ASIS INTERNATIONAL GUIDELINES COMMISSION

The ASIS International Guidelines Commission was established in early 2001 by ASIS International (ASIS) in response to a concerted need for guidelines regarding security issues in the United States. As the preeminent organization for security professionals worldwide, ASIS has an important role to play in helping the private sector protect business and critical infrastructure from terrorist attacks. Whereas ASIS previously had chosen not to promulgate guidelines and standards, the events of 9/11 brought to the forefront the need for a professional security organization to spearhead this initiative. By addressing specific concerns and issues inherent to the security industry, security guidelines will better serve the needs of security professionals by increasing the effectiveness and productivity of security practices and solutions, as well as enhance the professionalism of the industry.

Mission Statement of the ASIS Guidelines Commission
To advance the practice of security through the development of risk mitigation guidelines within a voluntary, non-proprietary, and consensus-based process utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS membership and the security industry.

Goals and Objectives
- Assemble and categorize a database of existing security-related guidelines
- Involve/organize ASIS Councils to support guidelines
- Develop and sustain alliances with related organizations
- Develop methodology for identifying recommended guidelines
- Identify and develop methodology for development, documentation, and acceptance of guidelines
- Produce national consensus-based guidelines in cooperation with other industries and the Security Industry Standards Council

Functions
- Assignment of guideline committee(s)
- Approve membership on guideline committees(s)
- Determine/select guidelines for development and assign scope
- Establish guideline projects to develop security guidelines
- Act as a correlating body to effectively manage and integrate guidelines from various ASIS Councils and security disciplines
- Monitor, revise, and update ASIS’ Glossary of Terms
- Review and monitor projects and project guideline development
- Approve Final Draft Guidelines
- Adjudicate appeals
- Select guidelines for submission to the Security Industry Standards Council for accreditation as American National Standards
I. Title
The title of this guideline is *The General Security Risk Assessment Guideline*.

II. Revision History
November 13, 2002    Guideline approved

III. Commission Members
Sean Ahrens, CPP
Norman Bates
Chad Callaghan, CPP
Pamela Collins, EdD, CFE
Grant Crabtree, CPP
Michael Crane, CPP
Edward Flynn, CFE
Arthur Kingsbury, CPP
Michael Stack
Basil Steele, CPP
Don Walker, CPP
Timothy Walsh, CPP
Timothy Williams, CPP

IV. Keywords
Risk, Assessment, Vulnerability, Threat, Asset, Security Survey

V. Guidelines Designation
This guideline is designated as ASIS GLCO 01 01 2003.

VI. Scope
This guideline is applicable in any environment where people and/or assets are at risk for a security-related incident or event that may result in human death, injury, or loss of an asset.

VII. Summary of Guideline
The General Security Risk Assessment seven-step process creates a methodology for security professionals by which security risks at a specific location can be identified and communicated, along with appropriate solutions. The guideline also includes definitions of terms, a process flow chart, illustrative material in appendices, and references/bibliography.

VIII. Purpose
To provide a methodology for security professionals by which security risks at a specific location can be identified and communicated, along with appropriate solutions.
IX. Terminology

Assets
Any real or personal property, tangible or intangible, that a company or individual owns that can be
given or assigned a monetary value. Intangible property includes things such as goodwill, proprietary
information, and related property. For purposes of this guideline, people are included as assets.

Consequential
A secondary result ensuing from an action or decision. From an insurance or security standpoint,
costs, loss, or damage beyond the market value of the asset lost or damaged, including other indirect
costs.

Cost/Benefit Analysis
A process in planning, related to the decision to commit funds or assets. This is a systematic attempt
to measure or analyze the value of all the benefits that accrue from a particular expenditure. Usually,
this process involves three steps:

- Identification of all direct and indirect consequences of the expenditure.
- Assignment of a monetary value to all costs and benefits resulting from the expenditure.
- Discounting expected future costs and revenues accruing from the expenditure to express
  those costs and revenues in current monetary values.

Criticality
The impact of a loss event, typically calculated as the net cost of that event. Impact can range from
fatal, resulting in a total recapitalization, abandonment, or long-term discontinuance of the enterprise,
to relatively unimportant.

Events
Something that happens; a noteworthy happening. In the security context, this usually represents an
occurrence such as a security incident, alarm, medical emergency, or related episode or experience.

Goodwill
The value of a business that has been built up through the reputation of the business concern and its
owners.

Loss Event
An occurrence that actually produces a financial loss or negative impact on assets. Examples include
security incidents, crimes, war, natural hazards, or disasters.

Natural Disaster
A naturally occurring calamitous event bringing great damage, loss, or destruction such as tornadoes,
hurricanes, earthquakes, and related occurrences.
**Probability**
The chance, or in some cases, the mathematical certainty that a given event will occur; the ratio of the number of outcomes in an exhaustive set of equally likely outcomes that produce a given event to the total number of possible outcomes.

**Qualitative**
Relating to that which is characteristic of something and which makes it what it is.

**Quantitative**
Relating to, concerning, or based on the amount or number of something, capable of being measured or expressed in numerical terms.

**Risk**
The possibility of loss resulting from a threat, security incident, or event.

**Risk Analysis**
A detailed examination including risk assessment, risk evaluation, and risk management alternatives, performed to understand the nature of unwanted, negative consequences to human life, health, property, or the environment; an analytical process to provide information regarding undesirable events; the process of quantification of the probabilities and expected consequences for identified risks.

**Risk Assessment**
The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel.

**Security Incident**
A security-related occurrence or action likely to lead to death, injury, or monetary loss. An assault against an employee, customer, or supplier on company property would be one example of a security incident.

**Security Vulnerability**
An exploitable capability; an exploitable security weakness or deficiency at a facility, entity, venue, or of a person.

**Site**
A spatial location that can be designated by longitude and latitude.

**State-of-the-Art**
The most advanced level of knowledge and technology currently achieved in any field at any given time.

**Statistics**
A branch of mathematics dealing with the collection, analysis, interpretation, and presentation of masses of numerical data. In security, this could represent a collection of quantitative data such as