RiskWatch

Physical Security Checklist

DOUG MARSH
THOMAS HEARD

RISKWATCH INTERNATIONAL | 1237 Gulfstream Avenue| Toll Free: 800-360-1898
Sarasota, FL 34236

SecureWatch

Table of Contents

How to Use

Step 1:

• Realize that doing assessments offline, manually via a checklist or spreadsheet is neither enjoyable nor effective.

• Visit WWW.RISKWATCH.COM today where you can complete an assessment for FREE with a trial of our SecureWatch application. You'll be able to use crime data, automate steps in the assessment, generate a polished report and easily compare this site to others within your organization with ease using our application.

Step 2:

•If you've read this far, you really should go back and read Step 1 more carefully. You wouldn't do this assessment using stone tablets and a chisel*…

•*If you are using a stone tablet and chisel to do assessments, no offense. We do not discriminate against risk assessing cavemen. Watch out for raptors around your access controls.

How to Calculate your Compliance Percentage and Risk Score

Step 1:

•Print this document

To save Ink, only print pages 6 through 40

Step 2:

•Walk your site. Complete the checklist. Respond to all questions.

Step 3:

•Count and Tally all answers. You need your totals for: Yes, No, N/A

Step 4:

•Subtract your total number of N/A responses from 122 (total number of questions) to get (X)

Step 5 (Compliance Percentage)

•Divide your total number of Yes responses by X to calculate overall compliance percentage

•Divide your total number of No responses by X to calculate overall non-compliance percentage

Step 6 (Risk Score)

• Consider the Likelihood Matrix on the next page. Determine your Likelihood Value.

•Consider the Consequence Matrix on the next page. Determine your Consequence Value.

•Divide your total number of No responses by 20 (Y)

•Add (Y) to your likelihood. (Z)

•Multiply (Z) by Consequence.

•You can use the resulting value as a comparative data point when assessing other sites with different likelihood and consequence.

Step 7 (Executive Summary – Optional)

•If you need to prepare a report for a superior or for later review, complete the Executive Summary portion of this worksheet.

Likelihood Matrix

Rating	Rating	Description:
1	Low	•Significantly below average crime rate. •No history of terrorists targeting the region or facility type. •Below average probability of natural disaster.
2	Medium Low	•Below average crime rate. •No history of terrorists targeting the region or facility type. • Average probability of natural disaster.
3	Medium	•Average crime rate. •Terrorists group(s) have indicated interest in targeting the region or facility type. •Average probability of natural disaster.
4	Medium High	•Above average crime rate. •Terrorist group(s) have repeatedly indicated interest in, or have targeted the region or facility type. •Above average probability of natural disaster.
5	High	•Significantly above average crime rate. •Terrorist group(s) have repeatedly indicated interest in, or have targeted the region or facility type. •Significantly above average probability of natural disaster.

Consequence Matrix

Rating	Rating	Description:
1	Low	•Replacement cost of less than $1 million. •Minimal critical system unavailability. •No impact to image/reputation.
2	Medium Low	•Replacement cost between $1 million and $10 million. •Critical systems unavailable for several hours. • Image/reputation impacted only locally.
3	Medium	•Replacement cost between $10 million and $20 million. •Critical systems unavailable 6 to 12 hours. •Significant customer disasitisfaction. Image/reputation impacted widely.
4	Medium High	•Replacement cost between $20 million and $50 million. •Critical systems unavailable 12 to 24 hours. •Major customer disasitisfaction. National coverage has major impact on image/reputation.
5	High	•Replacement cost exeeds $50 million. •Critical systems unavailable more than 24 hours •Disaster to image/reputation. Government intervention likely.

Executive Summary

Site Name:

(Name of your site)

Compliance Score:

(Complete Steps 3-5 Above)

Risk Score:

((Questions with "No" as the response + Likelihood) X Consequence)

Introduction:

(Discuss the purpose or objective for performing the assessment)

Background:

(What did you do to prepare for and perform the assessment?)

Narrative:

(Summarize the issues you found and what will be done to fix them)

Crime Prevention Through Environmental Design (CPTED)

1. Natural Barriers

Do you use signs or natural barriers to discourage or prevent access to restricted access points?

Natural access control: Employing physical and symbolic barriers to discourage or prevent access or direct movement to specific access points. Doors, fences, and other physical obstacles serve to prevent opportunities for criminal access. Symbolic barriers—such as signage—directs people to a particular route, and draws attention to those crossing the threshold.

Yes ☐ No ☐ N/A ☐

2. High Visibility

Is there a high level of visibility into all areas with no concealment areas for criminals to hide in?

Natural surveillance: Increasing visibility, both interior-to-exterior and exterior-to–interior, to increase witness potential, foster a sense of exposure to the criminal element, and give advance visibility to areas people are entering. This increases the feeling of safety to legitimate users of a space and increases the risk of detection to criminals. Neighborhoods with poor natural surveillance provide criminals with opportunities to observe, plan, and commit criminal activity.

Yes ☐ No ☐ N/A ☐

3. Defined Boundaries

Are the boundaries of the property identified through landscaping, barriers, or signs?

Natural territorial reinforcement/boundary definition: Establishing a sense of ownership by facility owners or building occupants to define territory to potential aggressors and to assist legitimate occupants or users to increase vigilance in identifying who belongs on the property and who does not. The theory holds that people will pay more attention to and defend a particular space or territory from trespass if they feel a form of "psychological ownership" in the area. Thus, it is possible—through real or symbolic markers—to encourage tenants or employees to defend property from incursion.

Yes ☐ No ☐ N/A ☐

4. Facility Maintenance

Is the facility and its surroundings well maintained and kept in good repair?

Management and maintenance: Maintaining spaces to look well-tended and crime-free. The "broken windows" theory (Wilson & Kelling, 1982) suggests that an abandoned building or car can remain unmolested indefinitely, but once the first window is broken, the building or car is quickly vandalized. Maintenance of a building and its physical elements (such as lighting, landscaping, paint, signage, fencing, and walkways) is critical for defining territoriality.

Yes ☐ No ☐ N/A ☐

5. Promote Intended Use of Space

Are spaces designed to engage legitimate visitors and promote the intended use of the space?

