2024

Non-Profit Security Grant Program

Threat, Vulnerability & Risk Assessment Tool

FOR OFFICIAL USE ONLY

(FOUO)

- SECURITY SENSITIVE INFORMATION -

FOUO information shall not be disseminated in any manner – orally, visually, or electronically – to unauthorized personnel. The holder of the information will comply with access and dissemination restrictions. Ensure the recipient of FOUO information has valid "need-to-know" and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

The following report is the result of a Threat, Vulnerability, and Risk Assessment (TVRA) for the

_____.

This report is specifically designed to assist organizations in their application for the United States Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA) administered Non-Profit Security Grant Program (NSGP).

This document consists of an assessment conducted by _____, a subsequent interview/ consultation conducted by _____, and representing _____.

Recommendations provided through this process are intended to inform efforts to increase the facility's prevention, protection, preparedness, mitigation, response, and recovery capabilities, with the overall goal of reducing the facility's vulnerability to terrorism, crime, and other all-hazard risks. The ability to deter, detect, delay, and respond to an incident is critical in establishing an effective safety and security program consistent with incident management protocols designed to prevent, protect against, mitigate, respond to, and recover from a significant incident or event. The survey process provides a snapshot of the conditions at the time of the assessment based on organizational input and is designed specifically to support the organization's efforts related to the NSGP. Safety and security efforts must be viewed as dynamic processes and accordingly, it is recommended that the organization work to implement a comprehensive strategic security framework as a component of a cohesive, professionally coordinated community-wide safety and security strategy. Regardless of results, it is recommended that organizations continually monitor their security environments and adjust security practices, policies, and procedures consistent with changes in the environment.

ABOUT SCN

The Secure Community Network (SCN), a nonprofit 501(c)(3), is the official safety and security organization of the Jewish community in North America. Founded in 2004 under the auspices of The Jewish Federations of North America and the Conference of Presidents of Major American Jewish Organizations, SCN works on behalf of 146 Federations, the 50 largest Jewish non-profit organizations in North America, and over 300 independent communities as well as with other partners in the public, private, nonprofit and academic sectors to ensure the safety, security, and resiliency of the Jewish people.

SCN serves as the Jewish community's formal liaison with federal law enforcement and coordinates closely with federal, state, and local law enforcement partners on safety and security issues related to the Jewish community; through the organization's Operations Center and Duty Desk, SCN analyzes intelligence and information, providing timely, credible threat and incident information to both law enforcement and community partners. SCN's team of law enforcement, homeland security, and military professionals proactively works with communities and partners across North America to develop and implement strategic frameworks that enhance the safety and security of the Jewish people. This includes developing best practice policies; emergency plans and procedures; undertaking threat and vulnerability assessments of facilities; providing critical, real-world training and exercises to prepare for threats and hazards; offering consultation on safety and security matters; and providing response as well as crisis management support during critical incidents.

SCN is dedicated to ensuring that Jewish organizations, communities, and life and culture can not only exist safely and securely but flourish.

TABLE OF CONTENTS

Introduction	6
Using the TVRA Tool	7
Threats To Jewish Facilities/Institutions	10
How To Read This Document	14
Site Characteristics & General Information	15
Assessment Findings:	
Surrounding Area, Perimeter, & Property Grounds	16
Lighting	19
Vehicle Access Control & Parking	22
Building Facade, Exterior Doors, & Windows	25
Access Control & Visitor Management	29
Video Surveillance Systems	32
Building Interior	35
Intrusion Detection Systems	38
Training & Exercises	41
Policies & Procedures	44

We encourage you to contact the assessor with any questions related to the contents of this report.

Should you have additional questions or concerns as you look to address the findings of this process and/or implement security improvements, please contact us.

NSGPsupport@SecureCommunityNetwork.org
844.SCN.DESK (844.726.3375)

DISCLAIMER

The following information is the result of a Threat Vulnerability Risk Assessment ("TVRA"). Due to circumstances that did not allow for an on-site review by Secure Community Network ("SCN") personnel, this TVRA was conducted via a virtual process for interacting with the facility concerned. To the extent possible, this TVRA was conducted within the confines of both security best practices and the U.S. Department of Homeland Security's recommended protective measures.

