



**NASPO**

NORTH AMERICAN SECURITY PRODUCTS ORGANIZATION

# **Security Risk Management Requirements Definition Document**

## **Overview for Prospective Members**

**Version 4.0**  
**September 24, 2003**  
© NASPO 2003

**2300 N Street, NW, Washington, D.C. 20037-1128, U.S.A.**

[www.naspo.info](http://www.naspo.info)

## Standards Document Summary

The standards document identifies and defines risks that a security product producer must manage and the degree to which those risks must be managed to be certified by NASPO as a Class I, II or III security product(s) producer. The risks defined are actions that criminals might take to fraudulently acquire, circumvent, mimic or subvert security products or information.

To obtain NASPO Certification, organizations must demonstrate a sharp awareness of possible fraudulent actions, recognize that they pose a threat to the value of their security products, implement countermeasures aimed at preventing them, put plans in place and be prepared to use them to mitigate their effects in the event that fraudulent acts occur.

The standards content enables security product producers, who know their product and customer needs for security assurance, to classify and officially certify themselves with the ability to deliver either a high, medium or basic level of security assurance.

Conversely, customers or security product end users who know their need for security assurance can use the content to specify their requirements broadly, by selecting a Class of Certification, or more specifically by choosing areas of risk and methods that suppliers must use to reduce those risks.

Either way, in this document, NASPO conveys a clear understanding of what is meant by **security assurance** (in the context of the anti-fraud industry) combined with an objective system for specifying, standardizing, quantifying and verifying the degree to which it is delivered.

NASPO has developed an organized system of credits that represent the **best practices** found in high security (NASPO Class I), medium security (NASPO Class II) and basic security (NASPO Class III) product organizations within the Industry. Credits are awarded by NASPO Auditors for the verifiable existence and use of these best practices which NASPO terms "Accreditation Criteria". The Accreditation Criteria represent specific risk reduction infrastructure, systems and techniques that assure security.

Organizations seeking NASPO Certification can determine their readiness by using the NASPO Audit Application Form & Guidelines. By carrying out a self assessment of compliance, applicants will be able to see where they stand relative to their likelihood of success. To be prepared, it is important that applicants come close to satisfying all of the mandatory Accreditation Criteria specified for each class. The system of awarding points is detailed in the document. Overall, Certification will depend on NASPO Auditors being satisfied that the Risk Management Objectives are actually being met. This means that the risk reduction infrastructure, systems, and techniques must be properly implemented and used and not just exist.

Verification that the required class of security assurance is being delivered will be the responsibility of NASPO Auditors. An outline of the audit process and the methods of verification are documented. The background to the development of these consensus standards and legal matters are also covered.

## Elements of the NASPO Standards

### Purpose

The purpose of NASPO Certification is to demonstrate to end-users that investment in the security value of NASPO Certified Organization products are unlikely to be undermined by fraudulent acts or supplier negligence.

To obtain NASPO Certification, organizations must demonstrate a sharp awareness of possible fraudulent actions, recognize that they pose a threat to the value of their security products; implement countermeasures aimed at preventing them, put plans in place and be prepared to use them to mitigate their effects in the event that fraudulent acts occur.

### Security Value of Products and Services

The goal of most security products and services is to prevent fraud. The function performed is that of a deterrent. Other security products perform a track and trace function and some combine track and trace with the power to deter. Track & trace products enable their users to detect fakes and furnish forensic evidence.

Products and services that are available to perform these functions we refer to as Security End Items (SEI's). Some are complete systems (or packages) such as passport documents, printers and readers. Some are components that require integration such as special inks, taggants, laminates and security devices. The goal of NASPO is to certify that the makers and suppliers of SEI's are bona-fide, observe a security industry code of practice and properly manage security risks to the benefit of themselves, their customers, end-users and the public at large.

### Scope of NASPO Requirements

The NASPO Requirements set forth in the document apply only to the management (control) of risks that have the potential to either reduce or eliminate the value of a security product or service. The NASPO requirements **do not** address the intrinsic functional security value of a product or service, or in any way imply that a product or service is of security value. NASPO intends to rely on the market for security products and services to evaluate properties such as; counterfeit resistance, alteration resistance, track and trace performance and forensic evidence value.

