atsec
the information security provider

# NEWS

07/2011

Constant training of employees is a reality that many companies have to deal with – and it is no different at atsec. We are involved with many different national and international IT security standards – which means being aware of changes, updates, interpretations, and the real-world impact of these standards.

We are eager to share this knowledge with our customers and would like highlight our training offerings detailed within this.

atsec consultants have held courses, workshops, and seminars all over the world, as well as hosted events for government and private organizations in our offices in the U.S., Germany, Sweden, and China.

Whether you need customized training with in-depth technical details or a high-level overview for your company's management team – atsec is the right partner for you.

How can we help you?

Regards,

***Andreas Fabis***
Marketing Director

Please join our

## FIPS 140-2 Validation Requirements Course

at the Homewood Suites in Austin, TX

Steve Weingart will be your tutor on
**August 2nd, 2011 – 9am to 5pm**
**August 3rd, 2011 – 9am to 3pm**

*http://atsec-information-security.ticketleap.com/fips-140-2-validation-requirements-course/*

## Recent news in short:

- atsec accredited as a NASPO Third-Party Auditor
- atsec completes PCI DSS Security Assessment for Damai
- Kanguru Defender Secure USB Product Family enters Common Criteria evaluation process
- atsec information security completes the CAVP cryptographic algorithm testing for Watchdata
- Wind River achieves Common Criteria Certification for Linux Secure 1.0 at EAL 4+
- Eastcom passes PA DSS Compliance Assessment performed by atsec information security
- Red Hat achieves six FIPS 140-2 Security Certifications on HP Systems
- DataLocker Enterprise receives FIPS 140-2 Certification

**More news on our website:**
*www.atsec.com*
*Did you know atsec has a security blog? Follow our consultant's thoughts and musings at: http://atsec-information-security.blogspot.com.*
*Also join us on Facebook and Twitter (@atsecitsecurity).*

Common Criteria (ISO/IEC 15408) ▪ FIPS 140-2 ▪ CAVS ▪ SCAP ▪ NPIVP ▪ GSA ▪ FIPS 201 ▪ PCI QSA ▪ PCI ASV ▪ PCI PA-QSA ▪ ISO/IEC 27001 ▪ SOX and Euro-SOX ▪ FISMA ▪ HIPAA ▪ VTDR ▪ Embedded Systems ▪ Hardware Security ▪ Testing and Analysis ▪ Penetration Testing ▪ US Export Control for Cryptography

# atsec’s Training Offerings

**One of atsec’s founding principles is: “Know the business.” That means the continuing education and training of our consultants is a priority for the company. A comprehensive knowledge of the IT security standards that we deal with in our daily work is as important as grasping the consequences that an evaluation or certification might have for a business.**

We like to share our expertise with our customers because we believe that both parties gain from this exchange. Development cycles can be shortened if the developers have an understanding of what a future evaluation or assessment might require of them. Instead of scrambling to meet the requirements after the product is finished – which often leads to costly and time-consuming patches – the developers can do their work with the requirements of an IT security standard in mind. This is especially useful during FIPS 140-2 and Common Criteria projects. We pride ourselves not only on conducting an evaluation with great professionalism, but also on helping customers to understand the evaluation process and making future projects run more smoothly. Training your technical staff is a great first step in that direction.

A training seminar or workshop is also a great opportunity to ask questions to which you won’t find answers in the standards documents. The practical application of standard requirements is our bread and butter – we know about the challenges of conducting an evaluation or being audited, as well as how the different national schemes interpret the standards. atsec is at the forefront of IT security standard development.

atsec offers both regularly scheduled and customized, on-demand education and training courses which can be held at our facility or on-site at your location. We have conducted several country-specific trainings in Korea, Taiwan, and Turkey, as well as other countries. We can also develop training for other IT security topics tailored to meet your company’s needs.

We invite you to take advantage of our professional real-world knowledge in the area of IT security and learn from our experienced consultants.

Here are some of the customized courses we offer:

**Overview of Common Criteria Evaluations for Business Decision Makers** (1 day)

- Acquaint attendees with a business justification to pursue Common Criteria evaluation and certification
- Provide attendees with knowledge of the Common Criteria Standard and the organization of international and U.S. national management bodies
- Provide attendees with an overview of how a Common Criteria evaluation project is initiated and progresses, and examples of typical documentary evidence developed for evaluation
- Provide attendees with a decision-hinging understanding of the different levels of assurance

**Necessary Skills for Product Developers Preparing for Common Criteria Evaluations** (2 days)

- Provide attendees with an overview of how a Common Criteria evaluation project is initiated and progresses, including examples of typical documentary evidence developed for evaluation
- Equip attendees with expertise to produce evaluation evidence by providing knowledge of and ability to use the functional requirements supplied by the Common Criteria Standard
- Enable attendees to interpret security requirements and determine development approaches by providing knowledge of the assurance levels

**Introduction to Common Criteria for Developers** (2 days)

- Understand and use the CC Parts 1, 2, 3, the CEM, and additional CCEVS guidance
- Understand his or her responsibilities in an evaluation process
- Contribute to evaluation projects as a member of the evidence development team
- Contribute to authoring a Security Target

**Protection Profile Development Workshop** (1 day)

- Specify the security problem definition
- Define security objectives to address the security problem
- Specify extended component definitions

- Specify security requirements that satisfy the security objectives for the proposed TOE
- Understand how to specify security functional requirements in a PP
- Provide attendees the ability to identify and specify assurance requirements in a PP
- Understand how to address the composition problem