This TVRA attempts to determine the vulnerabilities that threat actors could exploit as reported by the organization in the TVRA tool, and to the extent possible given current operating conditions. The vulnerabilities identified and the ultimate mitigation recommendations made are in response to the organization's reporting while following the TVRA tool's guidance. The mitigation recommendations which are included in the assessment are provided to coincide with increases in the organization's current security posture, fill in gaps where security is lacking, and/or improve or upgrade existing security measures to reduce the organization's vulnerability to crime, attack, and other risks. It is important to note that the recommendations given cannot guarantee that the facility will not become a victim of crimes, attacks, or other risks. This TVRA process merely provides a snapshot of the identified current security conditions reported by the organization upon their completion of the TVRA and is designed specifically to support the organization's efforts related to the NSGP. The mitigation recommendations are in response to the reported TVRA and are not necessarily the result of a TVRA performed by an SCN or other security professional. Safety and security preparedness, prevention, and protection efforts must be viewed as dynamic processes. Accordingly, we strongly recommend that the organization continually monitor its environment and adjust security practices, policies, and procedures consistent with changes in the environment – to include a comprehensive on-site TVRA conducted by SCN when circumstances permit. SCN does not assume any responsibility for the failure to detect, identify, or make known any additional hazards or threats that are or may come to be known beyond what has been self-identified in this TVRA, nor responsibility for the data or information input into the document.

This tool was developed based on general physical security best practices and to conform with the broad requirements of the NSGP, as articulated by DHS/FEMA in past Notice of Funding Opportunity announcements. Organizations should review the latest guidance issued by DHS/FEMA as well as their individual State Administrative Agencies (SAAs), to ensure compliance with all requirements. Organizations should pay particular attention to requirements related to assessments and the suitability and acceptance of this process by individual SAAs. SCN makes no warranties, express or implied, in connection with this tool or the performance of the same and accepts no responsibility for the use of this tool or its effectiveness, nor shall SCN be held responsible or liable for any costs, damages, or performance, or lack thereof, related to the use of this tool or any information provided therefrom.

Through an assessment process, a security professional or SCN may offer or recommend certain equipment for consideration to address the findings of this assessment. SCN is not affiliated with any manufacturers of equipment or hardware, nor does SCN receive any compensation from any

manufacturer; SCN and its personnel will make equipment recommendations based solely on technical specifications and/or verified performance, if at all. SCN assumes no responsibility or liability for the use and operation of any equipment or products recommended through this tool, and whether made by members of SCN or other security professionals. This assessment and accompanying process are intended to be useful as an organization takes steps to improve the security of a facility and those who use it.

This template was created by SCN as a guide and has been made available as a general resource; SCN cannot control the use of this document by others, including but not limited to non-security professionals. As a reminder, as stated throughout this document, the purpose of this assessment is to assist in the application of the NSGP, but it – alone – may not be sufficient to meet eligibility requirements related to assessments, as articulated by an SAA. Organizations must review the latest federal and state guidance to ensure they are meeting all applicable eligibility requirements.

INTRODUCTION

SCN has supported the development of this TVRA tool for Jewish and faith-based community partners. The assessment is designed using commonly recognized best practice methods and specifically to support an organization's efforts related to the NSGP, and with the purpose of the TVRA to: (1) understand the current threat environment, identify vulnerabilities, mitigate those vulnerabilities and prepare for emergencies; (2) guide the response to and recovery from emergency incident; and (3) enhance continuity of operations under high threat conditions.
This TVRA tool incorporates and adapts 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 *"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 practical and pragmatic approach must be taken when using the TVRA template, as the tool adopts a "defense-in-depth" approach, which is indicated by the core principles of *Deter, Detect, Delay, and Respond.*

The scope and overall objective of the TVRA is to provide a general evaluation of facility preparedness and security posture. The TVRA tool is designed to assist the organization in understanding their current threat environment and vulnerabilities within the confines of the NSGP administered by DHS and FEMA, and to seek remedies for the identified vulnerabilities via FEMA's Approved Equipment List (AEL) for the NSGP and can be used either in a self-guided fashion or by a security professional.

