



SECURE COMMUNITY NETWORK
FACILITY ASSESSMENT TOOL

23 December 2020
Version 01



Introduction

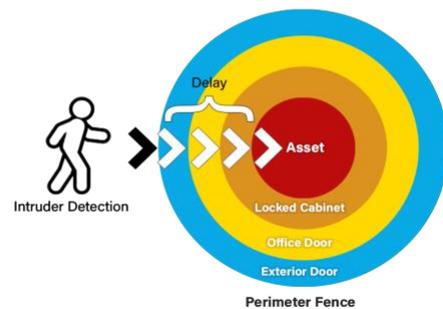
The Secure Community Network (SCN) has developed this Facility Assessment Tool, incorporating and adapting best practice guidance and examples, to aid non-profits and community organizations as well as related facilities in identifying areas of site security concerns. By answering a series of security related practice and equipment questions, users may quickly identify potential areas of concern. When a question is answered as a “No,” this may identify an area where enhanced attention may be warranted. Please note that not all questions will be relevant to all entities.

A common sense, pragmatic approach must be taken when using the SCN Facility Assessment Tool. This tool adopts a “defense-in-depth” approach, and which is indicated by the core principles of *Deter, Detect, Delay, Respond*.

A defense-in-depth posture helps to:

- Deter unwanted activity from a facility or area.
- Detect any unwanted or concerning activity at the earliest possible point.
- Delay any activity from reaching sensitive areas in order to enable a robust response.
- Respond to any unwanted activity quickly in order to prevent further escalation, damage or violence.

- Deterring intrusion is the first step in: “*Deter, Detect, Delay, Respond*”
- A well-designed system will detect a breach and allow enough time for proper response before a critical asset is reached by the intruder



What are we protecting against? What is the threat?

In order to understand and develop a physical protection system, it is necessary to define the potential threat to the facility.

Outsider:

An “outsider” is a person or persons who are not known to the community and who do not/should not have authorized access to the facilities or location. An outsider may have the intent to harass community members, engage in vandalism, theft, destruction of facilities, critical equipment or person-on-person violence.

Outsiders who pose a threat can be characterized by individuals who have specific religiously or racially based animus toward the facility or one of its members. Outsiders can also include vandals or criminal elements who may gain interest or access to the facility or its environs simply by proximity.

Insider:

An “insider” is a current or former community member, employee, contractor etc., who has authorized access to an organization, facility, or location.

Unacceptable Consequences:

An “unacceptable consequence” is considered a threshold that an organization considers to be severe enough that they can justify spending/obtaining resources to prevent. Unacceptable consequences can vary from organization to organization and have to be interpreted internally. For instance, some may consider minimal vandalism, such as graffiti and associated clean-up, an acceptable consequence versus spending resources in an attempt to deter and prevent it.



As areas of concern are identified, leadership may elect to make physical improvements, establish or adjust an internal policy, implement training or seek additional professional guidance to explore available options to address the concern(s).

Risk Scoring:

In some instances, there will only be a “yes” or “no” answer.

Yes	<ul style="list-style-type: none"> ▪ A “yes” score of 1 indicates that you have adequate and robust security for that question.
Some	<ul style="list-style-type: none"> ▪ A “some” score of 2 indicates that you have some, but not necessarily adequate security for that question. Or, for example, “<i>Are property boundaries of the facility easily recognizable by visual means?</i>” In this instance, only “some” of the boundaries may be recognizable. “Some” allows for subjectivity by the assessor.
No	<ul style="list-style-type: none"> ▪ An answer of “no” to a question means that you do not have any security measures in place related to that question.
N/A	<ul style="list-style-type: none"> ▪ “N/A” means that the question does not apply to your facility or location.

Upon completion of a category, a range is given for the total score within that category. For example, in category 1 – Facility External Environment, it is possible to have a low risk score of 1 - 2, a medium risk score of 3 – 4, and a high risk score of 5 – 6. In this category, a facility operator may be willing to accept any risk score of 4 and below, and choose to initiate action to reduce risk for any score of 5 or higher. Scores are aggregated and totaled for each category, as well as the entire facility enabling both category specific, and overall facility assessment.

