atsec NEWS 06/2011
the information security provider

最近新闻一览

更多新闻，请浏览我们的网站
www.atsec.com

atsec 被授权成为 NASPO 的第三方审计机构

atsec 信息安全很荣幸地宣布得到北美安全产品组织（NASPO：North American Security Products Organization）的认可并成为第三方的审计机构。在该角色中，atsec 将基于 ANSI/NASPO-SA-2008 标准为需要获得认证的机构执行审计，并且已经完成了来自 NASPO 的必要的培训。

由于认识到控制安全产品与技术的需要，NASPO 于 2002 年由安全产品行业的公司与个人发起建立。为了提供一个认可的框架，作为一个被认可的 ANSI 标准开发组织，NASPO 开发了一套权威的标准与审计实践，集中于运用风险管理的控制原则。NASPO 还贡献于开发有关国家身份校对与验证的国家标准。

atsec业务发展与战略总监，Fiona Pattinson指出：“我们期待着推出我们在多种美国和国际的IT安全标准中（例如FISMA风险管理框架、PCI DSS以及ISO/IEC 27001）执行审计和评估的长期经验。通过将该服务引入到atsec的服务包（portfolio），展示了对重要安全标准的合规性，它可支持我们的客户为利益相关者提供安全保证。该服 务为产品在诸如FIPS 201, FIPS 140-2 以及 Common Criteria安全标准的合规方面提供了额外的补充。（其英文原文如下：“We are looking forward to bringing atsec's longstanding 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 that include product compliance to standards such as FIPS 201, FIPS 140-2 and Common Criteria.”）

atsec 是首家且目前唯一拥有中国本土经认可的 NASPO 审计师的审计机构。

atsec 将于 2011 年 7 月 29 日在北京召开国内首次 NASPO 研讨会。

atsec NEWS
the information security provider

渗透测试助力 PCI DSS 合规建设

atsec 陈谨运

渗透测试与 PCI DSS 的关系

PCI（Payment Card Industry）中文全称为：支付卡产业。在这个产业里存在一个标准组织，称为--支付卡行业安全标准委员会，英文简写为 PCI SSC（Payment Card Industry Security Standards Council）。PCI 安全标准委员会是由国际知名的五家支付品牌共同建立而成，他们是美国运通（American Express）、美国发现金融服务公司（Discover Financial Services）、JCB、全球万事达卡组织（MasterCard）及 Visa 国际组织。PCI SSC 一共维护了三个安全标准：PCI DSS（Payment Card Industry Data Security Standard 支付卡行业数据安全标准）、PCI PA-DSS（Payment Card Industry Payments Application Data Security Standard）支付卡行业支付应用数据安全标准）以及 PTS（PIN Transaction Security PIN 传输安全标准）。从下图可以很清楚的反应这三个标准之间的关系。

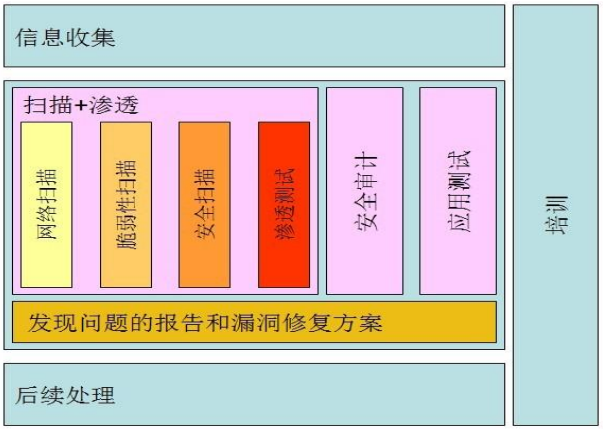
无论是 PTS 还是 PCI PA DSS，其最根本的目的是为了使最终的客户能够满足 PCI DSS 的要求。（关于 PTS 和 PA DSS 更多的介绍可参见 PCI 官方网站 www.pcisecuritystandards.org 和 atsec 官方网站 www.atsec-information-security.cn）。

在 PCI DSS 第 11.3 中有这样的要求“ Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following： Network-layer penetration tests and Application-layer penetration tests”其转译中文意思是：至少每年或者在基础架构或应用程序有任何重大升级或修改后（例如操作系统升级、环境中添加子网络或环境中添加网络服务器）都需要执行内部和外部基于应用层和网络层的渗透测试。

