

The process of evaluating a hotel's security capability must be pragmatic, practical and reasonable. That process begins with an awareness and understanding of the legal principles that shape the manner in which a hotel seeks to fulfill its legal and moral duty concerning safety and security. Unaware of the long history of litigation concerning premise security liability, key accounts often seek to evaluate a hotel's security capability by asking questions that often overlook fundamental components of a viable and defensible security program. Those issues would include (but are not limited to):

- Access Control – (i.e. management and control of electronic locking systems)
- Physical Security – (i.e. Fire rated guest room doors, high quality electronic locks, secondary locks, one-way viewing device, CCTV, parking area illumination etc.)
- Guest Information/Data Security
- Fire Safety – (Dead end corridors, fire suppression systems, fire safety planning and emergency response planning)
- Emergency Response Procedures: Evacuation planning and training, Active Shooter, Bomb Threats
- Security Personnel – (In house vs. contract, training, equipment, etc.)
- Pre-Employment background investigations
- New Hire Security training
- Affiliation with professional security organizations such as ASIS, OSAC and local security/intelligence organizations

- Measuring success
- Alignment with best industry practice