contact hours of **CPE** (**C**ontinuing **P**rofessional **E**ducation)
- Minimum 120 contact hours of CPE during a fixed three (3) year period
- US$ 40 towards **AMF** (**A**nnual **M**aintenance **F**ee)

Examination	**CIRISC**
Certifying Body	ISACA (**I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation)
Exam Fee	US$ 635
Exam Duration	4 hours
Exam Type	Offline paper based (conducted twice a year in June and December)
Exam Questions	200 multiple choice
Exam Pass Score	450 (Scaled score of 450 points on a 200-800 point scale)

IntelleSecure
Information Security & Compliance
www.intellesecure.com

COBIT

Home

COBIT 5

COBIT 5 provides a business framework for Governance and Management of Enterprise IT and allows managers to effectively bridge the gap between control requirements, technical issues and business risks.

ISACA (**I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation) defines the COBIT 5 framework using **5 basic principles** and **7 enablers** which cover **37 high level processes** meant primarily for governance and management of enterprise IT. Our workshop helps participants understand how to implement the COBIT framework and provide for better IT governance.

Prerequisite: Exposure to process control within the organization. Anyone aspiring to get a better understanding of the COBIT framework can also attend this workshop

Workshop Duration: 2 days

Schedule: Training Calendar

Examination	**COBIT Foundation**
Certifying Body	ISACA (**I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation)
Exam Fee	US$ 150
Exam Duration	40 minutes
Exam Type	Both online and offline paper based options
Exam Questions	50 multiple choice
Exam Pass Score	50%

IntelleSecure
Information Security & Compliance
www.intellesecure.com

SOX

Home

Sarbanes Oxley Act

Any organization listed in the US Stock Exchange has to comply with SOX - an act of legislation enacted in the US to protect investors from financial scams like Enron and World Com. This is also applicable for all subsidiaries of the listed company in other countries.

The Sarbanes Oxley Act deals mainly with more transparency in financial disclosures and better IT controls to manage and mitigate risk. Our workshop is designed to help individuals understand the basic framework of the Sarbanes Oxley Act and how it impacts today's organizations.

Participants get a better understanding

- *how to manage a SOX compliance initiative*
- *various control frameworks*
- *of the impact on IT*
- *how to use an integrated IT approach for SOX compliance*
- *on the significance of Application Controls, Business Cycles, System Interfaces*
- *of the implications on outsourcing and service providers and compliance attestation requirements*

Prerequisite: Exposure to process control either IT related or finance related within any organization.

Workshop Duration: 2 days
Schedule: Training Calendar
Examination: Not applicable since this is an act of US legislation; only organization needs to comply

IntelleSecure
Information Security & Compliance
www.intellesecure.com

SAS70 - SSAE16 - ISAE3402

Home

Attestation Standards

Compliance Attestation (**SAS70**, **SSAE16**, **ISAE3402**) is essentially the Auditor's Report on the controls at a service organization that are likely to impact internal control over financial reporting. The report typically consists of the audit opinion, the organization's description of controls, and a description of the auditor's tests of operating effectiveness.

Attestation is done by a **C**ertified **P**ublic **A**ccountant (**CPA**) as per detailed guidance on **S**ervice **O**rganization **C**ontrol (**SOC**) reporting outlined by **A**merican **I**nstitute of **C**ertified **P**ublic **A**ccountants (**AICPA**)

SAS 70	***S****tatement of* ***A****uditing* ***S****tandards was designed to enable an independent auditor to evaluate and issue an opinion on a service organization's controls.*
SSAE 16	***S****tatement on* ***S****tandards for* ***A****ttestation* ***E****ngagements effectively replaced SAS 70 as the standard for reporting on service organizations with effect from June 15, 2011.*
ISAE 3402	***I****nternational* ***S****tandards for* ***A****ssurance* ***E****ngagements defined by* ***IAASB*** *(****I****nternational* ***A****uditing and* ***A****ssurance* ***S****tandards* ***B****oard)*

Our workshop essentially helps participants understand the finer aspects of internal controls over financial reporting in line with the guidelines defined by AICPA and IAASB.