Legitimate activity support: Engaging legitimate occupants, residents, customers, or visitors in the desired or intended uses of the space. Criminal activity thrives in spaces that occupants and desired users do not claim and that offer no legitimate activities that can undermine or replace the criminal activities. CPTED suggests adding enticements to draw legitimate users to a space, where they may in effect crowd out undesirable illegitimate users of the space.

Yes ☐ No ☐ N/A ☐

6. Defense in Depth

Is security implemented in multiple layers that delay penetration into the areas that require the greatest protection?

Compartmentalization: One of the basic CPTED strategies is to design multiple or concentric layers of security measures so that highly protected assets are behind multiple barriers. These layers of security strategies or elements start from the outer perimeter and move inward to the area of the building with the greatest need for protection. Each layer is designed to delay an attacker as much as possible. This strategy is also known as protection-in-depth (Fay, 1993, p. 672). If properly planned, the delay should either discourage a penetration or assist in controlling it by providing time for an adequate response.

Yes ☐ No ☐ N/A ☐

7. Defined Access Points

Is access to the property limited to only defined access points?

Physical controls at the outer protective layer or perimeter may consist of fencing or other barriers, protective lighting, signs, and intrusion detection systems. It is the outermost point at which physical security measures are used to deter, detect, delay2, and respond (or defend) against illegitimate and unauthorized activities. Controls at this layer are generally designed to define the property line and channel people and vehicles through designated and defined access points. Intruders or casual trespassers will notice these property definitions and may decide not to proceed to avoid trespassing charges or being noticed.

Yes ☐ No ☐ N/A ☐

8. Access Lighting

Are all access points to buildings well lit?

The middle layer, at the exterior of buildings on the site, may consist of protective lighting, intrusion detection systems, locks, bars on doors and windows, signs, and barriers such as fencing and the façade of the building itself. Protection of skylights and ventilation ducts can discourage penetration from the roof.

Yes ☐ No ☐ N/A ☐

9. Intrusion Detection

Are sensors in place at all building access points to detect intrusion?

The middle layer, at the exterior of buildings on the site, may consist of protective lighting, intrusion detection systems, locks, bars on doors and windows, signs, and barriers such as fencing and the façade of the building itself. Protection of skylights and ventilation ducts can discourage penetration from the roof.

Yes ☐ No ☐ N/A ☐

10. Locks

Are locks in place at all building access points?

The middle layer, at the exterior of buildings on the site, may consist of protective lighting, intrusion detection systems, locks, bars on doors and windows, signs, and barriers such as fencing and the façade of the building itself. Protection of skylights and ventilation ducts can discourage penetration from the roof.

Yes ☐ No ☐ N/A ☐

11. Access Point Reinforcement

Are all building access points structurally reinforced to prevent penetration?

The middle layer, at the exterior of buildings on the site, may consist of protective lighting, intrusion detection systems, locks, bars on doors and windows, signs, and barriers such as fencing and the façade of the building itself. Protection of skylights and ventilation ducts can discourage penetration from the roof.

Yes ☐ No ☐ N/A ☐

12. Access Requirement Signs

Do interior areas with restricted access have signs defining the access requirements?

Usually, several inner layers are established. Their placement is designed to address an intruder who penetrates the outer and middle protective layers. The following physical controls are normal at this layer: window and door bars, locks, barriers, signs, intrusion detection systems, and protective lighting. The value of an asset being protected affects the amount of protection required. A high value asset housed in an inner area might require signs defining access requirements for the area, specially reinforced walls, a structurally reinforced door with a biometric lock, intrusion detection systems, video surveillance to monitor access, and safes and vaults to house the asset itself.

Yes ☐ No ☐ N/A ☐

13. Restricted Area Intrusion Detection

Are sensors in place at all access points to restricted areas to detect intrusion?

Usually, several inner layers are established. Their placement is designed to address an intruder who penetrates the outer and middle protective layers. The following physical controls are normal at this layer: window and door bars, locks, barriers, signs, intrusion detection systems, and protective lighting. The value of an asset being protected affects the amount of protection required. A high value asset housed in an inner area might require signs defining access requirements for the area, specially reinforced walls, a structurally reinforced door with a biometric lock, intrusion detection systems, video surveillance to monitor access, and safes and vaults to house the asset itself.

Yes ☐ No ☐ N/A ☐

14. Restricted Area Locks

Are locks in place at all access points into restricted areas?

Usually, several inner layers are established. Their placement is designed to address an intruder who penetrates the outer and middle protective layers. The following physical controls are normal at this layer: window and door bars, locks, barriers, signs, intrusion detection systems, and protective lighting. The value of an asset being protected affects the amount of protection required. A high value asset housed in an inner area might require signs defining access requirements for the area, specially reinforced walls, a structurally reinforced door with a biometric lock, intrusion detection systems, video surveillance to monitor access, and safes and vaults to house the asset itself.

Yes ☐ No ☐ N/A ☐

15. Restricted Area Structural Reinforcement

Are all access points into restricted areas structurally reinforced to prevent penetration?

Usually, several inner layers are established. Their placement is designed to address an intruder who penetrates the outer and middle protective layers. The following physical controls are normal at this layer: window and door bars, locks, barriers, signs, intrusion detection systems, and protective lighting. The value of an asset being protected affects the amount of protection required. A high value asset housed in an inner area might require signs defining access requirements for the area, specially reinforced walls, a structurally reinforced door with a biometric lock, intrusion detection systems, video surveillance to monitor access, and safes and vaults to house the asset itself.

Yes ☐ No ☐ N/A ☐

-Intentional Spacing – Continued Next Page-

Physical Barriers and Site Hardening

16. Site Perimeter Barrier

Is the site perimeter protected by a physical barrier to impede unauthorized access?

Barriers may be natural or structural (man-made). Natural barriers are intended to deter or impede entry, they include fields, creeks, rivers, lakes, mountains, cliffs, marshes, deserts, or other terrain difficult to traverse. Structural (man-made) barriers include berms, ditches, artificial ponds, canals, planted trees and shrubs, fences, walls, doors, roofs, and glazing materials. Natural and structural barriers physically and psychologically deter the undetermined, delay the determined, and channel authorized traffic through specified entrances.

Yes ☐ No ☐ N/A ☐

17. Perimeter Clear Zone

If the site perimeter is protected by a physical barrier, and if practical, is there a clear zone between the perimeter barrier and any interior structures?

