ISO 27001 & CYBERDEFENSE BOOTCAMPS

MAY - JUNE 2024

Milima Cyber Academy®

Milima Cyber Academy®

ISO/IEC 27001 Foundations

30th -31st May, 2024

Meilin International Hotel

Kampala, Uganda

UGX 2,000,000/= per participant

PECB

Designed For Personnel from Banks, Insurance Companies, Audit Firms and Financial Technology Providers

INTRODUCTION

Information today is considered one of the most valuable assets of an organization — whether it's intellectual property, customer data or trade secrets. This is the biggest driving force of cybercrime making every organization a potential target of cyber threats.
According to The RSA Cybersecurity Poverty Index survey, 80% of organizations report that they've had a security incident that negatively affected their business operations in the past 12 months.

ISO/IEC 27001 provides requirements for organizations and individuals seeking to establish, implement, maintain and continually improve an information security management system. This framework serves as a guideline towards continually reviewing the safety of information, which exemplifies reliability and adds value to services in organizations.

Milima Cyber Academy in partnership with **PECB** is organizing an ISO/IEC 27001 Foundations bootcamp training for various personnels in Information Handling roles at managerial, consultancy and executive levels.

ABOUT THE ISO/IEC 27001 FOUNDATIONS BOOTCAMP

Course Name: ISO/IEC 27001 Foundations
Course Duration: 16 Hours (2 Days)
Award: PECB ISO/IEC 27001:2022 Foundation Certification

About The Course

ISO/IEC 27001:2022 Foundation training allows you to learn the basic elements to implement and manage an Information Security Management System as specified in

ISO/IEC 2700:2022. During this training course, you will be able to understand the different modules of ISMS, including ISMS policy, procedures, performance measurements, management commitment, internal audit, management review and continual improvement.

WHO IS THIS TRAINING SUITABLE FOR?

- Managers and consultants seeking to know more about information security
- Professionals wishing to get acquainted with ISO/IEC 27001:2022 requirements for an ISMS
- Individuals engaged in or responsible for information security activities in their organization
- Individuals wishing to pursue a career in information security and information technology audits

WHY IS THIS TRAINING SUITABLE FOR YOU?

PECB ISO/IEC 27001 Certificate will prove that you have:

- Obtained the necessary expertise to support an organization to implement an Information Security Management System that complies with ISO/IEC 27001
- Understood the Information Security Management System implementation process
- Provide continual prevention and assessments of threats within your organization
- Higher chances of being distinguished or hired in an Information Security career
- Foundations to launch your career in information technology audit
- Understood the risk management process, controls, and compliance obligations
- Acquired the necessary expertise to manage a team to implement an ISMS

- The ability to support organizations in the continual improvement process of their Information Security Management System
- Gained the necessary skills to audit organization's Information Security Management System

ISO/IEC 27001 Lead Auditor

10th - 14th June, 2024

Meilin International Hotel

Kampala, Uganda

UGX 4,800,000 per participant

Designed For Personnel from Banks, Insurance Companies, Audit Firms and all Professional Bodies and Associations.

INTRODUCTION

Information today is considered one of the most valuable assets of an organization — whether it's intellectual property, customer data or trade secrets. This is the biggest driving force of cybercrime making every organization a potential target of cyber threats.
According to The RSA Cybersecurity Poverty Index survey, 80% of organizations report that they've had a security incident that negatively affected their business operations in the past 12 months.

ISO/IEC 27001 provides requirements for organizations and individuals seeking to establish, implement, maintain and continually improve an information security management system. This framework serves as a guideline towards continually reviewing the safety of information, which exemplifies reliability and adds value to services in organizations.

Milima Cyber Academy in partnership with **PECB** and **Birger** is organizing an ISO/IEC 27001 Lead Auditor bootcamp training for various personnels in Information Handling roles at managerial, consultancy and executive levels.

ABOUT THE ISO/IEC 27001 LEAD AUDITOR BOOTCAMP

Course Name: ISO/IEC 27001 Lead Auditor
Course Duration: 40 Hours (5 Days)
Award: PECB ISO/IEC 27001:2022 Lead Auditor Certification

About The Course
ISO/IEC 27001 Lead Auditor training enables you to develop the necessary expertise to perform an Information Security Management System (ISMS) audit by applying widely recognized audit principles, procedures and techniques.

WHO IS THIS TRAINING SUITABLE FOR?

- Auditors seeking to perform and lead information security management system (ISMS) audits
- Managers or consultants seeking to master the information security management system audit process
- Individuals responsible to maintain conformity with the ISMS requirements in an organization
- Technical experts seeking to prepare for the information security management system audit
- Expert advisors in information security management

WHY IS THIS TRAINING SUITABLE FOR YOU?

- During this training, participants will acquire the knowledge and skills to plan and carry out internal and external audits in compliance with ISO 19011 and ISO/IEC 17021-1 certification process.
- Based on practical exercises, you will be able to master audit techniques and become competent to manage an audit program, audit team, communication with customers, and conflict resolution.

TRAINING COVERAGE

- Fundamental concepts and principles of an information security management system (ISMS) based on ISO/IEC 27001
- Interpretation of the ISO/IEC 27001 requirements for an ISMS from the perspective of an auditor
- Evaluation of the ISMS conformity to ISO/IEC 27001 requirements, in accordance with the fundamental audit concepts and principles
- Planing, conducting, and closing an ISO/IEC 27001 compliance audit, in accordance with ISO/IEC 17021-1 requirements, ISO 19011 guidelines, and other best practices of auditing
- Management of an ISO/IEC 27001 audit program

PREREQUISITES FOR PARTICIPANTS

- A fundamental understanding of ISO/IEC 27001 and comprehensive knowledge of audit principles.
- ISO/IEC 27001 Foundations certificate is recommended.

