Building an Information Systems Security Policy

Overview

The efficient digital storage of information is becoming ever-more critical to the maintenance of efficient business functions. The compromise of data can have a devastating impact on an organisation's ability to function, placing high importance on the understanding of the systems and procedures for securing data as well as enabling data recovery. This course is specially designed for telecom operators, data-centres, Internet service providers and other organisations heavily dependent on customer data management.

More at
WWW.CTO.INT/TRAINING

For more information contact us on **programmes@cto.int** or **+44 208 600 3800**

Building an Information Systems Security nPolicy

Overview

The efficient digital storage of information is becoming ever-more critical to the maintenance of efficient business functions. The compromise of data can have a devastating impact on an organisation's ability to function, placing high importance on the understanding of the systems and procedures for securing data as well as enabling data recovery. This course is specially designed for telecom operators, data-centres, Internet service providers and other organisations heavily dependent on customer data management.

Objectives

The objectives of this course are to:
- To provide detailed understanding of enterprise security management frameworks
- To introduce regulatory requirements
- To understand and assess security risks and threats
- To explore data protection and recovery planning strategies
- Enable business continuity planning and disaster recovery

Target audience

This course is suitable for systems and network administrators, IT security professionals and business continuity teams.

Expected outcomes

On completion of this course, the successful participant will be able to:

- Identify major security management frameworks and assess the usefulness of security management practises in safeguarding IT assets
- Identify various regulatory requirements in computer security, privacy and crimes and justify the appropriate use of regulatory frameworks in enterprises
- Conduct risk assessments and apply risk management strategies in enterprise environments
- Identify and apply data protection and recovery planning strategies
- Appraise the fundamental elements of business continuity planning and disaster recovery management

Course outline

Enterprise security management frameworks: information security policy, standards, guidelines, procedures (Day 1)

- ISO/IEC 27001 based information security management system (ISMS)
- ISO/IEC 27001: establishment, implementation, control and improvement of the ISMS
- ISO/IEC 27002: code of practice on ISMS
- COBIT 5 for information security
- Generally accepted information security principles (GAISP)

Regulatory requirements (Day 2)

- Computer security, privacy, and crime laws - worldwide outlook of regulation and legislation, the essence of computer crime
- Laws and complexities of cybercrime
- Gramm-Leach-Bliley Act
- Payment card industry data security standard (PCI DSS)
- Sarbanes-Oxley Act (SOX)
- Data protection and intellectual property rights
- Introduction to digital forensics and investigations
- Information security ethics

Security risks, threats and management (Day 3)

- Introduction to principles of vulnerability, threat and risks
- Enterprise risk management

Trainer profile

Harshana Ranmuthugala

Harshana Ranmuthugala holds a bachelor of science in engineering specialized in computer science and engineering, master of science specialized in information systems security from University of Moratuwa, Sri Lanka and masters of business administration degree from Postgraduate Institute of Management, University of Sri Jayewardenepura, Sri Lanka. He is a chartered engineer recognized by engineering council, United Kingdom as well as The Institution of Engineers Sri Lanka and a chartered IT professional awarded by the British Computer Society, United Kingdom. He is a member of The Institution of Engineering and Technology, United Kingdom, and The Computer Society, Sri Lanka.

Ranmuthugala, a citizen of Sri Lanka, currently works at Sri Lanka Telecom PLC, the largest telecommunications services provider in Sri Lanka as a deputy general manager. He has a wide array of practical experience in information security management, ISMS audit, business continuity planning and disaster recovery management, corporate risk management, telecommunication services sales and business development and human resource management. He is a lead ISMS auditor/implementer and has extensive experience in implementation of ISO/IEC 27001:2005 based information security management system in Sri Lanka Telecoms' client facing divisions which offer ADSL, broadband, Internet, data hosting services and data services to more than 400,000 customers.

Ranmuthugala worked as a visiting lecturer, examiner, instructor and curriculum designer for the department of computer science and engineering as well as in the faculty of information technology, University of Moratuwa, Sri Lanka. He has authored several international research and journal publications in the area of information security and technology.

CTO
ICTForum'17
11 - 13 SEPTEMBER 2017, MAPUTO, MOZAMBIQUE

Digital Nations, Digital Wealth

Organised by
CTO COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

Hosted by
INCM

More info at: www.cto.int/events

#CTOtelecomforum