TRUETECH
Info Solutions

Certified Information Systems Auditor

Be a CISA.
Become a successful IS Auditor.

Threats

Cloud computing, mobility, social tools and other technologies that put more power in the hands of individual users pose new challenges for organizations seeking to secure data, devices and networks, recent research released by CompTIA, the non-profit association for the information technology (IT) industry, reveals.

Vulnerabilities

During late October 2012, FBI charged 14 individuals for the theft of over $1 million from Citibank using cash advance kiosks at casinos located in Southern California and Nevada. The fraudsters stole the money by exploiting a gap in the Citibank's ATM applications—which required multiple withdrawals all within 60 seconds—giving the fraud a popular name among the legal and security circles 'Gone in 60 Seconds'.

Exploitations

Zeus, a name that security experts know very well, is one of the most prolific and dangerous malware.

In the years several versions have been detected, it's one of the first malware which has applied an excellent business model that made possible its evolution in cybercrime; unique constant is the monetization process based on the exploit of bank accounts. Last version detected of Zeus botnet has been successful in the theft of about $47 million from European banking customers in the past year.

Security policy & guidelines

The reasons behind South Carolina Department of Revenue (DoR) data breach are more than shocking: All state agencies have some type of computer security system in place, but there is NO mandatory policy, standards, monitoring or enforcement for each of the approximately 100 state agencies, boards, commissions, colleges and universities that operate computers. The DOR breach, the biggest in the state's history, exposed 3.6 million Social Security numbers, 387,000 mostly encrypted credit or debit card numbers and information belonging to more than 650,000 businesses.

IT Climate

Information is one of the most important assets in any organisation. Technology is the key tool employed in the management of this asset, but it is not always a tool that is managed well. The increasing use of technology throughout the organisation environment can empower the organisation in enhancing the overall ability & efficiency towards achieving its strategic goals, aims and objectives.

However, technology is not only an enabler of business goals by providing new opportunities; it poses significant risks by increasing security threats in its operation. In addition, the technology environment is becoming increasing complex with ever greater compliance and regulatory obligations providing a growing challenge to the modern day organizations. Recent high profile corporate scandals and failures, and increased focus on regulation has drawn the attention of corporates to address and minimize risk. At a time profit margins are tight and companies are facing potentially disastrous and expensive regulatory investigations, an IT related failure can threaten a company's existence.

Face the challenges !

To face the challenges of technology and to understand the requirements in a proper perspective, individuals and organisations have to be geared up with appropriate skills, knowledge and orientation. Companies need to employ dedicated teams of technical IT auditors who work exclusively on IT audit and security assignments. The team members should not only understand audit, but also the risks associated with technology and its deployment. The team needs to be qualified and trained in technical and specialist IT network and security roles with deep understanding of the auditing concepts and controls.

CISA

Certified Information Systems Auditor (CISA) certification has been a globally accepted standard of achievement among information systems (IS) audit, control and security professionals. The CISA certification is designed for those who audit, control, monitor and assess an enterprise's information technology and business systems.

CISAs are recognized internationally as professionals with the assurance knowledge, skills, experience and credibility to leverage standards, manage vulnerabilities, ensure compliance, offer solutions, institute controls and deliver value to the enterprise. Often, the CISA credential is a mandatory qualification for an information systems auditor.

WHY CISA?

Corporates are looking for qualified professionals to address various issues relating to the risk and assurance of information assets. Globally, companies who have employed CISAs have better comfort level, as it assures them their audit team has right qualifications. To the individuals, it provides competitive advantage over peers, and demonstrate that they have acquired and maintain knowledge required to meet the challenges of a modern enterprise

HOW DO WE HELP YOU?

Normally offered globally twice a year, the CISA exam consists of 200 multiple- choice questions given during a four-hour session, that cover five job practice domains to test the candidate's knowledge and understanding. Our 4 day CISA review class room course exclusively focuses on the job practice domains that are tested by ISACA for the exam. The class room training are administered by experienced and highly qualified professionals to ensure the participants successfully

- understand the methodology & testing approach of the examination
- gain an understanding of the format, strategy and techniques of the CISA exam
- acquire thorough knowledge of the domain that are tested in the exam
- practice the sample questions with detailed discussions on the answers

Our trainers are the best of class internationally qualified & practicing professionals with decades of practical experience in IT Governance, Risk Management and Assurance services. They are exceptionally experienced in delivering IT training, including CISA, Information Security, Information Risk and Business Continuity Management training programs , to thousands of senior executives from various industry segments. They not only ensure the candidates are exam ready after the 4-day training but also continue to offer personal support through e-mails, blog etc.