The report is organized to address identified security vulnerabilities and propose mitigation measures to assist in implementing and maintaining a more robust security posture. The report provides historical threat information, identifies current vulnerabilities, and recommends potential mitigation products or technologies.

This abbreviated assessment accomplishes the following:

- Complements each location's existing security initiative and improvement plans;
- Assesses security vulnerabilities considering recent events and the current threat environment targeting similar facilities and institutions;
- Assesses each location's ability to detect and respond to external and internal physical security threats; and
- Determines the organization's ability to identify, respond to, and mitigate basic

emergencies and incidents.

USING THE TVRA TOOL

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, volunteer, contractor, etc., who has – or had – 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 it can justify spending/obtaining resources to prevent it. Unacceptable consequences can vary from organization to organization and must 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).

SCN’s TVRA tool is designed to provide a systematic method for performing a base-level security assessment of a facility. The TVRA is designed to follow security best practices for identifying threats to the facility, and ultimately identifying vulnerabilities and designing recommendations to defend against the identified threats.

The Process:

The TVRA is designed to provide the assessor with an easy-to-use tool that follows security best practices in order to understand the base-level security posture of a facility. It utilizes

standard security terminology and methodology to review the facility from a defense-in-depth "outside/in" approach. The assessor should follow the security questionnaire in the order the questions are presented, taking care to follow the logic of the questions, as they are designed to build off of each other – essentially walking the assessor from the facility's exterior perimeter into its inner sanctum, while considering each security layer during the process. It is a step-by-step, building block approach to assessing the facility.

Upon completion, the assessor will tabulate the risk score for each particular category. In this way, the TVRA provides the ability to identify not just the overall security posture for a facility, but individual areas that can be specifically identified and addressed. The next step is to complete the suggested recommendations section to address the identified vulnerabilities.

******IMPORTANT NOTE******

Specific review and guidance for the recommendations section must be provided by a member of SCN's professional security team or a recognized professional Community Security Director, Regional Security Advisor, or Regional Director to ensure that the recommendations align with the identified vulnerabilities.

Risk Scoring:

Assessors should utilize the tool to apply against their respective facility in the order in which the categories are provided; Surrounding Area, Perimeter, & Property Grounds, Lighting, Vehicle Access, Control & Parking, Building Façade, Exterior Doors & Windows, Access Control & Visitor Management, Video Surveillance Systems, Building Interior, Intrusion Detection Systems, Training & Exercises and Policies & Procedures. This outside/in approach provides a holistic methodology for assessing vulnerabilities much as an adversary would and provides the necessary insights for a defense-in-depth security posture.

In some instances, there will only be a *"yes"* or *"no"* answer.

Yes	▪ A *"yes"* score of 1 indicates that you have adequate and robust security for that question.
Some	▪ A *"some"* score of 2 indicates that you have some, but not necessarily adequate security for that question. Or, for example, *"Are property boundaries of the facility easily recognizable by visual means?"* In this instance, only *"some"* of the boundaries may be recognizable. *"Some"* allows for subjectivity by the assessor.
No	▪ An *"no"* score of 3 indicates that you do not have any security measures in place related to that question.
N/A	▪ *"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 – Surrounding Area, Perimeter, & Property Grounds it is possible to have a low-risk score of 1 - 14, a medium risk score of 15 - 28, and a high-risk score of 29 - 42. In this category, a facility operator may be willing to accept any risk score of 14 or below and choose to initiate action to reduce the risk for any score of 15 or higher. Scores are aggregated and totaled for each category, enabling both category specific and an overall general facility assessment. In addition, photographs of key areas may be uploaded for each category. It is recommended that JPEG files be uploaded into the document.

NSGP TVRA Completion Support

Upon completion of this document, an organization should contact SCN or a professional Federation Community Security Director, Regional Security Advisor, or Regional Director to schedule a consultation. These limited number of consultations are generally available on a first-come, first-serve basis.