**ISO/IEC 27001: 2005 Lead Auditor** (5 days)

- Acquire an expertise to perform an ISMS audit as specified by ISO/IEC 27000:2005
- Acquire the expertise necessary to manage an ISMS audit team
- Understand the application of the information security management system in the ISO/IEC 27000:2005 context
- Understand the relationship between an Information Security Management System (including risk management and controls) and compliance with the requirements of different stakeholders of the organization
- Improve the ability to analyze the internal and external environment of an organization, perform risk assessments and audit decision-making in the context of an ISMS

**NASPO Certification Workshop** (1 day)

- Provide attendees with an overview of the requirements of the ANSI/NASPO Standard
- Acquaint attendees with a business justification to pursue NASPO certification
- Provide attendees with knowledge of the certification process, procedures, and the challenges that may arise
- Enable attendees to interpret the difference between Class I, Class II, and Class III certification of compliance

**Workshop for IT Security in the U.S. Health Industry** (1 day)

- Understand the basic IT security and privacy requirements for products that are legislated by HIPAA and HITECH acts
- Understand the product certifications available to support conformance claims
- Understand how supportive certifications relate to legislation and requirements

**FIPS 140-2 Validation Requirements** (2 days)

- Understand FIPS 140-2 security requirements for each level
- Understand testing requirements
- Understand the required Security Policy content

*For more information contact us at info@atsec.com*
*or visit http://www.atsec.com/us/trainings.html*

## Featured online workshops:

**Introduction to FIPS 140-2** (1/2 day)

A Brief History

Three Decades of Evolution of Cryptographic Module Standards in the U.S. and ISO

*http://www.atsec.com/us/presentations/fips140-2.html*

**Protection Profile Development Workshop**

Protection Profile – Content

Mandatory Content

- A PP introduction containing a narrative description of the TOE type
- A security problem definition, showing threats, Organizational Security Policies and assumptions
- Security objectives, showing how the solution to the security problem is divided between security objectives for the TOE and security objectives for the operational environment of the TOE
- Security requirements (functional and assurance)

These are the mandatory parts, not necessarily sufficient to understand and use the PP!

*Please contact us if you are interested in this online training.*

## Upcoming Course

**FIPS 140-2 Validation Requirements**
(2 days)

**Tuesday, August 2nd 2011 – 9am to 5pm**
**Wednesday, August 3rd 2011 – 9am to 3pm**

- Venue: Homewood Suites
  10925 Stonelake Blvd
  Austin, TX 78759
- Course fees: Registered by July 1st: $1200
  Registered after July 1st: $1400

*For more information and registration:*
*http://atsec.com/us/fips-140-2-course.html*

NEWS

## atsec Accredited as a NASPO Third-Party Auditor

atsec information security is pleased to announce its accreditation as a third-party auditor for the North American Security Products Organization (NASPO). atsec completed the necessary training from NASPO and can now conduct audits required to attain certification under the ANSI/NASPO-SA-2008 standard.

NASPO was founded in 2002 by companies and individuals in the security products industry who recognized the need for the control of secure products and technologies. To provide a recognized framework, NASPO developed an authoritative set of standards and auditing practices focused on the principle of control using the concept of risk management. As an accredited ANSI standards development organization NASPO also contributes to the development of standards for national identity proofing and verification.

Fiona Pattinson, Director of Business Development & Strategy for atsec, commented: “We are looking forward to bringing atsec’s long-standing experience of performing security audits and assessments under a variety of U.S. and international IT security standards, such as the FISMA risk management framework, PCI DSS, and ISO/IEC 27001 to bear under the NASPO scheme. The addition of this service to atsec’s portfolio supports our customers who need to provide security assurance to their stakeholders by demonstrating compliance with important security standards. This service complements our existing offerings to customers in the security document supply chain, which includes product compliance to standards such as FIPS 201, FIPS 140-2, and Common Criteria.”

## Wind River Achieves Common Criteria Certification for Linux Secure 1.0 at EAL 4+

atsec information security is pleased to announce the successful Common Criteria certification of Wind River Linux Secure at EAL 4+ (augmented by flaw remediation), using the U.S. Government Protection Profile for General-Purpose Operating Systems in a Networked Environment. Wind River Linux Secure is the first commercial, embedded Linux operating system accepted by NIAP, enabling Linux to be deployed securely on hardware from multiple vendors, including Freescale, Intel, and Texas Instruments Incorporated.

atsec information security performed the Common Criteria evaluation and the FIPS 140-2 testing that was part of the overall scope of the evaluation. This testing was performed in atsec’s U.S. government accredited laboratories in Austin, TX.

Kenneth Hake, Common Criteria laboratory manager, commented: “We congratulate Wind River on their achievement of Common Criteria EAL4+ certification for Wind River Linux Secure. We are also happy about the decision to have both the Common Criteria evaluation and FIPS 140-2 testing done by the atsec laboratories. It shows that you can save time and effort by using a company that is proficient in a wide variety of IT security standards.”

“The need for embedded Linux with security assurance is growing across markets, as organizations must meet increasingly demanding security requirements. With Wind River Linux Secure, customers can meet their security needs with an open architecture software platform designed to comply with national security criteria, based upon a mature and widely-used Linux distribution,” said Paul Anderson, vice president of marketing and strategy for Linux products at Wind River. “Wind River partnered with atsec information security because it was essential to find a partner with strong expertise and history in evaluating operating systems per the Common Criteria guidelines.”

Under Common Criteria, products are evaluated against strict standards for various features, including security functionality, development environment, security vulnerability handling, documentation of security-related topics, and product testing.

### CONTACT US

**atsec information security corporation**
9130 Jollyville Road, Suite 260
Austin, TX 78759
USA

Phone: +1 512 615 73 00
Telefax: +1 512 615 73 01
Email: info@atsec.com