什么是渗透测试

渗透测试是通过模拟来自恶意的黑客或者骇客攻击，以评估计算机系统或者网络环境安全性的活动。从渗透测试的定义我们能够清楚的了解到渗透测试它是一项模拟的活动，主要的目的是进行安全性的评估，而不是摧毁或者破坏目标系统。

从下图我们可以看到，渗透测试与网络扫描，脆弱性扫描，安全扫描和安全审计其实并不相同。渗透测试是介于安全扫描和安全审计之间，它并不是纯粹的扫描工作，但是它执行的深度又没有安全审计那么深入。渗透测试是从攻击者的角度，试图通过各种技术手段或者社交手段去发现和挖掘系统的漏洞，最终达到获取系统最高权限的目的。无论是从测试的覆盖面和测试的深度来看，渗透测试都要比网络扫描，脆弱性扫描和安全扫描更为深入。



渗透测试的目的

对于渗透测试而言，除了满足某些特定标准（如 PCI DSS）的要求之外，渗透测试还会有如下的好处：

- 识别和发现机构可能被攻击的薄弱环节
- 通过外部独立的第三方评估机构的安全评估提高客户自身的安全级别和降低安全风险
- 提高人员对于信息安全的意识

渗透测试的方法论和业界参考实践

对于任何测试而言，都会相应的测试方法或者规则。在渗透测试领域，业界的渗透测试方法论或者最佳实践可以作为一个很好的参考，但是测试人员在测试过程当中更多的是依靠自身的能力和经验去完成测试工作，因为在测试过程当中可能会遇到各种各样的问题。下面是行业中被广泛接受的测试方法或者渗透测试的最佳实践：

OWASP（Open Web Application Security Project）Testing Guide – 关注在 web 应用安全测试的测试指导。该测试指导涵盖了 web 应用程序大部分功能点的安全性测试，测试指导同时会给出一些测试的实例进行简单的说明。

OSSTMM（Open Source Security Testing Methodology Manual） -- 开放源代码安全测试方法手册。OSSTMM 是一个关注在安全测试和评价的方法论。OSSTMM 的测试用例分为五个方面：

信息和数据控制；人员安全意识水平；欺诈和社会工程学控制水平；计算机和电信网络，无线设备，移动设备以及物理安全访问控制；安全流程，如建筑物，周边环境，以及军事基地的物理位置等安全流程。

Special Publication 800-115 Technical Guide to Information Security Testing and Assessment – 美国 NIST 发布的针对信息安全测试和评估的技术指导。

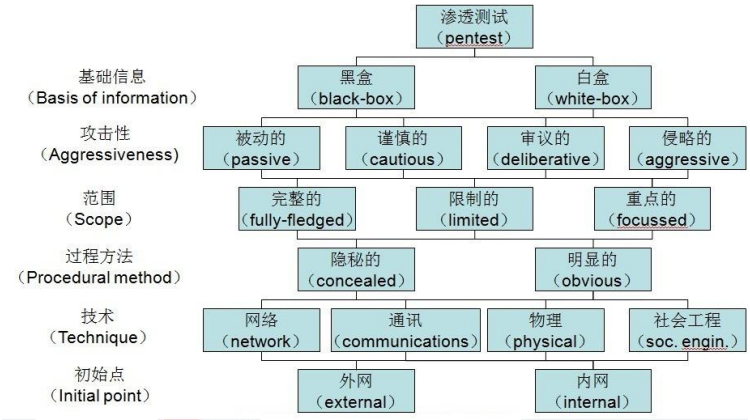
ISSAF（Information Systems Security Assessment Framework）-- 关注在信息系统安全评估的框架。

Penetration Testing Framework -- 渗透测试的框架，该测试框架是渗透测试实践的操作总结，它非常详细的描述了渗透测试过程当中每一步应该做什么，怎么去做。该份测试的框架对于渗透测试的实际操作有着非常好的参考价值。

渗透测试的流程

对于渗透测试，其流程大体包括：测试协议和方法确定，免责条款签署，信息收集，脆弱性分析，对脆弱性进行渗透和利用，权限提升，最终评估和报告编写以及客户根据渗透测试发现问题的整改和追踪等环节。以下是对于上述各个环节的简要介绍：