Wherever possible and practical, a clear zone should separate a perimeter barrier from structures inside the protected area. The width of the clear zone will depend upon the threat that is being protected against. An exception can be made when a building wall constitutes part of the perimeter barrier.

Yes ☐ No ☐ N/A ☐

18. Limit Concealment

If the site perimeter is protected by a physical barrier, does the perimeter barrier limit concealment?

Barriers are commonly used to discourage unauthorized access that takes place by accident, by force, or by stealth. In general barriers should explicitly define territorial boundaries. Barriers should not provide concealment for surprise attacks, enable intruders to gain access to upper levels, or obstruct lighting, video surveillance, or intrusion detection systems. Barriers should also not facilitate observation of the facility or its occupants. However, barriers may be used to prevent views of the facility and the introduction of clandestine listening devices.

Yes ☐ No ☐ N/A ☐

19. Prevent Access to Upper Levels

If the site perimeter is protected by a physical barrier, does the perimeter barrier not enable access to upper levels of interior buildings?

Barriers are commonly used to discourage unauthorized access that takes place by accident, by force, or by stealth. In general barriers should explicitly define territorial boundaries. Barriers should not provide concealment for surprise attacks, enable intruders to gain access to upper levels, or obstruct lighting, video surveillance, or intrusion detection systems. Barriers should also not facilitate observation of the facility or its occupants. However, barriers may be used to prevent views of the facility and the introduction of clandestine listening devices.

Yes ☐ No ☐ N/A ☐

20. Allow Full Functionality of Security Controls

If the site perimeter is protected by a physical barrier, does the perimeter barrier allow full functionality of lighting, videos surveillance, and intrusion detection systems?

Barriers are commonly used to discourage unauthorized access that takes place by accident, by force, or by stealth. In general barriers should explicitly define territorial boundaries. Barriers should not provide concealment for surprise attacks, enable intruders to gain access to upper levels, or obstruct lighting, video surveillance, or intrusion detection systems. Barriers should also not facilitate observation of the facility or its occupants. However, barriers may be used to prevent views of the facility and the introduction of clandestine listening devices.

Yes ☐ No ☐ N/A ☐

21. Limit Observation

If the site perimeter is protected by a physical barrier, does the perimeter barrier not facilitate the ability to better observe the facility or its occupants?

Barriers are commonly used to discourage unauthorized access that takes place by accident, by force, or by stealth. In general barriers should explicitly define territorial boundaries. Barriers should not provide concealment for surprise attacks, enable intruders to gain access to upper levels, or obstruct lighting, video surveillance, or intrusion detection systems. Barriers should also not facilitate observation of the facility or its occupants. However, barriers may be used to prevent views of the facility and the introduction of clandestine listening devices.

Yes ☐ No ☐ N/A ☐

22. Breach Detection

If the site perimeter is protected by a physical barrier, are there mechanisms in place to detect a breach in the perimeter barrier?

Since barriers can be breached, they should be accompanied where practical and appropriate by a means of determining when a breach has occurred or is occurring.

Yes ☐ No ☐ N/A ☐

23. Direct into a Predictable Pattern

If the site perimeter is protected by a physical barrier, does the perimeter barrier direct pedestrians and vehicles into a predictable pattern?

Barriers are also used to direct pedestrian or vehicle traffic into predictable patterns. This presents opportunities to detect abnormal and potentially illegitimate activities. A threat basis design strategy should be used when selecting physical barriers, and the barriers designed to address the specific threats.

Yes ☐ No ☐ N/A ☐

24. Barrier Wall

If the site perimeter is protected by a physical barrier, is your perimeter barrier a wall?

Walls can be made of materials such as brick, stone, concrete block, or glass brick. Some walls, particularly concrete ones, are strengthened with steel bars. Walls should be sufficiently high to discourage people from climbing over them, and can be topped with materials to prevent scaling of the wall.

Yes ☐ No ☐ N/A ☐

25. Discourage Climbing

If the site perimeter is protected by a physical barrier, does your perimeter barrier discourage people from climbing over them by being sufficiently high or topped with a material that makes scaling the barrier difficult?

Walls can be made of materials such as brick, stone, concrete block, or glass brick. Some walls, particularly concrete ones, are strengthened with steel bars. Walls should be sufficiently high to discourage people from climbing over them, and can be topped with materials to prevent scaling of the wall.

Yes ☐ No ☐ N/A ☐

26. Chain Link Fence Construction

If the site perimeter is protected by a chain-link fence, is the fence constructed with a tight mesh fabric, sufficiently thick wire, heavy duty posts and rails that are deeply buried in the ground?

To be effective, chain-link fencing must avoid overly large mesh fabric, undersized wire, lightweight posts and rails, and shallow post holes.

Yes ☐ No ☐ N/A ☐

27. Fence Height Requirements

If the site perimeter is protected by a chain-link fence, does the fence height meet your security requirements? (refer to control standard)

Height. The higher the barrier, the more difficult and time-consuming it is to breach. For low security requirements, a 5-6 ft. (1.5-1.8 meter) fence may be sufficient; for medium security, a 7 ft. (2.1 meter) fence may be appropriate; and for high security (such as a prison), an 18-20 ft. (5.4-6.0 meter) fence may be required.

Yes ☐ No ☐ N/A ☐

28. Barbed Wire at Top

If the site perimeter is protected by a chain-link fence, is outward-facing barbed wire installed on the top of the fence at a 45-degree angle?

Barbed wire. Barbed wires vary in gauge, coating weight, number of barbs, and spacing of barbs. If chain link or expanded metal fences are intended to discourage human trespassing, barbed wire should be installed atop the fence on an outward facing top guard at a 45-degree angle.

Yes ☐ No ☐ N/A ☐

29. Bottom Rail

If the site perimeter is protected by a chain-link fence, does the fence have a bottom rail that is well anchored or is the fence fabric buried or incased in a mow strip at 1 foot or more?

Bottom rail. Properly anchored, this prevents an intruder from forcing the mesh up to crawl under it. Burying/Mow strip. Burying or installing a mow strip (concrete), in addition to a chain-link fabric 1 ft. (0.3 meters) or more, prevents an intruder from forcing the mesh up.

Yes ☐ No ☐ N/A ☐

30. Top Rail

If the site perimeter is protected by a chain-link fence, does the fence have a top rail or tension wire that the fabric attaches to at intervals of no more than 2 feet?

