**Role of Security System Key Terms**

Criticality – a term used to help separate vulnerabilities into smaller, specific categories; also means the impact of a loss as measured in dollars

Intentional Threats – purposeful and deliberate crimes by an unknown person or group that results in some form of damage; these crimes include espionage, identity theft, computer hacking and terrorism

Natural Threats – global and environmental threats; these threats include natural disasters such as floods, earthquakes, tornadoes, hurricanes, and storms

One-Dimensional Security – relies on a single deterring factor (i.e. guards) Operational Audit (OA) – a comprehensive and accurate analysis that leads to effective

countermeasures; it consider all aspects of the security operation on a continuing basis; a methodical examination, or audit, of operations (Fischer and Green, 1998)

Packaged Security – standard security systems (equipment, personnel, or both) without a connection to any specific threats and with the assumption that packaged systems will take care of all problems

Piecemeal Security – security systems that have individual pieces added to the loss prevention function as the need arises, without a comprehensive plan

Probability – involves the chance that something will happen and typically involves the use of mathematics

Programmed Supervision (PS) – making sure that a supervisor or other employees go through a prescribed series of inspections that will determine whether the functions or procedures for which they are responsible are being properly executed (Fischer and Green, 1998)

Reactive Security – security systems that respond only to specific events of loss Risk Analysis – the overall role of security management that includes identifying potential areas of loss and developing/installing appropriate security countermeasures

Risk Avoidance – a technique used to avoid or eliminate a risk, problem, threat, or hazard

Risk Management – management techniques that identify, analyze, and assess risks/threats; if a risk/threat is detected, methods are employed to manage it

Risk Reduction – decreasing threats to safety and security whenever possible

Risk Spreading – decentralizing a procedure or operation so that a security or safety problem at one location will not cause a complete loss (Fischer and Green, 1998)

Risk Transfer – removing the risk to the company by paying for the protection of an insurance policy (Fischer and Green, 1998)

Security Survey – an assessment used to identify potential problem areas Self-assumption of risk – planning for the worse by creating a plan for an eventual loss

without insurance

Unintentional Threats – occur accidentally or by chance (i.e., a person accidentally unplugging a computer cord or reformatting a computer hard drive)

Vulnerability Analysis – (a.k.a. security survey) the method used to determine a threat or the vulnerability of a location