Milima Cyber Academy®

CYBERDEFENSE BOOTCAMP

24th -28th June, 2024

Meilin International Hotel

Kampala, Uganda

UGX 2,000,000/=per participant

PECB

Designed For Personnel from Banks, Tier 4 FIs (SACCOs), Insurance Companies, Audit Firms and Financial Technology Providers

INTRODUCTION

Information today is considered one of the most valuable assets of an organization — whether it's intellectual property, customer data or trade secrets. This is the biggest driving force of cybercrime making every organization a potential target of cyber threats.[1]

According to The RSA Cybersecurity Poverty Index survey, 80% of organizations report that they've had a security incident that negatively affected their business operations in the past 12 months.

The recent years have seen a significant rise in cyberthreats across the globe with individuals and businesses of all tiers falling victims to the raging cyber attacks.

A report by PurpleSec indicates a 600% rise in cybercrime globally, largely contributed by the impact of the COVID-19 pandemic which among many things has led to; Work from home policies and excessive spread of fake news. According to the Uganda Police Force, Criminal Investigation Department, the reported cases of losses attributed to cybercrime stood at approximately $4.5m for the year 2020

Building the right cyberdefense team continues to provide the biggest guarantee of security and business resilience. This also promises a significant return on investment with minimal use of third-party service providers.

Milima Cyber Academy delivers interactive, intense and immersive cyberdefense training programs designed to equip technical teams with relevant and dependable skills in cybersecurity and digital forensics.

Milima Cyber Academy is Uganda's top tier cyber-security and digital forensics academy supporting young professionals to gain practical and hands-on skills.

[1] https://www.rsa.com/en-us/resources/rsa-cybersecurity-poverty-index-2016

ABOUT THE CYBERDEFENSE BOOTCAMP

Milima Cyber Academy is organizing a Cyber Defense training for the various IT personnels in the different Saccos and MFI(s) in the region to enable them acquire professional skills in Cybersecurity attack techniques and defenses.

Course Name: Cyberdefense
Course Duration: 40 Hours (5 Days)
Award: Professional Certificate In Cyberdefense

About The Course

The Cyberdefense training program is a unique cybersecurity training designed to introduce participants to critical concepts of attacks and defense of the IT infrastructure. In this training, typical IT attacks are simulated in realistic virtual corporate networks. The aim is to enable each participant to understand and defend against a wide variety of modern IT attacks.
This includes:

- Understand, recognize and defend against IT attacks under guidance
- Learn attacker logic in overall context of a corporate network
- Correctly assess the limits of security products
- Prioritize hardening measures in the company network correctly

In various attack scenarios the participants learn, in increasing degrees of difficulty, to recognize typical attacks on corporate networks:

- Explanation of the theoretical basics before each attack with dedicated briefing
- Execution of all attacks by the participants (Red Team perspective)
- Recognition / Detection of all attacks by the participants (Blue Team perspective)

- Targeted demonstration of the possibilities and limits of IT security products (AV, FW, WAF, etc.)

Although specific products of individual manufacturers are used, the learnings are always kept generic, so that the acquired knowledge can be directly applied to similar products in your own company.

"Only those who understand modern attack techniques on a technical level, can successfully detect, defend off, prevent and analyze in an efficient way."

COURSE CHAPTERS COVERED

1. Awareness / General Global Threat Situation
2. Introduction - Getting to know the training environment
3. Hack-Like-A-Script-Kiddy
4. Attacker Kill Chain – Reconnaissance and the limitation of commercial security tools
5. Attacker Kill Chain – Initial Compromise Through Web Based Attacks
6. Attacker Kill Chain - Establish Foothold & Escalate Privileges on Web-Based Systems
7. Attacker Kill Chain – Initial Compromise by (Spear)-Phishing Attacks
8. Attacker Kill Chain – Establish Foothold & Escalate Privileges on Windows
9. Attacker Kill Chain - Complete Mission
10. Crypto Trojans in Corporate Environments
11. Outro

WHO IS THIS TRAINING SUITABLE FOR?

System, Database and Network Administrators / Operations Engineers

Learn to operate your IT systems more securely. Detect and stop internal and

external targeted attacks.

Application/Website Developers
Learn to develop your applications more securely. Become aware of common pitfalls on the application level and prevent them.

IT-Security Managers / Decision Makers
Make better decisions in the IT security environment on the base of your newly acquired knowledge and practical knowledge.

ADDED VALUE OF TRAINING

At the end of the training, participants will be able to identify, prevent / reduce technical risks for an organization holistically in an effective and efficient way. The acquired knowledge can be used in a targeted manner in the context of a wide variety of applications in the corporate context.

PREREQUISITES FOR PARTICIPANTS

No hacking experience is required. The necessary basics are explained in detail at the beginning of each chapter. Furthermore, no experience in dealing with typical IT security products is required.
However, technical IT experience is an advantage.

TECHNICAL REQUIREMENTS FOR MILIMA CYBER DEFENSE TRAINING

Participant Requirements:

Every participant needs a laptop / workstation with the following:

- Kali Linux OS to be installed before arrival at the training ground. Installation instructions and guidance will be provided to all confirmed participants.
- Metasploitable 2
- Web browser (IE, Edge, FF or Chrome)
- WiFi or Ethernet Adapter – depending on provided network access
- Preferably a large (external) screen for comfortably opening different tabs in parallel.

CERTIFICATE

At the end of the training, all participants receive a **Certificate of Cyberdefense.**

What Will Be Provided?

- Training materials for the Cyberdefense course
- Cyberdefense software tools that can be taken back to use in corporate environments
- Certificate at the end of the training.