Top rail. A horizontal member of a fence top to which fabric is attached with ties or clips at intervals not exceeding two feet. A top rail generally improves the appearance of a fence, but it also offers a handhold to those attempting to climb over. A top tension wire should be provided if a top rail is not installed.

Yes ☐ No ☐ N/A ☐

31. Fence Fabric Visibility

If the site perimeter is protected by a chain-link fence, is the fence fabric coated with a color to promote visibility?

Color fabric. Color polymer-coated chain-link fabric enhances visibility, especially at night.

Yes ☐ No ☐ N/A ☐

32. Fence Height

If the site perimeter is protected by an entirely barbed wire fence, is the fence at least 7 ft. (2.1 meters) tall, not counting the top guard?

Fences constructed entirely of barbed wire should be at least 7 ft. (2.1 meters) tall, not counting the top guard.

Yes ☐ No ☐ N/A ☐

33. Post Spacing

If the site perimeter is protected by an entirely barbed wire fence, are the strands of the fence tightly stretched and attached firmly to posts spaced less than 6 ft. (1.8 meters) apart?

The strands of fences constructed entirely of barbed wire should be tightly stretched and attached firmly to posts spaced less than 6 ft. (1.8 meters) apart.

Yes ☐ No ☐ N/A ☐

34. Wood Construction

If the site perimeter is protected by a wood fence, are the vertical picket sections no wider than 1-3/4 inches and the horizontal sections 50 inches apart, located on the protected side of the building?

When utilizing a wooden fence to delay entry, the vertical picket sections must be no wider than 1-3/4 inches and the horizontal sections should be 50 inches apart, located on the protected side of the building.

Yes ☐ No ☐ N/A ☐

35. Number of Gates

If the site perimeter is protected by a physical barrier, are the number of pedestrian and vehicle gates kept to the absolute minimum for efficient operations and safety?

The vertical picket sections must be no wider than 1-3/4 inches and the horizontal sections should be 50 inches apart, located on the protected side of the building.

Yes ☐ No ☐ N/A ☐

36. Gate Locks

If the site perimeter is protected by a physical barrier, do all gates have locks?

All gates should be provided with locks.

Yes ☐ No ☐ N/A ☐

37. Door Material

Are exterior doors and interior doors that protect valuable assets made either of metal or wood covered with metal?

In high security settings, a door must offer the maximum delay time before penetration by extraordinary means – i.e., by the use of cutting tools, hand-carried tools, and some explosives (Gigliotti & Jason, 2004, p. 148). Solid wood or sturdy hollow metal doors can be covered with metal to strengthen them against a tool attack.

Yes ☐ No ☐ N/A ☐

38. Door Construction

Do exterior doors and interior doors that protect valuable assets and their frames have equal level of strength so that neither one creates a vulnerability?

Doors create several vulnerabilities. A door can be weaker or stronger than its frame and the surface into which it is set. Hinges can be defeated. Measures can be taken to strengthen the doors by adding steel plate for reinforcement, anchoring frames, adding kick plates, using set screws in hinges or spot welding hinges.

Yes ☐ No ☐ N/A ☐

39. Door Hinges

Are hinges in exterior doors and interior doors that protect valuable assets spot welded or use set screws?

Doors create several vulnerabilities. A door can be weaker or stronger than its frame and the surface into which it is set. Hinges can be defeated. Measures can be taken to strengthen the doors by adding steel plate for reinforcement, anchoring frames, adding kick plates, using set screws in hinges or spot welding hinges.

Yes ☐ No ☐ N/A ☐

40. Exterior Openings Fortification

Are all exterior openings that exceed 96 square inches fortified with steel bars or grills, wire mesh, expanded metal, fencing, and/or intrusion detection devices?

Other openings include shafts, vents, ducts, or fans; utility tunnels; channels for heat, gas, water, electric power, and telephone; and sewers and other drains. Where such openings exceed 96 square inches7, openings should be fortified with steel bars or grills, wire mesh, expanded metal, and fencing (and/or possibly protected with intrusion detection devices). Consideration should also be given to other objects that might be passed through an opening (contraband, weapons, etc.).

Yes ☐ No ☐ N/A ☐

41. HVAC Intake Protection

Are exterior HVAC intakes either high above the ground or protected by physical barriers?

Consideration should be given to protecting HVAC systems by preventing the introduction of harmful materials into exterior air intakes. Many buildings place air intakes high above ground or on the roof. Other premises use physical barriers to prevent unauthorized access to air intakes.

Yes ☐ No ☐ N/A ☐

42. HVAC Monitoring

Are HVAC air intakes and mechanical rooms monitored with intrusion detection devices, video surveillance, and/or security officers?

It may also be appropriate to use intrusion detection devices, video surveillance, and security officers to monitor access to air intakes and to HVAC and mechanical rooms.

Yes ☐ No ☐ N/A ☐

43. Redundant Power

Is there a redundant source of power in the form of extra power feeds, emergency generators, or uninterruptible power supplies?

Measures to manage power generation and distribution systems include the use of redundant power feeds, emergency generators, and uninterruptible power supplies.

Yes ☐ No ☐ N/A ☐

44. Command and Control Center Hardening

Are security command centers and control stations protected by hardened walls, and if there are windows, bullet-resistant windows?

Security command centers and control stations may warrant special protection, such as wall hardening, installation of bullet-resistant windows, protection of HVAC systems serving the center, and provision of emergency power and backup communications.

Yes ☐ No ☐ N/A ☐

45. Command and Control Center HVAC

Are HVAC systems that serve the security command centers and control stations well protected from damage and tampering?

Security command centers and control stations may warrant special protection, such as wall hardening, installation of bullet-resistant windows, protection of HVAC systems serving the center, and provision of emergency power and backup communications.

Yes ☐ No ☐ N/A ☐

46. Command and Control Center Backup Communications

Do security command centers and control stations have backup power and communications?

Security command centers and control stations may warrant special protection, such as wall hardening, installation of bullet-resistant windows, protection of HVAC systems serving the center, and provision of emergency power and backup communications.

Yes ☐ No ☐ N/A ☐

47. Critical System Identification

Are rooms and closets dedicated to critical systems (water, gas services, electrical power, and telecommunications.) identified with non-descriptive signage?