This information has been prepared to help in establishing a base-level assessment of the relative safety and security status of a facility. Please note that this information is intended as guidance only; some of the information presented may not meet the specific requirements of a particular facility, nor is it intended to take the place of a comprehensive, formal and professionally undertaken risk assessment and gap analysis. Organizations interested in a receiving comprehensive security assessment should contact SCN, a local Federation Security Director or Regional Security Advisor, law enforcement, or a Protective Security Advisor with U.S. Department of Homeland Security.

Notice – Disclaimer:

This document is a compilation of existing security best practices, resources and guidance intended to assist organizations with general security planning guidance and basic security considerations. It is not intended to provide comprehensive, organization-specific advice on security matters nor is it meant to replace the design and development of a comprehensive security strategy.

SCN specifically disclaims any and all responsibility for, and is not responsible for, any loss or damage arising out of the use, nonuse or misuse of this information.

The Facility Assessment Tool was created based on the extensive experience and expertise as well as feedback of the Jewish security director network and SCN team, and incorporated as well as adapted numerous public and private security survey tools, consolidating core security information into a single document that can be used by an organization, facility or institution and without subject matter expertise.



1. Facility External Environment

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Is the immediate neighborhood free of "crime generators"? <i>"Crime generators" may include late-night social or retail establishments, open-air drug markets etc.</i>				
2. Are streets and walkways in the immediate vicinity of the facility well-lighted? <i>Adequate exterior lighting should allow at least 100 feet of visibility.</i>				
Totals:				
Risk Levels:	Low 1-2	Med 3-4	High 5-6	

2. Property Perimeter, Fences & Gates

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Are property boundaries of the facility easily recognizable by visual means?				
2. Is there a marquee or other sign visible from the adjacent roadway that identifies the presence of the facility?				
3. Can site entry points can be readily observed and monitored by staff and individuals in the facility in the course of their normal activities?				
4. Are there are at least two perimeter entry points to allow for emergency vehicle access?				
5. Can perimeter site entrances be secured?				
6. Can the perimeter of the site be secured to prevent unauthorized vehicles or pedestrians from entering?				
7. Can vehicle entry beyond checkpoints be controlled, permitting entry by only one vehicle at a time?				
8. Are there perimeter barriers capable of stopping vehicles?				
9. Does the site have perimeter fencing that is free of visual obstructions and clearly identifies the premises boundary?				
10. Are the fences 6 to 8 feet high and in good condition?				
11. Are gate locks/bars sufficient to prevent forced entry?				
12. Are any exterior playgrounds fenced with a restricted entry point?				
Totals:				
Risk Levels:	Low 1-12	Med 13-24	High 25-36	

3. Parking

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Are parking areas within view of the main office, other staffed areas, or surveillance cameras?				



2. Are parking areas 300 ft from occupied buildings?				
3. Is access to parking areas limited by curbs, barriers/fencing or gates, and a minimum number of entry points?				
4. Is handicapped/special parking access controlled and authenticated?				
Totals:				
Risk Levels:	Low 1-4	Med 5-8	High 9-12	

4. Landscaping, External Signage & Security

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Are bushes, shrubbery or other plant growth trimmed in an appropriate manner so as not to serve as a hiding place?				
2. Are sightlines from the facility to parking areas, pedestrian walkways, playing areas, etc. unobstructed by landscaping and plant growth?				
3. Is there clear, well-maintained signage that directs visitors to appropriate vehicle parking and building entry points?				
4. Are exterior or detached storage buildings secured?				
5. Have there been steps taken to prevent any exterior building recesses or alcoves from serving as hiding places for intruders?				
6. Are there appropriate warning signs, (e.g. No Trespassing, CCTV in Use, etc.), displayed around the perimeter of the premises?				
Totals:				
Risk Levels:	Low 1-6	Med 7-12	High 13-18	

5. External Lighting & Utilities

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Are designated parking lots or parking areas well-lighted?				
2. Are pedestrian walkways and building entrances well-lighted?				
3. Are all sides of the building illuminated by exterior lighting?				
4. Is motion detector-activated lighting located near doors and windows?				
5. Are exterior lights controlled by a photoelectric cell or timer?				
6. Are exterior lights checked weekly for functionality?				
7. Are exterior lighting fixtures obscured by man-made or vegetation obstacles?				
8. Are light switches, breakers or electrical panels accessible to the public?				