➢ 渗透测试与恶意黑客的攻击最大的区别就是：恶意黑客为了获得想要的信息可以不计后果对目标系统进行攻击测试，而渗透测试人员的所执行的测试活动是需要在特定的测试协议下执行的。因此在正式执行渗透测试之前，明确测试协议与测试方法是最重要的工作，测试协议与测试方法是后续测试人员开展渗透测试的参照标准。对于渗透测试协议和方法的确定，下述图示展示了 atsec 结合了前文所提及的方法论和业界参考实践的经验总结。



□ 在渗透测试中，根据客户提供信息的多少，我们可以人为的将渗透测试分为黑盒测试和白盒测试。所谓的黑盒测试是客户尽可能少的给测试人员提供测试目标的信息，测试人员在不了解目标系统的情况下展开测试。白盒测试是测试人员在完全了解系统的设计和架构或者网络配置的情况下对目标进行渗透，以确保所有安全问题都被发现了。

□ 从测试人员测试活动的攻击性的角度评价，可以将渗透测试划分成四种情况：

- □ 被动的测试活动
- □ 谨慎的测试活动
- □ 审议的测试活动
- □ 具有侵略性的测试活动

□ 从测试范围的选择，客户可以指定整体网络环境的系统组件，或者是部分的网络环境的系统组件，又或者是对于特定的目标系统进行测试。

□ 对于测试人员在测试过程当中的活动，客户可以要求测试人员隐秘的执行渗透测试活动，又或者明确测试人员并不需要隐藏测试活动可以公开执行渗透测试工作。

□ 在渗透测试活动中，客户可以要求测试人员对如下方面执行渗透测试工作：对互联网络执行渗透（如互联网上的 web 服务器，数据库服务器，网络设备等等）；对通讯执行渗透测试（如 PSTN 网络，电信网络，3G 网络等方面）；对物理安全执行渗透测试（如目标系统的物理防护，电磁辐射等方面）；执行社会工程学测试（主要是为了测试员工的安全意识）。

□ 在测试方法设定的时候，客户还可以要求测试人员以外网或者内网作为渗透测试活动的出发点。

➢ 在确定测试协议和方法之后，测试人员通常会要求客户出具一份渗透测试的免责声明，该声明中会明确声明测试人员不需要为测试过程中产生的任何风险承担法律责任。这份免责声明，对于渗透测试人员而言是很好的法律保护，因为任何的测试活动都不可能百分之百安全，在某些测试过程（如对漏洞进行渗透和利用）当中难免会存在一些安全风险，如果没有此份声明测试人员迫于法律的限制不可能完成后续的测试工作。

➢ 当完成上述两个准备阶段的工作之后，测试人员通常会进入非常重要和关键的一个环节----信息收集。在信息收集过程当中包括但不限于以下信息：IP 地址信息，关联域名信息，域名联系人信息，DNS 服务器信息，邮件服务器信息，IP 地址段路由信息，和目标系统相关的人员信息收集，目标系统漏洞信息，或者通过社会工程学从相关人员口中套取有用的信息等等。信息收集是一门比较高深的学科，如果信息收集得很好，很多时候都不需要使用技术手段对系统漏洞进行渗透利用都能获得系统的权限。

➢ 对于渗透测试而言，虽然它是一项通过模拟黑客或者骇客的攻击以评估系统或者网络环境安全性的活动，但是渗透测试比真实生活当中的攻击行为有着更多的限制。渗透测试并不以摧毁或者破坏系统的可用性为目的。在渗透测试过程当中，我们需要最大限度的保证客户业务的正常运转（当然客户的特殊要求除外），在这个前提下，尽最大可能发现和挖掘目标系统的脆弱性并进行利用。

因此，在进行真正渗透之前，我们通常需要对发现的脆弱性进行分析，分析和评估该脆弱性可能会对目标系统造成的影响，并制定相应的应急预案。对于脆弱性的分析通常会借助外部的脆弱性扫描工具如 Nessus，QualysGuard ，WebInspect 或者是 Nikto2 等等进行脆弱性的发现和识别，测试人员会根据所发现脆弱性的类型，CVE（Common Vulnerabilities and Exposures）依据 CVSS（Common Vulnerability Scoring System）对于脆弱性的评分，客户被测目标系统所处的实际环境等因素进行综合考虑以进一步对脆弱性进行分析。在 PCI DSS 第 11.2 中要求客户需要每个季度或者在基础架构或应用程序有任何重大升级或修改后（例如操作系统升级、环境中添加子网络或环境中添加网络服务器）都需要执行内部和外部脆弱性扫描。外部 脆弱性扫描是需要由 PCI SSC 授权的扫描服务提供商执行，业界的术语叫做 ASV（Approved Scanning Vendors）。目前 PCI DSS 对于外部脆弱性扫描活动不仅仅要求需要由 ASV 开展，对于实际执行脆弱性扫描的人员也需要经由 PCI SSC 进行培训，考核并获得相应资质证书之后才能出具具有资格的扫描报告。在渗透测试脆弱性分析的阶段，测试人员可以参考客户提供最近的 ASV 扫描报告作为脆弱性分析的输入数据。