There is also the need to protect utilities such as water, gas services, electrical power, and telecommunications. Utilities protection should include identifying critical systems rooms and closets with non-descriptive signage, where possible.

Yes ☐ No ☐ N/A ☐

-Intentional Spacing – Continued Next Page-

Physical Entry and Access Control

48. Access Throughput

Is adequate throughput to the facility maintained when access controls are being used?

The most secure systems use several methods to authenticate and validate access. Using too many, however, could significantly decrease throughput and slow access through an access control portal.

Yes ☐ No ☐ N/A ☐

49. Electromagnetic Lock Safety

If you use electromagnetic locks, do they meet all safety codes?

Electromagnetic locks should be coordinated with safety codes, as there are specific and additional requirements with these doors that must be provided.

Yes ☐ No ☐ N/A ☐

50. Rapid Entry Monitoring

If you use a Rapid Entry System, is access to the rapid entry boxes monitored by an alarm system?

Rapid entry key boxes may be monitored by the facilities alarm system to detect unauthorized opening or tampering.

Yes ☐ No ☐ N/A ☐

51. Emergency Responder Access

If you use a Rapid Entry System, do emergency responders have keys to the boxes?

A key to the box should be supplied to emergency responders at the time of installation.

Yes ☐ No ☐ N/A ☐

52. Key Inventory

If you use mechanical key locks, do you use a key management system to inventory keys?

Key management systems help managers control and account for keys. Typically, managers conduct initial and periodic inventories of keys, maintain records of who has which keys, and maintain a secure key storage facility.

Yes ☐ No ☐ N/A ☐

53. Monitoring Mechanical Key Locks

If you use mechanical key locks, are they also complimented with monitoring measures?

Because locks can be compromised, they should be complemented with other measures, such as intrusion detection sensors, video surveillance, and periodic checks by security officers.

Yes ☐ No ☐ N/A ☐

54. Vehicle Identification

If you perform vehicle access control, are vehicles given an identification device to signify that have been granted access?

Vehicles can be identified by devices such as cardboard placards, stickers, radio frequency identification (RFID) tags, bar codes, special license plates, and electronic tags.

Yes ☐ No ☐ N/A ☐

55. Vehicle Searches

If you perform vehicle access control, are vehicles searched for contraband (prohibited items) before access is allowed?

Contraband consists of prohibited items—such as weapons, explosives, drugs, audio recording devices, cameras, or even tools. Where these items are a part of the threat definition, all personnel, materials, and vehicles should be examined for contraband before entry is allowed.

Yes ☐ No ☐ N/A ☐

56. Vehicle Search Station

If you perform vehicle searches, are searches conducted in a portal or monitoring station by trained security officers?

Vehicle searches should be conducted in a portal or monitoring station by trained security officers.

Yes ☐ No ☐ N/A ☐

57. Vehicle Detention Safety

If you perform vehicle searches, is there a way to safely detain a vehicle during a search?

The search location should include a way to detain the vehicle, such as using vehicle gates or barriers, until searches are completed.

Yes ☐ No ☐ N/A ☐

58. Access Badges

Are badges issued to individuals that have been granted access to the facility?

The following are some of the important access issues that should be addressed through procedures and controls: Wearing of badges.

Yes ☐ No ☐ N/A ☐

59. PIN Sharing

Is the sharing of personal identification numbers (pins) prohibited?

The following are some of the important access issues that should be addressed through procedures and controls: Sharing of personal identification numbers (pins).

Yes ☐ No ☐ N/A ☐

60. Access Card Sharing

Is the sharing of access cards prohibited?

The following are some of the important access issues that should be addressed through procedures and controls: Sharing of access cards.

Yes ☐ No ☐ N/A ☐

61. Unbadged Persons

Are personnel instructed to challenge all unbadged persons?

The following are some of the important access issues that should be addressed through procedures and controls: Challenging of unbadged persons.

Yes ☐ No ☐ N/A ☐

62. Failed Access Attempts

When using electronic access controls, is there a limit to the number of failed access attempts before there is an alarm or other elevated action is taken?

The following are some of the important access issues that should be addressed through procedures and controls: Number of access attempts allowed.

Yes ☐ No ☐ N/A ☐

63. Bag Search

Are visitor's packages, briefcases, and purses searched for contraband before access is granted?

The following are some of the important access issues that should be addressed through procedures and controls: Searching of packages, briefcases, and purses.

Yes ☐ No ☐ N/A ☐

64. Metal Detector Use

Are metal detectors used for the detection of contraband?

The following are some of the important access issues that should be addressed through procedures and controls: Calibration of metal detectors.

Yes ☐ No ☐ N/A ☐

65. Metal Detector Calibration

If metal detectors are used, are they calibrated on a regular basis?

The following are some of the important access issues that should be addressed through procedures and controls: Calibration of metal detectors.

Yes ☐ No ☐ N/A ☐

66. Explosive Detector Use

Are explosive detectors used to scan visitors and packages for explosives?

The following are some of the important access issues that should be addressed through procedures and controls: Use of explosives detectors.

Yes ☐ No ☐ N/A ☐

67. Prohibited Materials List

Does the organization have a documented list of prohibited materials that is communicated to personnel and visitors?

The following are some of the important access issues that should be addressed through procedures and controls: List of prohibited materials.

Yes ☐ No ☐ N/A ☐

68. Access Control Lists

Are access controls lists maintained that define levels of access for personnel and their access hours?

The following are some of the important access issues that should be addressed through procedures and controls: Access hours and levels of access.

Yes ☐ No ☐ N/A ☐

69. Credential Tampering Detection

Do you have controls for detecting credential tampering?

The following are some of the important access issues that should be addressed through procedures and controls: Credential tampering and replacement.

Yes ☐ No ☐ N/A ☐

70. Accommodation for the Disabled

Does your facility meet the accommodation requirements of the Americans with Disabilities Act?

The following are some of the important access issues that should be addressed through procedures and controls: Accommodation of disabled or physically impaired persons.

Yes ☐ No ☐ N/A ☐

71. Equipment Maintenance

Is all equipment subject to regular scheduled preventative maintenance?

The following are some of the important access issues that should be addressed through procedures and controls: Preventive maintenance of equipment

Yes ☐ No ☐ N/A ☐

Security Lighting

72. Continuous Illumination

In areas where security lighting is used, does it provide continuous illumination during all hours of darkness?