During that consultation, and should one be available, a professional will work with an organization to translate the findings into recommendations, providing the foundation for an organization to complete the *Investment Justification* of the NSGP grant application.

This information has been prepared to help organizations 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 receiving a comprehensive security assessment should contact SCN, a local Federation Community Security Director, Regional Security Advisor, or Regional Director, if available, law enforcement, or a Protective Security Advisor with the U.S. Department of Homeland Security.

THREATS TO JEWISH FACILITIES/INSTITUTIONS

FBI HATE CRIME DATA

This summary provides an overview of open-source statistics regarding reported antisemitic incidents in the United States and Canada. Please note, that the NSGP requires threat data specific to the applicant; this information is meant to be general and contextual in nature. It is not sufficient to effectively complete the NSGP application. All statistics included in this summary were obtained through open sources and may contain unofficial data. This summary should be considered preliminary in nature. Exact counts are subject to change pending official end-of-year data reporting.

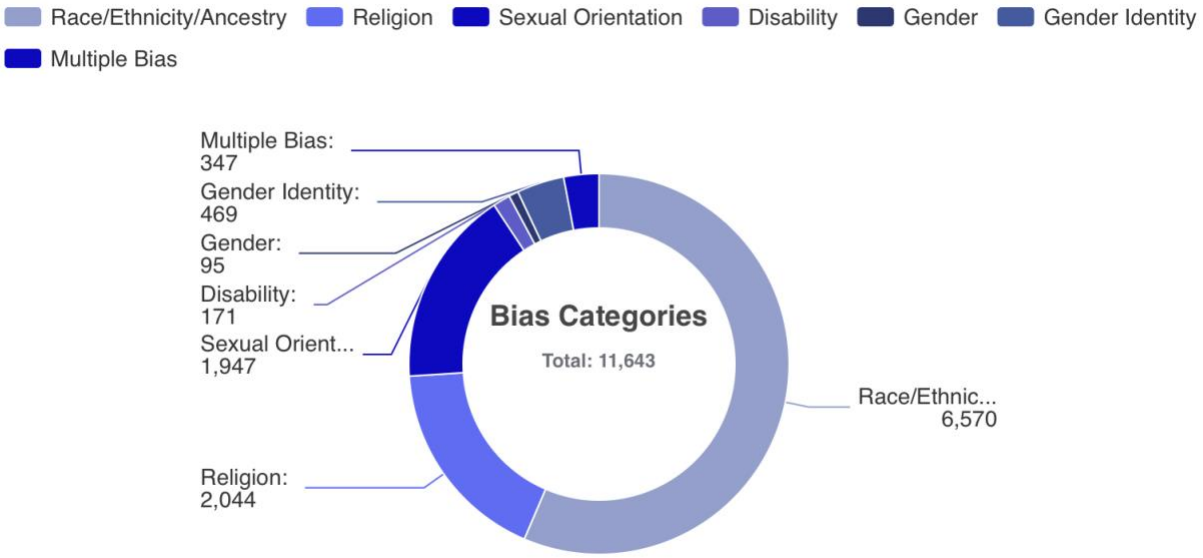
The FBI numbers for 2022 indicate a slight increase in both the overall hate crimes and hate crimes directed against the Jewish community. This increase demonstrated improved reporting following an adjustment period for law enforcement agencies to provide hate crime data to the federal government. It is important to note this as there have been four deadly attacks against the Jewish community since just October 2018. For 2022, 2,044 of the 11,643 (18%) hate crimes reported to the FBI were religiously motivated. Of these, 1,305 (65%) were motivated in whole or in part by anti-Jewish bias. In comparison, in 2021, 324 of the 1,013 religiously motivated hate crimes (32%) were anti-Jewish, out of 7,303 hate crimes reported.

Bias Motivation Categories	2022	2021
Race/Ethnicity/Ancestry	6,567	6,643
Religion	2,042	1,590
Sexual Orientation	1,944	1,707
Gender Identity	469	342
Disability	171	152
Gender	95	96
Total	11,288	10,530

• Of the 1,305 anti-Jewish hate crimes reported in 2022, 775 (59%) included property damage or vandalism, 358 (27%) were intimidation, 103 (8%) simple assaults, 38 (3%) aggravated assaults, and 8 (1%) theft offenses.

