



IMPLEMENTATION OF HIGH-PERFORMANCE SECURITY MANAGEMENT PROCESSES

OBJECTIVES >



This course is specifically designed to improve your skills as an information security manager. Using O-ISM3 as a framework, you will master process management, and you will be able to:

- Prioritize security efforts using business significant criteria.
- Communicate the value that Information Security Department brings to the organization.
- Design, implement and use information security metrics proven in the field, enabling short cycle continuous improvement.
- Simplify ISO27001 compliance.
- Complement ITIL security.
- Manage outsourced security services with SLA's.
- Implement TOGAF and SABSA architectures.

O-ISM3 is an information security management maturity standard published by The Open Group, a leader in the development of open, vendor-neutral IT standards and certifications. Check some O-ISM3 Resources.

GOALS OF THE COURSE >

- Deep understanding of complex security and management concepts.
- Alignment of security objectives with an organization's mission.
- Classifying and setting requirements for information systems that satisfy security objectives.
- Communication of the value of information security.
- Access control management concepts.
- Implementation of security processes.
- Process management activities.
- Design, implementation and use information security metrics.
- Understanding of the relationship between metrics, managements practices, capability and maturity.
- Techniques for visualization of security metrics.
- Understanding of distribution of responsibilities concepts.
- ISM3-RA Risk Assessment.
- Management of Outsourced Security processes.

1ST DAY >
9:00AM 17:00PM

- **Concepts:** You will gain a deeper understanding of complex security concepts.
- **Assets & Goals:** You will be able to set security objectives aligned with your organization's mission, and you will be able to communicate what is the value that the information security department brings to the organization.
- **Security Objectives:** You will be able to set requirements for information systems that satisfy security objectives.
- **Access Control:** You will gain an understanding of the management ramifications of access control.
- **Classification of Systems:** You will be able to prioritize efforts using business significant criteria for systems classification.
- **Activities & Deliverables:** You will gain an understanding of the relationship between activity and achievement of goals.
- **Bottom-up Process Implementation:** You will learn how to apply O-ISM3 to processes under your own responsibility.
- **Top-down Security Program:** You will learn how to apply O-ISM3 when you have support from top IT management.

2ND DAY >
9:00AM 17:00PM



- **General Processes:** You will familiarize yourself with auxiliary but essential processes.
- **Strategic Processes:** You will familiarize yourself with processes related to goals definition and provision of resources.
- **Tactical Processes:** You will familiarize yourself with processes related to continuous improvement and resource distribution.
- **Operational Processes:** You will familiarize yourself with technical hands-on processes.
- **Management Practices:** You will learn the basics about process management activities.
- **Metrics:** You will learn in detail how to design, implement and use information security metrics.
- **Maturity:** You will become familiar with the relationship between metrics, management practices, capability and maturity.
- **Reports, Dashboards & Visualization:** You will learn how to make the best of metrics, enabling interpretation and communication.

3RD DAY >
9:00AM 17:00PM

- **Security Organization:** You will understand how the distribution of responsibilities make processes tick, and how to avoid related risks.
- **Security Modeling:** You will gain a working knowledge of advanced security models.
- **O-ISM3-RA:** You will learn to perform a simple yet meaningful Risk Assessment.
- **ISO27001:** You will learn how to make O-ISM3 help you with ISO27001 compliance.
- **IT Architecture:** You will learn how to use O-ISM3 effectively whith SABSA and TOGAF.
- **ITIL & SLA's:** You will learn how to complement ITIL with O-ISM3, and how to design SLA in order to manage outsourced security processes.
- **Certification:** You will peek at O-ISM3's certification process
- **Techniques & References:** You will learn general security techniques in order to treat security threats
- **Recapitulation:** You will look back at the last three days highlighting the most important ideas and concepts.

TRAINER PROFILE >

Vicente Aceituno, principal author of O-ISM3, experienced Information Security Manager and Consultant with broad experience in outsourcing of security services and research. He focuses in information security outsourcing, management and related fields like metrics and certification of ISMS.

Member of ISMS Forum, The Open Group's Security Forum Steering Committee, President of the ISSA Spanish Chapter, Director of R&D of ISQWorld, Member of the advisory committee of Red@Seguridad (This magazine grants the most prestigious security awards in Spain), former president of the Conferencias FIST association.

CISA certified.

TARGET PROFILE >

Professionals with responsibilities for information security, consultants, outsourcing providers, CISO/CSO, auditors, consultants, professionals with CISA, CISM, CISSP, or ISO27001 Lead Auditor certification who want to apply proven management techniques to information security.

PARTIAL LIST OF PUBLICATIONS >

- Optimizing ISO27001 using O-ISM3 (The Open Group, 2012).
- Usefulness of an Information Security Management Maturity Model (ISACA "Control", March 1, 2008).
- ISM3: A Standard for Information Security Management (ISSA Journal, 2006).
- Security Metrics for Information Security Management (ENISA Quarterly, 2007).
- How Secret is a Secret? (ISSA Journal, 2006).
- On Information Security Paradigms (ISSA Journal, 2005).
- The Information Security Assurance Markup Language (Computer Society of India, 2007).
- Information Assurance Markup Language (ISM3 Consortium, 2007).
- Events Logging Markup Language (ISM3 Consortium, 2007).
- Security Metrics (ISSA Ireland, 2008).
- El dilema del burócrata (ISMS Forum, 2008).
- Seguridad de la Información (Editorial CreacionesCopyright, 2001).
- Threat Taxonomy (Inovement, 2013).
- Cobit CMMI and O-ISM3 Capability Levels Mapped (Inovement, 2013).

DATES >

- Madrid Course - Wednesday 8th to Friday 10th October 2014
- London Course - Wednesday 5th to Friday 7th November 2014
- Barcelona Course -Wednesday 26th to Friday 28th November 2014

**MORE
INFORMATION >**

aulavass@vass.es