9. Are exterior lighting fixtures vandal resistant, beyond easy reach (at least 12 to 14 feet off the ground), maintainable, and built with break-resistant lenses or protected by cages or other means?				
10. Can exterior lighting controls be centrally accessed from the main administration area?				
11. Is access to site utilities, such as electrical transformers, generators, and phone lines, limited and secure from persons?				
12. Do site utilities create hiding places?				
13. Is exposed equipment protected against vandalism and damage?				
14. Are exterior mechanical equipment enclosures lockable?				
15. Is exterior mechanical equipment reachable by vehicles protected with bollards or other devices?				
16. Are fire hydrants on or around the site readily visible and accessible?				
17. Are locations where gas and electric utilities enter the building secured?				
18. Are dumpsters enclosed in a designated service area or surrounded on three sides by a high wall or fencing?				
19. Are dumpsters and their enclosure access strictly controlled?				
20. Are dumpster covers locked and dumpster area well-lighted?				
21. Are dumpsters set back 100 feet or more from occupied buildings?				
Totals:				
Risk Levels:	Low 1-21	Med 22-42	High 43-63	

6. Vehicle Access/Control

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Does emergency vehicle access around the building meet local requirements?				
2. Are roadways through the site serpentine or otherwise indirect?				
3. Are public routes over 300 feet from buildings?				
4. Do curb lanes adjacent to building prohibit parking?				
5. Are there clear, traffic-calmed pick-up/drop-off points?				
Totals:				
Risk Levels:	Low 1-5	Med 6-10	High 11-15	

7. Exterior Doors

Indicate the answer that best applies.



	Yes = 1	Some = 2	No = 3	N/A
1. Are exterior doors not used as designated entry points locked to prevent entry from the exterior?				
2. Are external doors equipped with propped open alarms?				
3. Are perimeter entryways equipped with full flush metal or solid core doors at least 1 3/4" thick and secured with deadbolt locking devices and door hinges that do not permit the pins to be removed from the exterior?				
4. Are the locks on all building entry points functional and in a good state of repair?				
5. Is there no more than 1/8" clearance between the exterior doors and their door frames?				
6. Are exterior doors equipped with high quality cylindrical locks with a deadbolt at least 1" in length?				
7. Are exit doors equipped with push-bars?				
8. Do you designate staff to check that all doors are closed and locked at the end of the business day?				
9. Are doors periodically checked for proper operation, ensuring that locks actually latch when the door is closed?				
10. Are the number of exterior doors minimized?				
11. Are exterior doors designed to prevent unauthorized access into the building?				
12. Do exterior doors have narrow windows, sidelights, fish-eye viewers or cameras to permit seeing who is on the exterior side?				
13. Are windows and sidelights sized and located so that if they are broken, persons cannot reach through and open a door from the inside?				
14. Are exterior doors designed and certified to resist thrown or wind-blown objects?				
Totals:				
Risk Levels:	Low 1-14	Med 15-28	High 29-42	

8. Windows

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Are all exterior windows easily locked?				
2. Are exterior windows checked for being locked at the end of each day?				
3. Is the glass in a door, or within 3 feet from the door lock, resistant to breaking?				
4. Do windows have security film, laminate, wire mesh, steel shutters, security drapes or other application that offers enhanced protection from debris and enhanced security?				
5. Are window hardware and frames in good condition or reinforced with slide bolts or other security devices?				



6. Are windows designed to serve as a secondary means of escape blocked by screens, security grills, louvers, awnings or other devices?				
7. Are second-floor windows inaccessible or protected against entry?				
8. Does tempered and wired glass meet the building code and Consumer Product Safety Commission's requirements when used in doors, sidelights, locations near the floor and other "hazardous" locations?				
9. In high risk areas, are windows and their framing and anchoring systems designed and located to resist the effects of explosive blasts, gunfire and forced entry?				
Totals:				
Risk Levels:	Low 1-9	Med 10-18	High 19-27	