Prerequisite: Exposure to risk assessment, audit process & compliance.

Workshop Duration: 2 days

Schedule: Training Calendar

Examination: Not applicable since only the organization needs to comply with attestation engagement.

IntelleSecure
Information Security & Compliance
www.intellesecure.com

PCI DSS

Home

Payment Card Industry Data Security Standard

PCI DSS is an information security standard for organizations that handle cardholder information for major debit, credit, prepaid, e-purse, ATM, and POS cards. It provides a framework for developing a process for data security - including preventing, detecting and reacting to security incidents.

PCI SSC - **P**ayment **C**ard **I**ndustry **S**ecurity **S**tandards **C**ouncil develops, maintains and manages the PCI Security Standards, which include

- ***DSS** (**D**ata **S**ecurity **S**tandard)*
- ***PA DSS** (**P**ayment **A**pplication **D**ata **S**ecurity **S**tandard)*
- ***PTS** (**P**IN **T**ransaction **S**ecurity) requirements.*

Our workshop helps participants understand how the standards apply to all organizations that store, process or transmit cardholder data - with guidance for software developers and manufacturers of applications and devices used in those transactions.

Prerequisite: Exposure to information systems assessment of the payment card industry

Workshop Duration: 2 days
Schedule: Training Calendar

Examination: Not applicable since only an organization can be validated as a **QSA** (**Q**ualified **S**ecurity **A**ssessor) or **ASV** (**A**pproved **S**canning **V**endor).

IntelleSecure
Information Security & Compliance
www.intellesecure.com

HIPAA

Home

Health Insurance Portability & Accountability Act

HIPAA was adopted in the US to protect private information of patients, primarily directed to healthcare professionals and staff of outsourced BPO companies, who have access to patient information, such as doctors, healthcare office workers, healthcare technicians and healthcare managers.

HIPAA mandates that all the patient information is to be secure, whether it is transmitted electronically or in written format. The HIPAA Privacy Rule establishes regulations for the use and disclosure of **PHI** (**P**rotected **H**ealth **I**nformation).

Our workshop helps participants understand the implications of HIPAA legislation and identifies critical compliance requirements for business / client in line with

- *HIPAA Administrative Simplification Act*
- *HIPAA Privacy Rule.*

Prerequisite: Some exposure to the privacy concerns of the healthcare industry in the US

Workshop Duration: 2 days
Schedule: Training Calendar

Examination: Not applicable since this is an act of US legislation; only organization needs to comply

IntelleSecure
Information Security & Compliance
www.intellesecure.com

ITIL

Home

Information Technology Infrastructure Library

ITIL is based on a set of best practice guidelines used as a framework for IT Service Management. The earlier versions outlined best practices for Service Delivery and Service Support. ITIL v3 / 2011 introduces Service Lifecycle and Capability Management with concepts like

- ***Service Strategy***
- ***Service Design***
- ***Service Transition***
- ***Service Operation***
- ***Continual Service Improvement***
- ***Technology & Architecture***

Prerequisite: Exposure to IT services or operations within any organization.

Workshop Duration: 2 days

Schedule: Training Calendar

Examination	ITIL Foundation
Certifying Body	APMG / ISEB / EXIN / LCS
Exam Fee	US$ 150
Exam Duration	1 hour
Exam Type	Online via Prometric & Pearson Vue Test Centres
Exam Questions	40 multiple choice
Exam Pass Score	65%

IntelleSecure
Information Security & Compliance
www.intellesecure.com

ISO 20000

Home

Information Technology Service Management System

ISO 20000 is the **I**nternational **S**tandards **O**rganization (**ISO**) standard for **I**nformation **T**echnology **S**ervice **M**anagement **S**ystem (**IT SMS**). It consists of a set of best practices guideline for effective IT service management to be implemented and audited prior to the organization getting certified.

Our workshop gives participants an understanding of the key elements of the international standard for ITSM along with the specific requirements of the Quality Management System. Participants learn how to implement and audit as per ISO/IEC 20000 guidelines and specifications supported by relevant checklists.