- 在完成对脆弱性分析之后，测试人员会根据与客户之间的渗透测试方法和协议进一步对脆弱性进行渗透或者利用。在测试过程当中，渗透测试人员可能在初次攻击完成之后获得了有限的权限，此时渗透测试方法和协议则是测试人员最好的参考。如果客户允许执行进一步的权限提升操作，测试人员则可能会尝试将以获得的权限提升至管理员级别或者系统级别的权限。
- 在完成对脆弱性的渗透和利用之后，测试人员会对渗透的结果进行评估和判断，以确定脆弱性的可利用价值，同时渗透测试的过程以及测试过程中发现信息将会被编写到最终的渗透测试报告当中。对于在渗透测试过程当中，由于特定的原因（如客户的要求，漏洞利用条件的限制等等）导致脆弱性并没有被实际测试，测试人员将会在报告当中描述恶意人员可能对该脆弱性使用的攻击方法以及该脆弱性被成功利用后可能带来的安全风险。
- 客户根据渗透测试报告中所发现的脆弱性以及测试人员提供的解决方法进行脆弱性修复。对于完整的渗透测试流程通常还会包含对修复后的脆弱性进行验证测试，从第三方的角度去评估脆弱性修复的有效性。

基于应用层和网络层的渗透测试

对于 PCI DSS 第 11.3 中有要求至少每年或者在基础架构或应用程序有任何重大升级或修改后需要执行内部和外部基于应用层和网络层的渗透测试。应用层渗透测试指的是对 web 应用程序进行渗透测试，测试要求覆盖 OWASP Top 10（OWASP 项目组会周期性的根据 OWASP 联盟中应用开发和测试专家反馈的结果定期对 web 应用面临的安全问题进行统计和排名，Top 10 是 web 应用程序前 10 名影响最大的脆弱性）中的所有安全问题。对于网络层的渗透测试，通常是指对操作系统，网络设备等系统组件进行系统级别的渗透测试。

下图是 2007 年和 2010 年 OWASP Top 10 的排名对比。从图中可以看到 Top 10 的内容在这两年的评估当中出现了变化。所以在渗透测试过程当中我们除了参照 PCI DSS 的要求之外，还需要参照 OWASP 最新的关于 Top 10 的排名情况。

OWASP Top 10 – 2007 排名		OWASP Top 10 – 2010 排名
A2 – Injection Flaws	↑	A1 – Injection
A1 – Cross Site Scripting (XSS)	↓	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	↑	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	=	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	=	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	+	A6 – Security Misconfiguration (NEW)
A8 – Insecure Cryptographic Storage	↑	A7 – Insecure Cryptographic Storage
A10 – Failure to Restrict URL Access	↑	A8 – Failure to Restrict URL Access
A9 – Insecure Communications	=	A9 – Insufficient Transport Layer Protection
<not in T10 2007>	+	A10 – Unvalidated Redirects and Forwards (NEW)
A3 – Malicious File Execution	-	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	-	<dropped from T10 2010>

怎样选择合适的渗透测试合作机构

前面介绍了很多关于渗透测试介绍，以及测试流程和方法，然而我们在实际执行渗透测试工作的时候，应该如何选择合适的渗透测试实验室或者渗透测试人员进行测试工作呢？对于渗透测试人员的选择，PCI DSS 在第 11.3 的要求：测试人员可以是内部具有能力且独立的内部人员或者外部合格的第三方评测机构。对于内部人员的选择，技术能力的考虑和测试人员的独立性是最为重要的因素。对于第三方的评测机构的选择，除了技术水平的考虑，以下的参考因素能够为客户在渗透测试过程当中可能会面临的安全风险提供很好的安全保障。