• Of the known locations in which the reported anti-Jewish hate crimes occurred, 208 (16%) occurred in homes, 116 (9%) on streets or sidewalks, 109 (8%) in schools, and 90 (7%) in parks or playgrounds.

• Of the 1,139 reported direct victims, 731 (57%) were individuals, 201 (16%) were businesses, 157 (16%) were government-related, and 42 (6%) were religious organizations



Information for the FBI comes from 2022 Hate Crime statistics.

ADL – 2022 DATA

In 2022, ADL recorded 3,697 antisemitic incidents in the United States; a 36% increase when compared to 2021. This is the highest number on record since ADL began tracking antisemitic incidents in 1979. Incidents increased over several incident types: antisemitic harassment increased 29% to 2,298; antisemitic vandalism increased 51% to 1,288 and antisemitic assaults increased 26% to 111. Notably, visibly Orthodox Jews were targeted in 53% of the assault incidents nationally.

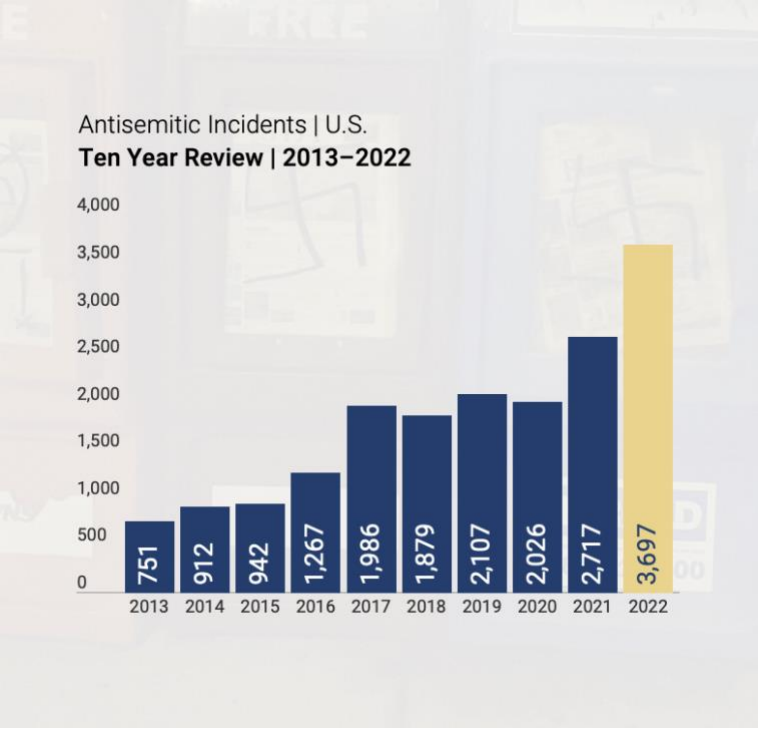
In 2022, the ADL reported 589 incidents at Jewish institutions such as synagogues, Jewish community centers, and Jewish schools, an increase of 12% from the 525 incidents reported in 2021. In addition, there were 219 antisemitic incidents at colleges and universities in 2022, an increase of 41% from the 155 incidents in 2021. Of the 219 campus incidents, 127 were incidents of harassment, 90 were vandalism, and two were assaults.

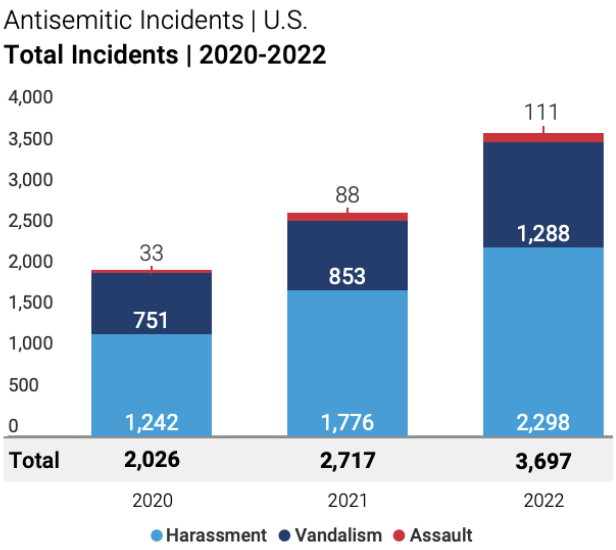
- Of the 3,697 incidents in the United States, 2,298 incidents were categorized as

