atsec information security
Tel: +86-10-82893001
Fax: +86-10-82890017
www.atsec.com

本文为 atsec 和作者技术共享类文章，旨在共同探讨信息安全业界的相关话题。转载请注明：atsec 和作者名称。

采用 NASPO 标准进行风险管理

atsec 张力 2011 年 5 月

关键词：NASPO

NASPO（North America Security Product Organization：北美安全产品组织）是一个非盈利的标准组织，由于认识到控制安全产品与技术的需要，于 2002 年由安全产品产业的公司与个人发起建立。为了提供一个认可的框架，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 (North American Security Products Organization) is a not-for-profit standards organization, which was founded in 2002 by companies and individuals in the security products industry that 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.

目的

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。

为了获得NASPO认证，组织必须识别可能的欺诈活动，认识他们对安全产品价值的威胁，实现预防他们的反措施，设置合适的的计划，以及运用他们以减轻欺诈行为发生时所产生的影响。

角色

有四种不同的角色参与在 NASPO 组织中，每一种角色被描述如下：

- 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）

atsec information security

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。

范围

NASPO需求仅应用于风险管理（控制），这种风险会潜在的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

参考文献

[1] NASPO Homepage. http://www.naspo.info

[2] NASPO standard