- 专一性，IT 安全是否是该公司的主营的业务？
- 该公司自身是否切实执行 IT 安全流程？
- 评估机构和他们员工是否具有相关的资质？
- 该评估机构是否为行业的领导者，帮助或者能够分享相关的标准信息？
- 该机构是否具有相关的成功项目经验？
- 该评估机构是否能够提供除渗透测试以外其他能够提高客户流程等有价值的服务？
- 该评估机构是否能够在很多不同的技术领域提供专业知识和经验？
- 评估机构安全评测的独立性，是否能够为客户提供第三方独立的不带任何偏见的评估报告？
- 该评估机构是否为客户提供足够的保险和合理的法律协议保障？
- 谁是该评估机构的服务客户？

采用 NASPO 标准进行风险管理

atsec 张力

NASPO 的使命是开发国家和国际反措施与控制标准，用以验证在金融交易、身份管理与材料物品领域针对这些标准的合规性。NASPO 使得安全产品公司能够分类与验证他们在整个操作过程中高（一级）、中（二级）或基本（三级）安全保障的交付能力。

NASPO 设计标准旨在帮助认证组织识别与定义不正当的获取、规避、模拟和破坏安全产品或信息的风险。NASPO 认证的提供商的最终用户选择增强供应产品与材料的安全价值，这是通过控制与约束对安全技术与信息的访问来实现的。

NASPO认证的目的是证明由NASPO认证组织所提供的产品、服务与技术不可能由欺诈活动或过失所破坏。

角色

有四种不同的角色参与在 NASPO 组织中。

- 制造商（Producers）

提供安全产品的制造商必须理解对他们的客户与公众的内在责任，未能保护制造业环境的制造商对整个安全产品产业的可信性是一种威胁。由于这个原因，NASPO 区分未通过认证的安全产品制造商与通过认证的安全产品制造商。

- 供应商（Suppliers）

供应商有责任确保在安全生产厂商利用的原材料是经授权和负责任的方法小心分发的。失败保障供应链将导致伪造产品的增加，那将是非常危险的，将付出昂贵的代价。NASPO 认证供应商及他们的操作以减缓这些风险。

- 品牌所有者（Brand Owners）

品牌保护在现代社会中是最为困难的挑战之一。估计世界范围内销售的 15%以上的品牌产品是伪造的。NASPO 提供了一种方法来保护品牌所有者，即通过认证所有链条，包括产品被制造前以及产品离开工厂后的分发链。

- 安全顾问（Security consultant ）

随着 NASPO 的成长，有一种增长的需求，要求合格的个体能够在风险减缓与供应链安全方面提供建议与咨询给制造商、供应商与品牌拥有者。咨询资格要求有安全文档制造、法律执行、审计与计费方面的背景。

随着 NASPO 的成长，有一种增长的需求，要求合格的个体能够在风险减缓与供应链安全方面提供建议与咨询给制造商、供应商与品牌拥有者。

范围

NASPO需求仅应用于风险管理（控制），这种潜在的风险会降低或消除安全技术、产品或服务的价值。NASPO标准并不关注产品或服务的内在功能的安全价值。由于这些原因，NASPO倾向依赖市场来评估特性，诸如防伪造、防篡改、追踪特性、认证价值与辩论证据价值等。

管理的风险包括：

- 客户相关的风险（Customer Related Risks）
- 信息风险（Information Risks）
- 安全材料风险（Security Material Risks）
- 供应链风险（Supply Chain Risks）
- 物理入侵风险（Physical Intrusion Risks）
- 人员风险（Personnel Risks）
- 灾难恢复风险（Disaster Recovery Risks）
- 安全失效风险（Security Failure Risks）
- 安全管理风险（Security Management Risks）

认证

每个 NASPO 成员必须维护一套一致的标准与操作协议。这将保证需要安全产品或服务的品牌拥有者、产品制造者与客户能够证明作为一个 NASPO 成员公司在它的认证级别内操作。成员公司需要 NASPO 合格的审计员一年执行一次认证，将在成员公司的工厂执行现场认证。

拥有良好声誉的制造商、供应商、品牌拥有者与咨询顾问可以获得 NASPO 成员资格，NASPO 成员资格仅被 NASPO 合格审计员审计完成，NASPO 审计员将帮助品牌拥有者、产品生产厂商与消费者建立组织结构与认可的安全级别。

