

ISO 27001 Implementation Master Class

To enable you to implement and certify ISO 27001 compliant information security management systems in organizations



On

October 8, 9 and 10, 2009,
Domaine Les Pailles, Mauritius

What will you learn?

How to implement and certify ISO 27001 in an organization.

How to manage ISO 27001 systems after certification.

The people aspect of information security - Information security awareness and behavior management.

Presented by



MULTIEVENTS
Your preferred Events partner
www.multievents.mu

InterSecApp

International

Security

Applications

www.intersecapp.com

Program outline and syllabus

IMPORTANT – ALL DELEGATES ARE ADVISED TO BRING A LAPTOP OR CARRY ONE LAPTOP IF THEY ARE ATTENDING AS A GROUP TO EFFECTIVELY PARTICIPATE IN THE TRAINING PROGRAM.

Day 1 – October 8, 2009

Session 1: Short movie & Introduction session: “Even a football team can use ISO 27001” : Time - 08.30 to 10.00

- The need for protecting business information
- Linking business goals to information security
- Breaking-the-ice session (Role play): 3 teams will be created. Each team must create a 10 slide presentation that explains,
 - o Why is information security important for their business?
 - o What are the current information security risks? What is the potential impact of these risks?
 - o Why is an ISMS required to treat these risks?
 - o What do you think will be the MTP (Money, Time and People) requirements for the ISMS?

Session 2: Information security management systems: ISO 27001 and ISM3: Time 10.00 to 10.45

- Explanation of ISMS and the PDCA (Plan-Do-Check-Act) Model
- The ISO 27001 ISMS standard, architecture and components
- Real life case study of ISO 27001 certification: From scope-definition to certification
- The ISM3 model & using ISM3 for improving the ISO 27001 ISMS beyond certification

Step 1 of the ISMS – The PLAN Phase

Session 3: Creating the Information Security Management Forum (ISMF) & ISMS Scope definition : Time 11.00 to 12.00

- Identify business functions that must be protected using the “Security in Context” (SIC) model
- Creation of ISMF: Identify key members, define responsibilities of ISMF members
- Define the scope of the ISMS: Explain “exclusions” and “inclusions”; Submit to Top management
- Group activity: Define a sample scope ,explain the “exclusions” and “inclusions” & submit to Top management

Session 4: Identification, classification and rating of information assets: Time 12.00 to 13.00

- Identify & classify information assets from each business function
- Rate the value of information assets using the CIA (Confidentiality, Integrity and Availability) triad.

Session 5: Risk assessment, Risk scoring & Risk prioritization: Time 14.00 to 15.45 & 16.00 to 17.00

- Understanding of risk assessment: Concepts of “threat”, “vulnerability”, “impact” & “probability of occurrence”
- Assess risks at 3 levels
 - o Organizational information security risks
 - o Asset specific information security risks
 - o Special session – Identify people specific information security risks – Risks due to poor security “awareness” & “behavior”
- Score the risk assessment output using a scoring model & prioritize risks based on scores
- Group activity: Role play
 - o Team 1: Will play the role of risk assessors and business managers: They will do a sample risk assessment, score the risks and prioritize

Program outline and syllabus

- o Team 2: Will play the role of decision makers who will analyze the risks, ask intelligent questions and approve or disapprove the risk assessment report

Day 2 – October 9, 2009

Step 2 of the ISMS – The DO Phase

Session 6: Risk treatment: Planning, assignment and setting performance targets with metrics : Time 08.30 to 10.45 and 11.00 to 13.00

- Creating the information security policies and essential ISMS documents
- Over view of 11 domains and 133 ISO 27001 controls
- Choose controls from the ISO 27001 standard to treat the,
 - o Organizational information security risks
 - o Asset specific information security risks
 - o People specific information security risks
- Group activity: Form 3 teams and each team will create one information security policy each
 - o Primary information security policy of the organization
 - o Any two policies corresponding to the 11 domains of ISO 27001

Session 7: Implementing the risk treatment plan: Time 14.00 to 15.45 and 16.00 to 17.00

- Implementing ISO 27001 controls : Responsibilities of the risk owner
 - o Creating an implementation plan
 - o Selecting the implementation team, providing guidance, actual implementation and monitoring
- Case study: 4 real-life examples of information security risk treatment in action
 - o Treating the security risks of an off-shore IT business
 - o Treating the security risks of a manufacturing business that has internal intellectual property design and development
 - o Treating the security risks of a healthcare business with focus on privacy protection and adherence to privacy regulations
 - o Special session – Treating people specific risks (a model for creating information security awareness and improving responsible information security behavior)

Day 3 – October 10, 2009

Step 3 of the ISMS – The CHECK Phase

Session 8: Internal security audits for checking the effectiveness of risk treatment : Time 08.30 to 10.45

- Defining the audit methodology: Setting targets, audit strategies, creating the audit check list
- Selecting the internal information security audit team
- Group activity: 3 teams will be created and each team will be assigned the following tasks
 - o Create an audit check list
 - o Perform the audit (mock audit) and record the findings
 - o Create a 10 slide presentation about the audit findings and present it to top management

Program outline and syllabus

Day 3 – October 10, 2009 continues...

Step 4 of the ISMS – The ACT Phase

Session 9: Acting on the audit findings, reviewing the performance of the ISMS and making improvements: Time 10.45 to 12.00

- Reviewing the audit reports and checking whether ISMS performance targets have been achieved
- Root cause analysis and making corrections; Improving performance targets and metrics
- Group activity – Root cause analysis: 3 teams will be formed. The trainer will present a set of security audit reports with positive and negative findings. Each team will be asked to,
 - Perform the root cause analysis of each finding
 - Make corrections
 - Suggest improvements in performance targets and metrics

The ISO 27001 Certification process

Session 10: Preparing for the certification, the certification process: Time 12.00 to 13.00 & 14.00 to 15.00

- Understanding the ISO 27001 2-stage external certification audit process
Certification activities
 - Before the audit: Preparing the SOA (statement of applicability) & essential documents, internal briefings, closure of gaps etc.
 - The day of the audit: The expectations of the auditor, essential preparation and mistakes to avoid
 - After the audit: Post-certification recommendation activities to be completed
- Case study: An example of an ISO 27001 certification process and audit report

Post certification maintenance of the ISMS

Session 11: Maintaining the ISMS after the certification audit: Time 15.00 to 16.00

- The real challenge: Maintain the quality and efficiency of the ISMS
- The importance of repeating internal information security audits Improving performance targets (+ metrics) based on audit findings and business growth
- Showcasing your ISMS to your customers and vendors

Certification test

Session 12: 45 minute multiple choice (objective) test: Time 16.15 to 17.00

A 45 minute multiple choice test shall be administered at the end of the exam for all candidates. The test shall be paper-based with a set of multiple choice questions focusing on the topics covered during the course. The test results shall be conveyed to all candidates within 7 days of course completion. All candidates who successfully pass the test shall be awarded the "ISO 27001 Lead Implementer" certificate by International Security Applications.