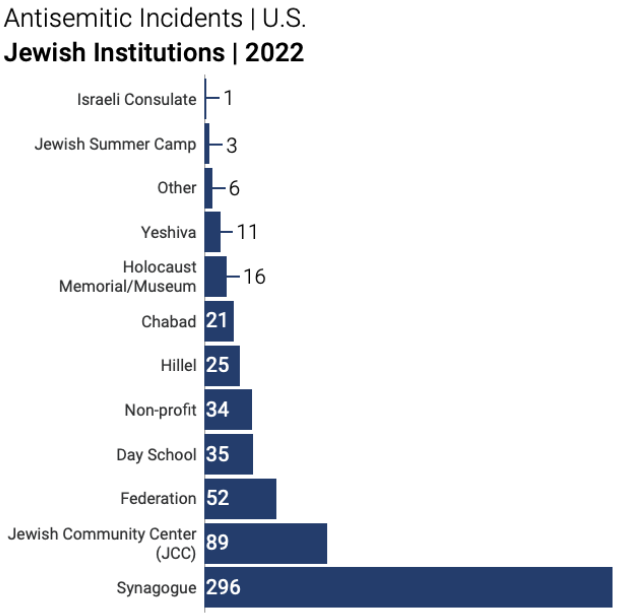
harassment, defined as cases where one or more Jewish people (or people perceived to be Jewish) were harassed verbally or in writing with antisemitic slurs, stereotypes, or conspiracy theories.

- Of the total 3,697 incidents in the United States, 1,288 incidents were categorized as vandalism, defined as cases where property was damaged in a manner that incorporated evidence of antisemitic intent or which had an antisemitic impact on Jews. Swastikas, which are generally interpreted by Jews to be symbols of antisemitic hatred, were present in 792 of these incidents.

- Of the total 3,697 incidents in the United States, 111 incidents were categorized as assault, defined as cases where Jewish people (or people perceived to be Jewish) were targeted with physical violence accompanied by evidence of antisemitic animus.







Information for the ADL comes from the [Audit of Antisemitic Incidents 2022](#).

HOW TO READ THIS DOCUMENT

Within each category is a list of recommendations to help mitigate the potential vulnerabilities noted through the self-assessment process. The security professional reviewing the report may utilize the pre-established "recommendations" for each category or make specific notes in the Additional Comments/ Recommendation section. Each recommendation may be assigned a priority level as follows:

[P1] HIGH Priority – Strongly recommended to provide the appropriate level of protection, safety, and security.

[P2] MODERATE Priority – Important to maintain the appropriate level of protection, safety, and security.

[P3] LOW Priority – Recommended for best-practice consideration but not critical to the maintenance of safety and security under most conditions.

The recommendations provided indicate mitigation strategies that can be used with the NSGP application process. The mitigation strategies can be translated into physical security solutions that may be eligible for NSGP funding.

Shown below is an example of recommended mitigations and priority levels for vulnerabilities identified during the self-assessment process. The reviewing security professional may choose from a list of pre-established "recommendations" and assign a priority based on the review of the self-assessment process.

Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

P1	Install & implement a Visitor Management System for identification and processing of visitors prior to access - 14SW-01-SIDP
P2	Install & implement an Access Control System to ensure entry doors are closed and secured at all times - 14SW-01-PACS
P3	Install signage advising of visitor access control policies and procedures – NO AEL

SITE CHARACTERISTICS & GENERAL INFORMATION

FACILITY NAME _____ **DATE CONDUCTED** _____

ADDRESS _____

Brief Description of Property and Surrounding Area: (Identify all key features of the facility, property, and surrounding areas. This will assist reviewers of the assessment in identifying important components of the facility that will be part of the overall assessment evaluation.)