Where practical, security lighting during the hours of darkness should be continuous and equipped with an alternative power source. In addition, the system's wiring and controls should be protected against tampering or vandalism.

Yes ☐ No ☐ N/A ☐

73. Lighting Alternative Power

Does security lighting have an alternative power source?

Where practical, security lighting during the hours of darkness should be continuous and equipped with an alternative power source. In addition, the system's wiring and controls should be protected against tampering or vandalism.

Yes ☐ No ☐ N/A ☐

74. Lighting Tamper Protection

Is security lighting protected from tampering and vandalism?

Where practical, security lighting during the hours of darkness should be continuous and equipped with an alternative power source. In addition, the system's wiring and controls should be protected against tampering or vandalism.

Yes ☐ No ☐ N/A ☐

75. Lighting Maintenance

Is security lighting inspected and maintained regularly?

Lighting equipment must be inspected and maintained regularly. In that process, one should do the following: Check electrical circuits and test all connections; Ensure proper lamp functionality; Ensure that lamps are kept clean and maintain their proper lighting angle; Ensure that the lighting intensity continues to meet security requirements; and Ensure that batteries are charged for emergency lighting in compliance with regulations.

Yes ☐ No ☐ N/A ☐

76. Outdoor Light Mounting

Is outdoor security lighting mounted on high masts?

Regarding placement, in outdoor applications "high-mast lighting is recommended, because it gives a broader, more natural light distribution, requires fewer poles (less hazardous to the driver), and is more aesthetically pleasing than standard lighting" (FEMA, 2003), although it is subject to lightning strikes.

Yes ☐ No ☐ N/A ☐

-Intentional Spacing – Continued Next Page-

Intrusion Detection Systems

77. Intrusion Detection System Use

Is there an Intrusion Detection System (IDS) in place?

Intrusion Detection systems are integral factors in a security program's effort to: Deter. The presence of an IDS may deter intruders when signs are posted warning that a site is protected by such a system. Detect. Most IDSs are designed to detect an impending or actual security breach. Delay. When detection occurs, intruders may be delayed or denied by activating other measures. Respond. IDSs facilitate security responses by pinpointing where an intrusion has occurred and possibly where the intruder has moved within the site.

Yes ☐ No ☐ N/A ☐

78. IDS Effectiveness

If there is an IDS in place, does it meet all of the security needs of the facility?

When considering IDSs, the security manager should ensure that the system (Fay, 2008, p. 258) and its ongoing maintenance: Meets the security needs of the facility

Yes ☐ No ☐ N/A ☐

79. IDS Integration

If there is an IDS in place, does it work harmoniously with other systems and not interfere with business operations?

When considering IDSs, the security manager should ensure that the system (Fay, 2008, p. 258) and its ongoing maintenance: Operates in harmony with other systems; and Does not interfere with business operations.

Yes ☐ No ☐ N/A ☐

80. IDS Cost Benefit

If there is an IDS in place, has a cost benefit analysis been done on it to ensure that its total cost of operation does not exceed the benefits it provides?

When considering IDSs, the security manager should ensure that the system (Fay, 2008, p. 258) and its ongoing maintenance: Is cost-effective (i.e., that the value of benefits derived from the system is at least equal to the costs of the system).

Yes ☐ No ☐ N/A ☐

81. IDS Codes and Standards

If there is an IDS in place, does it meet all applicable codes and standards?

The IDS should be installed according to any applicable codes and standards.

Yes ☐ No ☐ N/A ☐

82. IDS Zone Identification

If there is an IDS in place, does it transmit their zone or individual alarm point to monitoring system or personnel when there is an alarm/alert?

Alarm signals can be transmitted to alarm monitoring systems and personnel. They may be transmitted via wire or wirelessly, and by zone or by an individual alarm point. Being able to identify a particular alarm point may reduce security officer's response time and make it easier to identify malfunctioning alarm points.

Yes ☐ No ☐ N/A ☐

83. Alarm Supervision

If there is an IDS in place, are alarm transmission, monitoring, and notification mediums/devices supervised?

Alarm transmissions, monitoring, and notification mediums/devices should be supervised to better detect occurrences of tampering or interception.

Yes ☐ No ☐ N/A ☐

84. IDS Testing

If there is an IDS in place, is it regularly tested with the results documented?

Regular tests should be performed to assure accuracy and timeliness of transmitted information. Auditing. This ongoing process tests and documents a security system's operations to ensure that all parts are functioning properly.

Yes ☐ No ☐ N/A ☐

85. IDS Monitoring

If there is an IDS in place, is it monitored either in-house or by a third party?

Alarm monitoring, performed either in-house (proprietary) or on a contract basis, can have the system owner notified by several methods, including telephone, e-mail, and pager. A list of all persons to be notified and their associated phone numbers (and alternate contact information) should be developed.

Yes ☐ No ☐ N/A ☐

86. IDS Notifications

If there is an IDS in place, does it notify the system owner of alarms/alerts?

Alarm monitoring, performed either in-house (proprietary) or on a contract basis, can have the system owner notified by several methods, including telephone, e-mail, and pager. A list of all persons to be notified and their associated phone numbers (and alternate contact information) should be developed.

Yes ☐ No ☐ N/A ☐

87. IDS Notification List

If there is an IDS in place, is a list of all personnel that are to be notified of IDS alerts developed and maintained?

Alarm monitoring, performed either in-house (proprietary) or on a contract basis, can have the system owner notified by several methods, including telephone, e-mail, and pager. A list of all persons to be notified and their associated phone numbers (and alternate contact information) should be developed.

Yes ☐ No ☐ N/A ☐

88. IDS Installation

If there is an IDS in place, was it engineered and installed by qualified technicians?

Engineering and installation. These are essential for a properly functioning alarm system. Even if all the devices, panels, and annunciators are of good quality, the system will fail without proper design engineering, if the selected components are not installed properly, or are not the correct components for the application.

Yes ☐ No ☐ N/A ☐

89. IDS Maintenance

If there is an IDS in place, is it regularly maintained?

Maintenance. Alarm systems require regular maintenance, which can be provided by facility staff (such as an in-house security systems specialist) or system vendors.