Prerequisite: Exposure to ITSM within any organization.
Workshop Duration: Lead Auditor - 5 days
Schedule: Training Calendar

Examination	ISO 20000 Lead Auditor
Certifying Body	IRCA (**I**nternational **R**egistrar of **C**ertificated **A**uditors)
Exam Fee	Included in training fee
Exam Duration	2.5 hours
Exam Type	Offline paper based (conducted on last day of training)
Exam Questions	4 sections of multiple choice and scenario based
Exam Pass Score	70%

IntelleSecure
Information Security & Compliance
www.intellesecure.com

ISO 27001

Home

Information Security Management System

ISO 27001 is the **I**nternational **S**tandards **O**rganization (**ISO**) standard for **I**nformation **S**ecurity **M**anagement **S**ystems (**ISMS**). It consists of a set of best practices guideline for information security management which is implemented and audited prior to the organization getting certified.

Our workshop covers the clauses and controls of the international standard for ISMS along with the specific requirements of the Quality Management System. Participants learn how to implement and audit as per ISO 27001 guidelines and specifications supported by relevant checklists.

Prerequisite: Exposure to ISMS within any organization.
Workshop Duration: 5 days
Schedule: Training Calendar

Examination	ISO 27001 Lead Auditor
Certifying Body	IRCA (**I**nternational **R**egistrar of **C**ertificated **A**uditors)
Exam Fee	Included in training fee
Exam Duration	2.5 hours
Exam Type	Offline paper based (conducted on last day of training)
Exam Questions	4 sections of multiple choice and scenario based
Exam Pass Score	70%

IntelleSecure
Information Security & Compliance
www.intellesecure.com

ISO 22301

Home

Business Continuity Management System

ISO 22301 is the first international standard for business continuity management. It consists of a set of best practices guideline for effective business continuity management. ISO 22301 places greater emphasis on setting the objectives, monitoring performance and metrics. Participants learn how to evolve appropriate response strategies in line with the organization's requirement.

- ***Business Continuity Policy***
- ***Business Impact Analysis***
- ***Risk Assessment***
- ***Business Continuity Strategy / Options***
- ***Business Continuity Plans***
- ***Exercising & Testing***

Prerequisite: Exposure to BCP / DR in any job function in an organization. Anyone aspiring to get a better understanding of business continuity management can also attend this workshop

Workshop Duration: Lead Auditor - 5 days

Schedule: Training Calendar

Examination	**ISO 22301 Lead Auditor**
Certifying Body	IRCA (**I**nternational **R**egistrar of **C**ertificated **A**uditors)
Exam Fee	Included in training fee
Exam Duration	2.5 hours
Exam Type	Offline paper based (conducted on last day of training)
Exam Questions	4 sections of multiple choice and scenario based
Exam Pass Score	70%

IntelleSecure
Information Security & Compliance
www.intellesecure.com

ISO 31000

Home

Enterprise Risk Management

Enterprise Risk Management provides an overview of the purpose and requirements of a **R**isk **M**anagement **S**ystem (**RMS**) based on the principles of **ISO 31000**. The 31000 standard is a framework that helps examine, control and continually improve an organization's RMS.

ERM is a risk-based approach to managing an enterprise, integrating concepts of strategic planning, operations management, and internal control. This includes the methods and processes used by organizations to manage risks related to the achievement of their objectives.

Our workshop provides a framework for risk management and helps participants understand magnitude of impact and how to develop an appropriate response strategy. Participants understand how to manage risk within the enterprise using sample templates, walk-through and case studies.

This workshop would particularly help those who involved in the development, implementation and management of RMS based on ISO 31000 and explains how to integrate ISO 31000 with other standards.

Prerequisite: Exposure to risk management within any organization. Anyone aspiring to get a better understanding of ERM can also attend this workshop

Workshop Duration: 2 days

Schedule: Training Calendar

Examination: ISO 31000 is intended to be a family of standards related to risk and has not been developed with the intention of certification