9. Building Identification & Access

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Do visitors have to check in at an administrative office or desk before they can access other parts of the building?				
2. Does visitor access allow for stand-off/remote identification?				
3. Are entry points to the facility supervised?				
4. Do all staff wear facility issued identification credentials while on premises?				
5. Do visitors require appointments?				
6. Are visitors escorted at all times?				
7. Are visitors asked to provide proof of identification (govt. issued) and sign in/out?				
8. Are visitors provided with visitor's passes?				
9. Are passes designed to look different from staff identification?				
10. Are visitor passes collected from visitors when they sign out?				
11. Do passes have an expiration date on them?				
12. Are visitors prevented from accessing unauthorized areas such as utility rooms and sensitive areas?				
13. Does staff challenge or offer to assist people not wearing a visitor's pass or identification credential?				
14. Are all incoming deliveries inspected before being delivered to the designated recipient?				
15. Are mail/package handling procedures posted in a conspicuous location?				
16. Are separate wings' buildings, doors and windows externally marked for emergency responders?				



17. Have external markings been coordinated with local first responders?				
18. Is access into the building(s) 100 percent controllable through designated, supervised or locked entry points, including windows and service entries?				
19. Is entry granted by supervising staff, greeters, ushers or through the use of proximity cards, keys, coded entries or other devices?				
20. Are portions of the facility that are not being used readily secured?				
21. Are there exit signs, in all relevant languages and with simple maps or diagrams where needed, to direct visitors to designated building exits?				
22. Are panic or duress alarm buttons installed at the reception desk?				
23. Are panic alarms linked to the entire facility and EMS and routinely tested?				
24. Can doors be electronically locked to block visitors' entry into the building?				
25. If main entry doors are unlocked, can internal doors force visitors to confer with the receptionist to gain entry?				
26. Is the reception area protected by bullet-resistant windows, hardened counters or other measures?				
27. Are entries designed to mitigate explosive blast hazards? Do doors and walls along the line of security screening meet requirements of UL 752, Standard for Safety: Bullet-Resisting Equipment?				
28. Have steps been taken to restrict easy access to the roof, such as ladders and other items that could be used to access the upper floors and/or rooftop of the facility secured?				
29. Are mechanical equipment enclosures on the roof protected from unauthorized access or vandalism?				
30. Is roof access from inside the building only and locked?				
31. Is access into the facility through skylights blocked by security grilles or other devices?				
Totals:				
Risk Levels:	Low 1-31	Med 32-62	High 63-93	

10. Electronic Intrusion Detection System

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Does the facility have an electronic intrusion detection system ("burglar alarm")?				
2. Does the alarm system cover all exterior entry points?				
3. Is the intrusion detection system armed (activated) every night?				



4. Are there clear signs and/or decals posted on the exterior of the building (doors and windows) indicating the facility is equipped with an intrusion detection system?				
5. Is the intrusion detection system monitored?				
6. Are appropriate organizational members and staff formally trained on alarm system arming and disarming procedures?				
7. Is there a testing & maintenance program for the intrusion detection alarm system?				
8. Is there a procedure for the periodic replacement or upgrading of the intrusion detection system?				
9. Are the arm/disarm codes for an intrusion detection system changed and reissued at least annually?				
10. Are the names and call numbers of persons on the central station call list reviewed and updated at least annually?				
11. Are there panic buttons with audible alarms?				
Totals:				
Risk Levels:	Low 1-11	Med 12-22	High 23-33	

11. Electronic Access Control System

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Are primary exterior doors controlled by a functioning electronic access control system (magnetic swipe card or proximity device)?				
2. Are there interior areas or doors controlled by an electronic access control system?				
3. Is there a preventive maintenance program for the electronic access control system?				
4. Is the database of cardholders for the electronic access control system periodically audited to deactivate users who no longer need access to the facility?				
5. Are all mechanical and electronic locks in proper working order?				
Totals:				
Risk Levels:	Low 1-5	Med 6-10	High 11-15	

12. Video Surveillance System

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Do you have CCTV equipment installed? (CCTV = closed circuit tv)				
2. Are the cameras actively monitored?				
3. Do the CCTV cameras cover the entrances and exits to your building?				