NASPO标准说明了申请NASPO三个级别认证的组织所必须遵从的安全保障的标准，内容包括：

- 组织必须管理的风险区域
- 1、2、3级认证的差别
- 采用的风险降低方法所必须满足的目标
- 风险降低基础设施、系统与过程的类型，这些类型必须被实现已遵从1、2或3级认证
- NASPO审计员遵循的过程，用以验证组织所声称的安全保障级别事实上是符合的

atsec 拥有众多的 NASPO 审计员，可以从事相关的审计工作，并颁发最终证书。

安全保障级别

针对最终用户，安全产品或服务的价值是一综合体现，包括所交付的安全功能、花费、制造者阻止所有下列欺诈活动的程度。

- 窃取最终产品或关键组件
- 窃取关键技术数据
- 窃取关键产品专门技能或设备
- 窃取辩论特征数据
- 假冒忠诚客户

- 窃取原材料
- 窃取与公开机密或个人信息

一级认证（**Class I** certified）：期望交付非常高级别的安全保障，通过预测和有效控制所有形式的欺诈活动，使尝试活动能被消除。在欺诈活动发生的事件中，一级认证组织必须做好准备以完全减轻他们的影响。

二级认证（**Class II** certified）：制造安全产品或提供安全服务的组织，对于欺诈活动所产生的后果是轻微的，但必须维持高级别的安全保障。这种保障级别必须是符合要求的，足以保护最终用户在安全产品或服务中的投资。在欺诈活动发生的事件中，二级认证组织必须做好准备以充分减轻他们的影响。

三级认证（**Class III** certified）：不集中于安全产品，也不排除制造安全产品。这些产品基本上仅遭受很小经济损失与有限后果的威胁。因此，专业的安全保障不必被担保，但必须是符合要求的，足以保护最终用户在安全产品中的投资。三级认证组织必须有合适计划以减轻欺诈活动发生时所产生的效果。

市场

有良好声誉的 NASPO 成员是受欢迎的，鼓励其运用 NASPO logo 在他们的市场材料中。认证成员被鼓励运用 NASPO 认证 logo。这提供了公司对客户的安全利益的承诺的不同级别。

NASPO 主要集中在北美市场，但认证全球的用户。如果一个美国或加拿大以外的公司想要卖安全产品或服务到北美市场，获得 NASPO 认证将提升他们产品与服务的竞争性。

下列产品或服务的制造者或供应者将成为潜在的审计客户：

- 文档安全（电子护照、电子驾照、ATM卡等等）
- 品牌保护服务（涉及行业：奢侈品、药剂、汽车配件、化妆品、玩具等等）
- 航空绝缘材料
- RFID应答器等等

联系我们

艾特赛克（北京）信息技术有限公司
北京市海淀区上地七街1号2号楼119室
100085
电话：84834011
传真：82890017
Email:info_cn@atsec.com

atsec开展为期一天的NASPO研讨会

atsec将于2011年7月29日在北京召开国内首次NASPO研讨会。

北美安全产品组织（NASPO：North American Security Products Organization），是一个非盈利的组织，创建于2002年。于2004年被ANSI认可作为一个美国国家标准开发组织（SDO：Standards Development Organization）。符合ANSI/NASPO-SA 2008的认证证书被组织在美国境内外所使用，以展示其满足由不同采购机构所指定的安全保障标准要求。

课程目标

学员将了解到NASPO认证的微妙之处，以及它是如何在业务成功中扮演关键的角色。

具体目标为：

- 为学员概述ANSI/NASPO标准的要求
- 使学员了解实行NASPO认证的商业原因
- 为学员提供认证过程、流程以及可能遇到的挑战的相关知识
- 使学员了解符合不同级别（一级、二级和三级）认证的差异

目标对象

该课程面向有意获得NASPO认证的公司安全管理者。

课程周期和类型

本课程设置为一天。

本课程将以研讨会的形式展开，包括讲演、教师指导的讨论。

培训资料和证书

参加本课程将获得由atsec颁发的（课程完成）证书。

讲师和语言

本次培训讲师为 atsec 的资深顾问。

培训的语言采用中文。

价格

培训的价格为每位学员 3,000 元 人民币。

本价格包括培训、午餐，以及证书费用。

时间和地点

培训时间：2011 年 7 月 29 日

培训地点：北京，详细地址在完成报名后提供。

联系人： 白海蔚 李丽
Email： haiwei@atsec.com lily@atsec.com
联系电话：+86 10 84834011
传真： +86 10 82890017