NASPO will make no determination of the level of security and therefore Class of Certification required for individual products or organizations unless a NASPO Auditor believes that a major mismatch exists between the class applied for and level of Security Assurance that should accompany a specific security product.

### Classes of Security Assurance

**NASPO Class I** Certified Organizations will be expected to deliver a very high level of Security Assurance by anticipating and effectively controlling all credible forms of fraudulent action to the point where attempts are eliminated because the barriers appear insurmountable and the chance of success appears non-existent. In the event that fraudulent acts do occur, organizations in Class I must be prepared to fully mitigate their effects.

**NASPO Class II** Certified Organizations make security products where the consequences of fraudulent action are less serious, but still must maintain a high level of Security Assurance. This level of assurance must be satisfactory and sufficient to protect the end-user's investment in the

security product. In the event that fraudulent acts do occur, organizations in Class II must be prepared to substantially mitigate their effects.

**NASPO Class III** Certified Organizations (unlike Class I & II organizations) are not focused on, and/or do not exclusively manufacture security products. Those products produced, generally suffer only from the threat of minimal economic loss and have limited consequences. As a result, full time Security Assurance may not be warranted but must be satisfactory and sufficient to protect the end-users investment in the security product. Organizations in Class III must have plans in place to mitigate the effects of fraudulent acts should they occur.

### **Risks to be Managed**

Regardless of the Class of Certification, all NASPO Certified Organizations will be expected to deliver Security Assurance that addresses and controls the following areas of risk to a greater or lesser degree :

- Customer Related Risks
- Information Risks
- Security Material Risks
- Supply Chain Risks
- Physical Intrusion Risks
- Personnel Risks
- Disaster Recovery Risks
- Breach of Security Risks
- Other Risks

All audits carried out by NASPO will aim to verify that organizations have developed a sharp awareness of possible fraudulent actions specific to their security product portfolio, recognize that they pose a threat to the value of their security products, implement countermeasures aimed at preventing them, put plans in place and be prepared to mitigate their effects in the event that fraudulent acts occur.

### **Risk Management Objectives and Certification Criteria**

This portion of the standard specifies each of the areas of risk as outlined in Risks to be Managed, and provides for an evaluation of individual criteria for each of the classes. This is the key objective component in the evaluation process used by NASPO Auditors. It outlines each Accreditation Criteria and provides a numerical evaluation for the determination of the Certification level of each organization.

### Security Assurance – Verification

Verifying delivery of Security Assurance by NASPO Certified Organizations will be the responsibility of NASPO Auditors. To validate that Security Assurance is being delivered in accordance with the requirements of the class for which the organization is seeking Certification, trained auditors will use a combination of the following:

- Documentary Evidence
- Experience Reports
- Analysis Reports
- Interviews
- Site Visits
- Simulations
- Similarity with other Proven Systems
- Demonstration
- Testing

All NASPO audits will be carried out under a strict Confidentiality Agreement.

NASPO audits will be conducted under the highest level of confidentiality. No elements of the audit will be discussed or evaluated by the Auditors with other NASPO members. The status of audits shall be recognized by the terms: "Certified", whereby all criteria have been evaluated by the auditor, passed and approved by the Standards Board or, "Pending", indicates that an audit is in process and is awaiting the completion of variance issues or Standards Board approval. In the event that an organization fails to comply, auditors will require a plan for rectification and will return to the organization to verify that rectification has taken place. No audited member shall ever be deemed "failed". At no time will the actual audit results be made public.

### Legalities

The use of the standards is voluntary to non-certified security product producers and end users.

The Certification process is based upon the voluntary implementation of risk reduction infrastructure, systems and procedures followed by a mandatory audit by trained NASPO Auditors. The training received by NASPO Auditors is available to independent auditors under the terms and conditions of a licensing agreement. NASPO retains the right to withhold or revoke such licensing agreements as the Board deems appropriate.

Under no circumstances shall the NASPO standards be implied as a restriction of trade. The lawful right of free enterprise will prevail regardless of NASPO Certification.

The set of standards issued by the North American Security Products Organization may be revised or revoked at any time. The standards must be reviewed in its entirety by the Standards Review Committee every two years. Any revision or revocation of standards presented by this committee must be approved by a majority of a quorum in attendance at a NASPO meeting designated by the board of directors.

For all Classes of Certification, there shall be no right of appeal following the submission of an Auditors Final Report and Certification review by the NASPO Board of Directors.