Yes ☐ No ☐ N/A ☐

-Intentional Spacing – Continued Next Page-

Video Surveillance

90. Video Surveillance Requirements

If you use a Video Surveillance System, have the functional requirements been determined and documented for the Video Surveillance System defining its target, activity to be monitored, and its purpose?

Once the system's purpose is determined (for example, by using the ASIS General Security Risk Assessment Guideline), a functional requirement for each component of the system should be written. A functional requirement is like a job description. A video surveillance system's functional requirement can be discerned by asking these questions: What is the purpose of the system? What specifically is each camera supposed to view? What are the requirements for real-time monitoring or recorded video?

Yes ☐ No ☐ N/A ☐

91. Video Surveillance Monitoring

If you use a Video Surveillance System, is technology employed to assist in video monitoring? (e.g. motion detection, access control system integration, intelligent video analytics)

If the purpose of the video surveillance system is to generate a response to specific incidents, then a trained person should monitor the system and respond accordingly. Even a trained person can only monitor a limited number of cameras simultaneously, and needs frequent breaks to maintain comprehension of the scene. Certain technology can help with the human factor.

Yes ☐ No ☐ N/A ☐

92. Video Surveillance Quality

If you use a Video Surveillance System, do recordings have adequate quality to distinguish key features and are stored on a device with enough storage capacity to ensure a high level of availability?

If a video recording is to be useful, it must clearly show the incident, target, or action it was meant to record, and, of course, the recording itself must be available.

Yes ☐ No ☐ N/A ☐

93. Video Surveillance Integration

If you use a Video Surveillance System, do all components of the system integrate effectively with each other?

When selecting video surveillance system equipment, it is important to use a systems approach as opposed to a components approach. A systems approach examines how equipment will work with other elements of the video surveillance system, with other workplace systems, and with the environment in which it is needed. This approach results in a video surveillance system that operates effectively and satisfies a facility's needs. By contrast, buying components separately and without an integration plan often results in a system that does not perform as expected, or to its fullest capacity.

Yes ☐ No ☐ N/A ☐

94. Video Surveillance Illumination

If you use a Video Surveillance System, is the system's illuminations needs met by the existing lighting?

Video surveillance system manufacturers specify the amount of illumination needed for minimum function and for maximum performance. Image quality is also affected by excessive shadows (light to dark ratio), lens glare, and backlighting.

Yes ☐ No ☐ N/A ☐

95. Video Surveillance Camera Protection

If you use a Video Surveillance System, are the cameras sufficiently protected from the environment?

Specialized enclosures are also available to protect cameras used outdoors in extreme weather or extreme environments.

Yes ☐ No ☐ N/A ☐

96. Video Surveillance Repair

If you use a Video Surveillance System, are there spare parts and trained service technicians available for quick repairs to the system?

When a video surveillance system (i.e., cameras, recording devices, monitors) is not operating as it should, the organization may be vulnerable, incident response may be delayed, and liability may be incurred. Camera maintenance must be considered before system implementation. Having adequate spare parts available and trained staff or a service agreement with a vendor or systems integrator is advisable.

Yes ☐ No ☐ N/A ☐

Security Personnel

97. Security Manager

Does the facility have a Security Manager that is part of senior management and understands issues such as the legal aspects of officer selection and screening, authority to detain or arrest, and use of force?

When security managers are employees of an organization, it is preferable that they be part of senior management. Such placement helps demonstrate that the organization considers security an important function by involving the security manager in the planning and the decision-making process. Security managers should understand issues such as the legal aspects of officer selection and screening, authority to detain or arrest, and use of force.

Yes ☐ No ☐ N/A ☐

98. Security Guard Age

If you use security officers/guards, are your guards at least 18 years for unarmed positions, and 21 years for armed positions?

The ASIS Private Security Officer (PSO) Selection and Training Guideline recommends that both proprietary and contract security guards meet the certain criteria and requirements.

Yes ☐ No ☐ N/A ☐

99. Security Guard Legality

If you use security officers/guards, are your guards of Legal working status?

The ASIS Private Security Officer (PSO) Selection and Training Guideline recommends that both proprietary and contract security guards meet the certain criteria and requirements.

Yes ☐ No ☐ N/A ☐

100. Security Guard Verified SSN

If you use security officers/guards, do your guards have a verified social security number (in the United States)?

The ASIS Private Security Officer (PSO) Selection and Training Guideline recommends that both proprietary and contract security guards meet the certain criteria and requirements.

Yes ☐ No ☐ N/A ☐

101. Security Guard Address and Phone

If you use security officers/guards, do you have the addresses and telephone numbers for the preceding seven years of each of your guards?

The ASIS Private Security Officer (PSO) Selection and Training Guideline recommends that both proprietary and contract security guards meet the certain criteria and requirements.

Yes ☐ No ☐ N/A ☐

102. Security Guard Education Level

If you use security officers/guards, do your guards have at least a high school diploma or equivalent?

The ASIS Private Security Officer (PSO) Selection and Training Guideline recommends that both proprietary and contract security guards meet the certain criteria and requirements.

Yes ☐ No ☐ N/A ☐

103. Security Guard Background Check

If you use security officers/guards, have you done a criminal history check for all of your guards?

The ASIS Private Security Officer (PSO) Selection and Training Guideline recommends that both proprietary and contract security guards meet the certain criteria and requirements.

Yes ☐ No ☐ N/A ☐

104. Security Guard Employment History

If you use security officers/guards, do you have a verified employment history for at least the preceding seven years for all of your guards?

The ASIS Private Security Officer (PSO) Selection and Training Guideline recommends that both proprietary and contract security guards meet the certain criteria and requirements.

Yes ☐ No ☐ N/A ☐

105. Security Guard License or Certification

If you use security officers/guards, and if appropriate, do your guards have a verified license or certification to work as a security officer?

The ASIS Private Security Officer (PSO) Selection and Training Guideline recommends that both proprietary and contract security guards meet the certain criteria and requirements.

Yes ☐ No ☐ N/A ☐

106. Security Guard Drug Screening

If you use security officers/guards, are your guards screened for drug use?

The ASIS Private Security Officer (PSO) Selection and Training Guideline recommends that both proprietary and contract security guards meet the certain criteria and requirements.

Yes ☐ No ☐ N/A ☐

107. Security Guard Training

If you use security officers/guards, are your guards thoroughly trained on all topics appropriate to their assignment?