4. Is there video surveillance of areas adjacent to the facility?				
5. Do you have CCTV cameras covering critical areas in your business, such as server rooms or cash offices?				
6. Are CCTV images recorded offsite via web base, retained for future use as needed and stored in a secure area? For how long?				
7. Are all of the cameras and recording devices in proper working order?				
8. If the facility has a video surveillance system, is a preventive maintenance program in place?				
Totals:				
Risk Levels:	Low 1-8	Med 9-16	High 17-24	

13. Internal Building Areas

Indicate the answer that best applies.	Yes = 1	Some = 2	No = 3	N/A
	1. Are all interior hallways and rooms well-lighted?			
2. Are there lockable doors or other means to secure sections of the facility when the section is not in use?				
3. Are areas under stairwells enclosed or otherwise inaccessible?				
4. Are building restrooms located to maximize visual surveillance, such as near classrooms or staffed areas?				
5. Are interior lights within restrooms controlled by means other than by wall switches?				
6. Is the lockable door hardware of interior doors routinely tested to ensure doors close and lock properly and that the door hardware is in a good state of repair?				
7. Are there locks on mechanical room doors?				
8. Is there a reinforced and alarmed storage room or closet for the secure storage of portable equipment of significant value?				
9. Are corridor sight lines maximized for natural surveillance and safety?				
10. Are corridor lighting controls protected from unauthorized use?				
11. Are recesses, niches or blind corners visually exposed with windows, convex mirrors, chamfered (angled) corners or surveillance cameras?				
12. Are lockers, vending machines, trash containers, display cases, cabinets and water coolers mounted flush with walls to avoid injury and allow natural surveillance?				
13. Do hidden corridors and stairwells receive visual surveillance through the use of video surveillance equipment?				



14. Are decorative materials, streamers and fabrics flame resistant?				
15. Are corridors wide enough to prevent crowding and provide adequate room for maneuvering wheelchairs/gurneys?				
16. Are exit signs well-maintained, easily seen and pointing in the right direction?				
17. Are clear and precise emergency evacuation maps posted at critical locations? Do they match their positions in the building and protected from vandalism or removal?				
Totals:				
Risk Levels:	Low 1-17	Med 18-34	High 35-51	

14. Interior Doors & Lockers

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Is the lockable door hardware of interior doors routinely tested to ensure doors close and lock properly and that the door hardware is in a good state of repair?				
2. Does door hardware allow staff to quickly lock rooms from the inside without having to step into the hallway?				
3. Do door access devices such as master keys or proximity cards allow staff to gain quick entry to any room where individuals have secured themselves?				
4. Does door hardware permit criminals or vandals to lock or chain corridor doors as a way of significantly slowing down security officers in pursuit?				
5. Can classroom doors always be opened from the inside for emergency exit purposes?				
6. Do recessed doors project more than 7 inches into the corridor?				
7. Are doors sized and arranged to reduce congestion and avoid crowding?				
8. Are lockers locked with facility-owned padlocks or electronic pass cards?				
9. Are lockers checked regularly and/or required to be opened and left empty nightly?				
Totals:				
Risk Levels:	Low 1-9	Med 10-18	High 19-27	

15. Courtyards

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Are entries into courtyards from the exterior of the facility controlled and lockable?				
2. Are courtyard entries next to administration or staff spaces, with windows permitting visual surveillance?				



3. Are courtyards configured to eliminate unauthorized after-hours access?				
4. Do windows in occupied areas of the building overlook courtyards?				
5. Are outer courtyard walls climbable, and are outside seating, planters and landscaping features far enough from courtyard enclosures to eliminate climbing opportunities?				
Totals:				
Risk Levels:	Low 1-5	Med 6-10	High 11-15	

16. Exit Ways

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Is every passageway from corridors and stairs to the street clear of obstructions or impediments?				
2. Are exit doors free of locks, chains or fastenings that would prevent escape from inside the building?				
3. Do exit doors open in the direction of egress?				
4. Are all exits and the routes to them clearly visible, conspicuously indicated and reliably illuminated and with signs in appropriate languages?				
5. Is "EXIT" lettering at least 6 inches high with principal strokes not less than 3/4-inch wide?				
6. Decorations and other materials do not obstruct the view of, or access to, emergency exits?				
Totals:				
Risk Levels:	Low 1-6	Med 7-12	High 13-18	

17. Key Management & Control Valuables

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Is there a single person responsible for key issuance and record keeping?				
2. Is there an alternate person also responsible for key issuance and record keeping?				
3. Is there an accurate record of who has been issued keys to the facility?				
4. Is key duplication prohibited, except for authorized personnel?				
5. Are keys stored in a locked cabinet with limited, auditable access?				
6. Are affected locks replaced or rekeyed whenever a key is lost or stolen?				
7. Are keys, identification credentials and uniforms collected upon employee separation?				



