C)ISSO™
Certified Information Systems Security Officer

Certified Information Systems Security Officer™

DATOS CLAVE

Nombre del curso
CISSO™

Duración: 40 horas

Pre-requisitos:

- Se recomienda experiencia en por lo menos 2 módulos del curso, más no es indispensable.

Materiales digitales:

- Key Security Concepts &Definitions Books

Examen de Certificación:

- CISSO - Certified Information System Security Officer™

DESCRIPCIÓN DEL CURSO

El curso CISSO está diseñado para un pensamiento avanzado con visión para el futuro profesional que maneja y juega un papel clave en la seguridad de la información de determinada organización

CISSO aborda una amplia gama de las mejores prácticas, conocimientos y habilidades que se esperan de un líder en la industria de TI

El participante aprenderá teoría y los requerimientos para la implementación práctica y de control, de los conceptos de seguridad. Mediante el uso de un enfoque basado en el riesgo CISSO es capaz de implementar y mantener controles de seguridad rentables que están estrechamente alineados con los requerimientos del negocio.

El CISSO Certified Information Systems Security Officer fue una iniciativa directa del DND – Departamento de Defensa de Canadá en conjunto con el DOD – Departamento de Defensa de los Estados Unidos. Definido en esta doble iniciativa CANUS CDISM MOU - ID#: 1974100118 que se encuentra en:

http://www.state.gov/documents/organization/111449.pdf

A. The CDRSN National Information System Security Officer (ISSO) is the focal point for all security issues pertaining to this network.

B. The Director Information Management Security (DIMSECUR) is the DND authority for security assessment of the CDRSN, including the approval of Interim Authority to Process (IAP) and Authority to Communicate.

With these initiatives in mind, Mile2 created a certification for the ISSO called Certified ISSO.

"The Certified Information Systems Security Officer training and certification program prepares and certifies individuals to analyze an organization's information security threats and risks, and design a security program to mitigate these risks. ISSO's will be proficient in risk analysis, risk mitigation, application security, network security, operations security and business continuity."

Whether you are a responsible for the management of an Information Security team, a Security Officer, an IT auditor or a Business Analyst the Certified Information Security Officer – C)ISSO course is an ideal way to increase your knowledge, expertise and skill. The C)ISSO course, and subsequent examination, is the most up to date, practical and effective program available in the world today. The C)ISSO program is closely aligned with the leading standards of ISO27001, NIST, CISM® and the 2012 CISSP® CBK® Exam objectives, but it excels by providing a well-rounded and comprehensive overview of each topic area without being restricted to a single model or conceptual approach.

Mile2's Certified ISSO training differs from the Standard CISM, ISO27001, NIST & CISSP in the following:

The popular CISSP stands for 'Certified Information Systems Security Professional'. We focus on information systems security, not information technology security. The fact is that many participants are technological experts in their own rights, be it network operations, storage management systems, database administration, etc. They don't need us to tell them what an MPLS network is, or the advantages of fiber over copper coaxial, etc. What they do need is a mind-set change; how to think 'big-picture' instead of 'vertical silo'. How deep principles within each domain interconnect into a beautiful whole; how to view their area of responsibility through the fascinating lenses of risk management. How to perform a threat and risk analysis, derive a residual risk position for their department, enterprise or client, articulate the same as an organizational, issue-specific or system policy, with advisory, regulatory or informative goals, and implement this policy through the right mix of physical, administrative and technical controls, performing one or more of the six control services in a defense-in-depth enterprise security architecture. Light bulbs flash when the penny drops, and we know we have succeeded in effecting this mind-set change when 25-years experienced IT Directors are just as excited and eager to learn as 5-year experienced systems administrators!

We deliver the content within a proprietary 'Theory, Technique, Tool' delivery framework via a proprietary 'Discuss, Demonstrate, Do' action learning model. The ten domains are chock-a-bloc full of theory, which when implemented, is compromised for practical reasons. Take your relational database for example. Theoretically, a database must be normalized to at least 4 (out of 5) normal forms to qualify as a relational database, as this is the minimum level of atomicity required to yield the functional benefits of the relational model for data organization. But no vendor has ever complied with this theoretical principle as the performance overhead required to do so is too high. Understanding the differences between relational database theory, and the technique used by vendors to develop their products (tools) automatically explains 80% of the constant vulnerabilities we see in said databases. This understanding leads us to a logical choice of compensating deterrent, preventive, detective, recovery, and corrective controls to govern access to relational data repositories in adhering to a relevant residual risk position. In many cases, we are able to create learning labs where the theory is discussed, the technique demonstrated, with participants actively exploring (do) the 'vulnerabilities-within-the-gap', the natural, man-made and/or technical threats that can exploit these vulnerabilities, leading to non-disaster, disaster and/or catastrophic impact levels, and the likelihood thereof, and select the right mix of controls to mitigate the same. In other words, participants actively learn the risk management mind-set!

MÓDULOS DEL CURSO

Módulo 1: Risk Management
Módulo 2: Security Management
Módulo 3: Authentication
Módulo 4: Access Control
Módulo 5: Security Models and Evaluation Criteria
Módulo 6: Operations Security
Módulo 7: Symmetric Cryptography and Hashing
Módulo 8: Asymmetric Cryptography and PKI
Módulo 9: Network Connections
Módulo 10: Network Protocols and Devices
Módulo 11: Telephony, VPNs and Wireless
Módulo 12: Security Architecture and Attacks
Módulo 13: Software Development Security
Módulo 14: Database Security and System Development
Módulo 15 – Malware and Software Attacks
Módulo 16: Business Continuity
Módulo 17: Disaster Recovery
Módulo 18: Incident Management, Law, and Ethics
Módulo 19: Physical Security

5584215929
www.bitnueve.mx
@bitnuevemx
cursos@bitnueve.mx
Bitnuevemx