Security officers should be trained and tested on topics appropriate to their assignment.

Yes ☐ No ☐ N/A ☐

108. Security Guard Weapons Training

If you use security officers/guards, do your security guards that are equipped with weapons receive extensive ongoing training?

If security officers are to be equipped with any weapons (such as firearms, batons, chemical sprays, or electrical weapons), they must be properly trained in their use. Officers who will be equipped with firearms need extensive, ongoing training.

Yes ☐ No ☐ N/A ☐

109. Security Guard Reviews and Testing

If you use security officers/guards, are your security guards given regular training reviews, as well as periodic proficiency testing?

Security officers should be given regular training reviews, as well as periodic proficiency testing.

Yes ☐ No ☐ N/A ☐

110. Security Guard Communication Device Testing

If you use security officers/guards, are the guards' communications devices regularly tested?

Communications devices: In the form of a two-way radio or mobile telephone device, the officer should be fully trained on their proper use. These items should be tested regularly in order to reduce the risk of device failure during a critical or emergency situation.

Yes ☐ No ☐ N/A ☐

111. Security Guard ID Badges

If you use security officers/guards, are your guards issued ID badges identifying them as security personnel?

ID Badge: Normally provides the officer with proper identification and access to areas which are either toured regularly or where an officer may need to enter during an emergency.

Yes ☐ No ☐ N/A ☐

112. Security Guard ID Maintenance and Storage

If you use security officers/guards, do you have documented policies and procedures that ensure proper maintenance and storage of ID badges?

ID Badges should be cared for, not defaced, and kept in a secure location when not in use. Badges may also contain electronic devices such as proximity or memory chips. These electronic devices can be damaged if not properly cared for.

Yes ☐ No ☐ N/A ☐

113. Key Management Policy

Do you have documented policies and procedures for key management?

Keys: A fundamental tool to most security officer positions. Keys should be appropriately stored, and proper training for use of the key box is essential. Keys may be of differing varieties, including mechanical and electronic types. Care should be taken to ensure that all keys are accounted for at the beginning and end of shift. Additionally, proper care should be taken so that damage to keys does not occur.

Yes ☐ No ☐ N/A ☐

114. Security Guard Vehicle Use

Do your security guards use vehicles?

Vehicles: Safe driving techniques, regular vehicle inspections, and adherence to all standard procedures is a must for all security officers. Regular training and driving observations should be a consideration by security management.

Yes ☐ No ☐ N/A ☐

115. Security Guard Driving Training

If you use security officers/guards that use vehicles, are your security guards trained in safe driving techniques?

Vehicles: Safe driving techniques, regular vehicle inspections, and adherence to all standard procedures is a must for all security officers. Regular training and driving observations should be a consideration by security management.

Yes ☐ No ☐ N/A ☐

116. Security Guard Vehicle Inspections

If you use security officers/guards that use vehicles, are security vehicles subjected to regular inspections?

Vehicles: Safe driving techniques, regular vehicle inspections, and adherence to all standard procedures is a must for all security officers. Regular training and driving observations should be a consideration by security management.

Yes ☐ No ☐ N/A ☐

117. Security Awareness Training

Are all personnel given security awareness training?

In a broad sense, every employee should be considered part of the security program. Through a security awareness program, employees should be taught to understand the relationship between security and the organization's success, learn their obligations under the security program, understand how various security measures support security program objectives, and become familiar with available resources to help with security concerns.

Yes ☐ No ☐ N/A ☐

-Intentional Spacing – Continued Next Page-

Security Policies and Procedures

118. Security Policies and Procedures Documentation

Do you have documented security policies and procedures?

Security policies establish strategic security objectives and priorities for the organization, identify the organization representatives primarily accountable for physical security, and set forth responsibilities and expectations for managers, employees, and others in the organization. A policy is a general statement of a principle according to which an organization performs business functions. Security procedures are detailed implementation instructions for staff to carry out security policies. Procedures are often presented as forms or as lists of steps to be taken.

Yes ☐ No ☐ N/A ☐

119. Security Policies and Procedures Communication

Are your security policies and procedures effectively communicated to all personnel?

Policies and procedures must be communicated effectively to staff members, who will then be expected to perform accordingly. Policies and procedures can also form the basis for corrective action in the event of inappropriate behavior or underperformance.

Yes ☐ No ☐ N/A ☐

120. Security Policies and Procedures and Business Objectives

Are security policies reviewed by executive officers to ensure that they are aligned with the overall business objective of the organization?

Policies are generally reviewed, approved, and issued at the executive level of an organization. Once established, they tend to remain in place for an extended period. Therefore, they should be aligned with the overall business objectives of the organization. Policy documents may affect decision making throughout the organization, even beyond the immediate subject of a policy. Moreover, the existence of a security policy tends to emphasize top management's commitment, thereby increasing the probability of employees' compliance with the policy.

Yes ☐ No ☐ N/A ☐

121. Security Policies and Procedures Application

Are the organization's security policies consistently applied?

An organization may increase its liability if it ignores the policy or applies it inconsistently. However, a concerted effort to address security issues on a policy level shows due-diligence and that management was aware of such issues and attempted to address them.

Yes ☐ No ☐ N/A ☐

122. Standard Operating Procedures

Does the organization have a set of standard operating procedures (post orders) that have, at the least: The date of its last revision; a confidentiality notice; emergency contact information; facility description; discussion/review of access control, keys and equipment control, property removal, escort of facility users, mobile patrols, arrest policy, and other policies and procedures; instructions for emergency situations; security staffing levels, hours of coverage, and specific functions and duties; operation of communications equipment; public relations; code of ethics; and standards of conduct.

Post Orders: Post orders, which are sometimes called standard operating procedures, state the essential elements of security officers' work assignments. They should contain at least the following minimum information: Date of revision. Notice of confidentiality. Emergency contact information (internal and external), including after-hours contact information. Description of the facility and its users (and floor plans if possible). Discussion and review of subjects such as access control, keys and equipment control, property removal, escort of facility users, mobile patrols, arrest policy, and other policies and procedures. Specific instructions on the handling of emergency situations. Security staffing levels, hours of coverage, and specific functions and duties. Proper operation of all emergency and non-emergency communication equipment. Instructions on public relations. Code of ethics and standards of conduct.

Yes ☐ No ☐ N/A ☐