8. Does staff have a location to secure their personal items?			
9. Does this location have restricted access?			
10. Are lost keys investigated?			
Totals:			
Risk Levels:	Low 1-10	Med 11-20	High 21-30

18. Property Inventory

Indicate the answer that best applies.	Yes = 1	Some = 2	No = 3	N/A
1. Is the responsibility for property inventory assigned to a specific staff member?				
2. Is there an alternate with responsibility for property inventory?				
3. Is valuable property engraved with an owner-applied number in a manner that permits easy identification?				
4. Is there a written (preferably computerized) inventory of all property and equipment of value?				
5. Are there written policies for personal use of equipment or property?				
6. Are assets, equipment and items of value inventoried annually?				
Totals:				
Risk Levels:	Low 1-6	Med 7-12	High 13-18	

19. Children & Youth Security

Indicate the answer that best applies.	Yes = 1	Some = 2	No = 3	N/A
1. Is there a written, up-to-date child and student safety and protection policy?				
2. Is there a child and youth security training program for employees and volunteers?				
3. Is there a policy that requires a background check of staff and volunteers?				
4. Are fingerprints taken of all facility employees who work with children?				
5. Is there a policy that requires volunteers to be a member of the facility or active in facility activities for at least six months before they can be directly involved in children and youth activities?				
6. Are doors to classrooms and youth activity areas equipped with windows that provide unobstructed visibility into the areas?				
7. Is there a policy that requires that two or more adults be present during facility-sponsored programs involving children and youth?				



8. Is there a policy that requires an adult to announce to another adult when assisting a child in a bathroom or changing a diaper?				
9. Is there a child-tag system or other child check-in and drop-off procedure?				
Totals:				
Risk Levels:	Low 1-9	Med 10-18	High 19-27	

20. Financial Security

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Is there a written, up-to-date accounting procedure manual that identifies how money and financial resources are handled, counted, deposited, reported and audited?				
2. Is there a policy that no one person has the authority to approve purchases, issue funds and sign checks?				
3. Are bank statements reconciled by someone who does not have the authority to issue or sign checks?				
4. Is there a policy that requires all checks issued by the facility to have at least two signatures?				
5. Does a certified public accountant or other qualified outsider conduct an annual financial audit?				
6. Does the facility have a UL Listed money safe on-site for the storage of cash funds?				
7. Does the facility have a policy for value of money that can be stored before triggering a mandatory deposit?				
Totals:				
Risk Levels:	Low 1-7	Med 8-14	High 15-21	

21. Information Security

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Do you have a clear-desk policy for sensitive documents during non-working hours?				
2. Do you have a policy requiring employees to log off, shut down and secure all computers at the end of the business day?				
3. Are all your computers password-protected?				
4. Are computer passwords changed regularly?				
5. Is there a clear internet use policy?				
6. Are computer screens shielded from public view? Do auto screen savers initiate after a short period of activity?				
Totals:				
Risk Levels:	Low 1-6	Med 7-12	High 13-18	



22. Security Communication

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Do you have a written security policy?				
2. Is the policy regularly reviewed and, if necessary, updated?				
3. Do you regularly meet with staff and discuss security issues?				
4. Do you encourage staff to raise their concerns about security?				
5. Do you interact with law enforcement and neighboring businesses/facilities on issues of security and crime trends that might affect all?				
6. Do you and your staff know the various methods of contacting authorities like 911, 311, applications for your smart phone, etc.?				
7. Does the organization's website prohibit detailed information on the location of the management team/schedules/children's activities, names and locations?				
8. Is there an active shooter response program?				
Totals:				
Risk Levels:	Low 1-8	Med 9-16	High 17-24	

23. All-Hazards Preparedness

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. Facility is not located in a flood plain or area prone to flooding.				
2. In areas prone to earthquakes or high winds, are other routes into and out of the site available to avoid potential fallen trees, buildings, utility lines or other hazards?				
3. In areas prone to earthquakes, does the facility meet all applicable building code requirements for earthquakes?				
4. In areas prone to earthquakes, high winds, flooding or other natural or man-made hazards, have nearby facilities been identified as safe areas of refuge or community gathering places?				
Totals:				
Risk Levels:	Low 1-4	Med 5-8	High 9-12	

24. High-Risk Issues

Indicate the answer that best applies.				
	Yes = 1	Some = 2	No = 3	N/A
1. In areas of high fire risk, are fire evacuation sites at least 300 feet from at-risk buildings?				



2. Are bomb threat evacuation sites limited to administrators, staff and law enforcement?				
3. Are outdoor containers in which explosives can be hidden (such as garbage cans, mailboxes, and recycling or newspaper bins) kept at least 300 feet from the building and designed to restrict the size of objects placed inside them?				
4. In areas considered susceptible to explosive attack, is the stand-off distance between buildings and the nearest parking or roadway at least 500 ft?				
Totals:				
Risk Levels:	Low 1-4	Med 5-8	High 9-12	

25. Training & Emergencies

Indicate the answer that best applies.	Yes = 1	Some = 2	No = 3	N/A
1. Are your telephones pre-programmed with emergency contact numbers?				
2. Are your telephone lines protected from being compromised?				
Are staff trained and have they practiced their response to handle emergencies?				
3. Nuisance phone calls				
4. Active shooter threat				
5. Evacuation				
6. Severe weather				
7. Suspicious bags/packages/bomb threat				
8. Fire				
9. Workplace violence				
10. Vehicle-Borne Improvised Explosive Device (VBIED)				
11. Are staff trained to report maintenance problems and Occupational Health and Safety concerns?				
12. Have local first responders toured the facility to gain a greater understanding of the physical layout?				
13. Are local first responders aware of the increase in population and/or potential threats during special events?				
Totals:				
Risk Levels:	Low 1-13	Med 14-26	High 27-39	

Total

Facility Risk Rating Ranges:	Low 1-232	Med 233-464	High 465-696	
Cumulative Facility Risk Rating:				



Additional Resources

Secure Community Network

<https://www.securecommunitynetwork.org/>

- [Low-Cost/No-Cost Safety & Security Measures for Individuals & Families \(PDF\)](#)
- [Leadership Safety Guide \(PDF\)](#)
- [Back to Business-A Jewish Community Guide for Reopening Facilities & Resuming Operations in the Age of COVID-19 \(PDF\)](#)
- [Safety & Security Considerations for Facility Closures \(PDF\)](#)
- [Considerations for Reopening and Resumption of Operations \(PDF\)](#)

Active Shooter Information:

<http://www.dhs.gov/active-shooter-preparedness>

Developing Emergency Plans:

<https://www.fema.gov/media-library/assets/documents/33007>

Emergency Preparation:

<http://www.ready.gov/>

Federal Emergency Management Agency:

<http://www.fema.gov/>

NJ Office of Emergency Management:

<http://www.state.nj.us/njoem/>

New Jersey Office of Homeland Security and Preparedness

<http://www.njhomelandsecurity.gov/resources>

FEMA IS-906 Workplace Security Awareness Training (free training):

<http://www.training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-906>

FEMA IS-921.A Implementing Critical Infrastructure Security and Resilience:

<http://www.training.fema.gov/is/courseoverview.aspx?code=IS-921.a>

Source Information

- American Red Cross, Ready Rating, Multi-Building Physical Security Checklist, United States of America
- Cambridgeshire Constabulary, Home Security Self-Assessment, United Kingdom
- Hertfordshire Constabulary, Business Premises Self-Assessment Checklist, United Kingdom
- Howell Police Department, Business Security Survey, New Jersey
- Jefferson City Police Department, Commercial or Business Security Survey, Missouri
- Lakewood Police Department, Business Security Survey, New Jersey
- National Crime Prevention Council, Business Watch Brochures, United States of America
- Newark Police Department, Business Security Survey, New Jersey
- Orange Police Department, Business Security Survey, New Jersey
- San Diego Police Department, Small Retail Business Security Reference Material and Survey Form, California
- Westerville Police Department, Security Survey Checklist: Business, Ohio
- Windsor Police Department, Home or Business Property Self Audit, New Jersey
- American Crime Prevention Institute, House of Worship Safety and Security Assessment, United States of America
- New Jersey Office of Homeland Security and Preparedness, Facility Self-Assistance: Building Identification and Access, New Jersey