Security Incidents on or Around the Property: (Identify any security incidents on or around the facility's property. Examples may be previous issues with transients, disruptive persons, suspicious person's reports, etc.)

ASSESSMENT FINDINGS

SURROUNDING AREA, PERIMETER, & PROPERTY GROUNDS

A facility's surrounding area may comprise of activities that contribute to criminal behaviors or other nefarious actions. Well maintained and defined property grounds display a distinct transition or boundaries between the surrounding area and the facility area. Perimeter security measures should be considered your first line of defense in a comprehensive defense-in-depth security plan. Well-defined boundaries between public and private areas can be achieved by using physical elements such as fences, architectural design and water features, pavement treatment, art, signage, and landscaping to express ownership and identify intruders and individuals who do not belong. The proper application of these types of items can achieve measures of perimeter access control by incorporating deterrence and delay into the security design. In order to perform a perimeter review, the assessor must physically walk around the outer boundaries of the facility property and answer the following questions.

Assessment Section

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, with a clear delineation between the facility's property and adjacent properties?				
2. Is the facility visible from the street during both day and night so that police/security patrols can conduct external security checks?				
3. Is the immediate area of the facility void of "crime generators"? (Crime generators may include late-night social, shopping, retail establishments, and entertainment areas)				
4. If the facility is adjacent to a public use facility (i.e., park, walking trail, etc.), is there a fence or other barrier separating the facility from the public use facility?				
5. Is there a marquee or other sign visible from the adjacent roadway that identifies the presence of the facility?				
6. Does the facility have the appropriate security warning signs displayed around the perimeter of the premises? Such as "No Trespassing" or "Video Surveillance System In Use" signs posted at the site perimeter?				
7. Can the perimeter of the site be secured to prevent unauthorized vehicles or pedestrians from entering?				
8. Can site entry points be readily observed and monitored by staff and individuals in the facility in the course of their normal activities?				
9. Does the site have perimeter fencing that is free of visual obstructions and clearly identifies the boundary of the premises?				
10. Are the fences 6 to 8 feet high and in good condition?				

11. Are gate locks/bars in place and secured when not in use?				
12. Are any exterior playgrounds fenced with a restricted entry point?				
13. Are bushes, shrubbery, or other plant growth trimmed in an appropriate manner so as not to serve as a hiding place, ambush points, or areas of concealment?				
14. Are exterior or detached storage buildings or facilities well-constructed and secured?				
Totals	0	0	0	0
Risk Level:	Low 1-14	Med 15-28	High 29-42	

Photographs (upload photographs of key issues here – JPEG format)

Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

Additional Comments/ Recommendations

ASSESSMENT FINDINGS

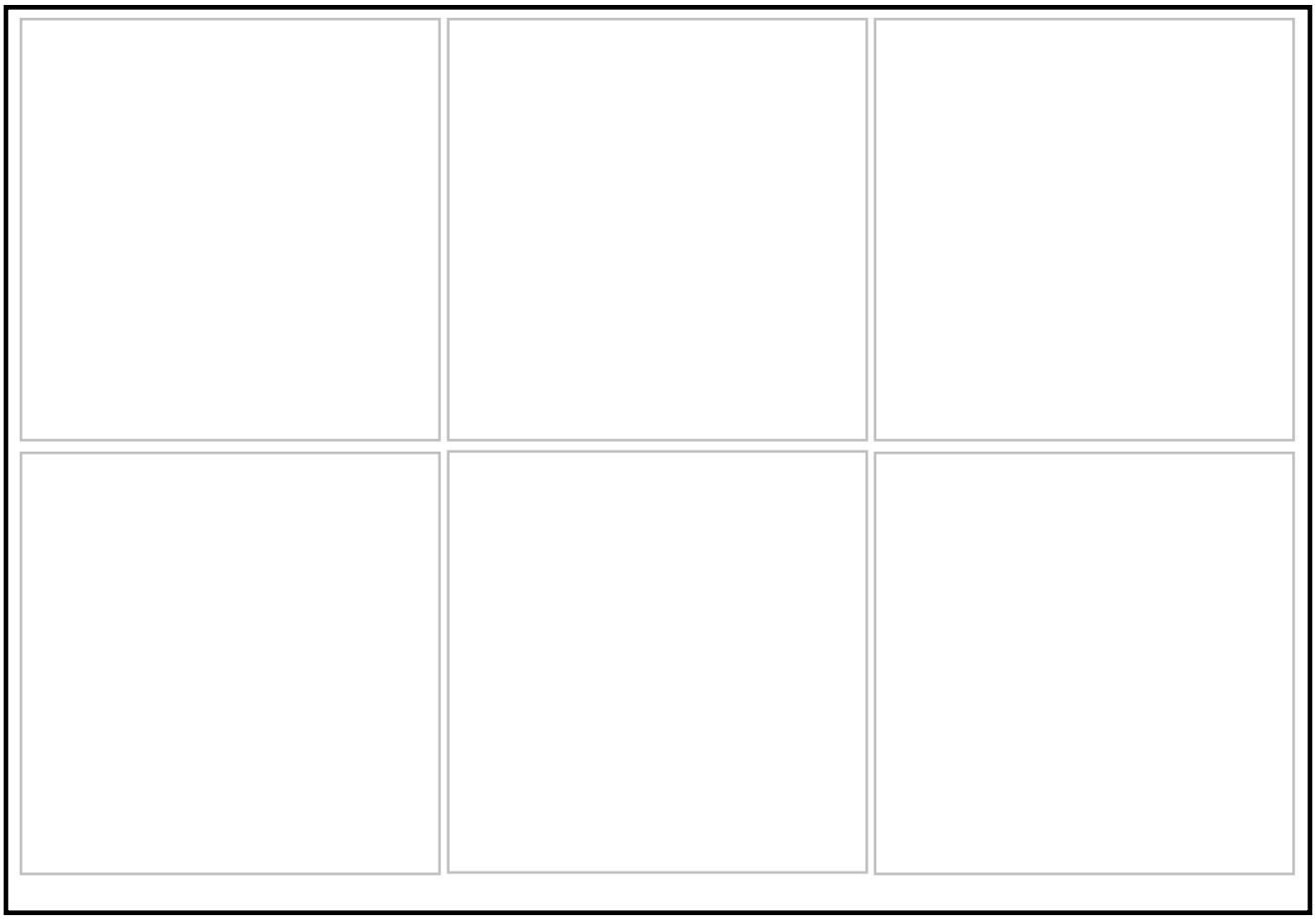
LIGHTING

Security lighting systems are an essential element of a physical security protection program assisting in the first line of deterrence, detection, response, and defense. Security lighting systems are utilized to provide enough illumination to enable a person or a camera system to assess a security area or zone for general safety, hazards, or threats. As part of the first phase of a security system, adequate lighting will not only assist with general safety awareness and threat detection but can also serve as a psychological deterrent to nefarious activity. In order to perform a review of the facility's lighting, the assessor must physically walk around the facility in dusk and darkness conditions and answer the following questions to fully assess the facility's lighting posture.

Assessment Section

Indicate the answer that best applies	Yes=1	Some=2	No=3	N/A
1. Is the facility's perimeter illuminated along all property lines?				
2. Are designated parking lots or parking areas well-lighted?				
3. Are pedestrian walkways and building entrances well-lighted?				
4. Are all sides of the building illuminated by exterior lighting?				
5. Are exterior lighting fixtures free of obstructions by vegetation or man-made obstacles?				
6. Is exposed equipment protected against vandalism and damage?				
7. Are exterior lights checked weekly for functionality?				
8. Is there a reliable system or process for the timely reporting and repair of inoperable external lighting?				
Totals	0	0	0	0
Risk Level:	Low 1-8	Med 9-16	High 17-24	

Photographs (upload photographs of key issues here – JPEG format)



Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

Additional Comments/ Recommendations

ASSESSMENT FINDINGS

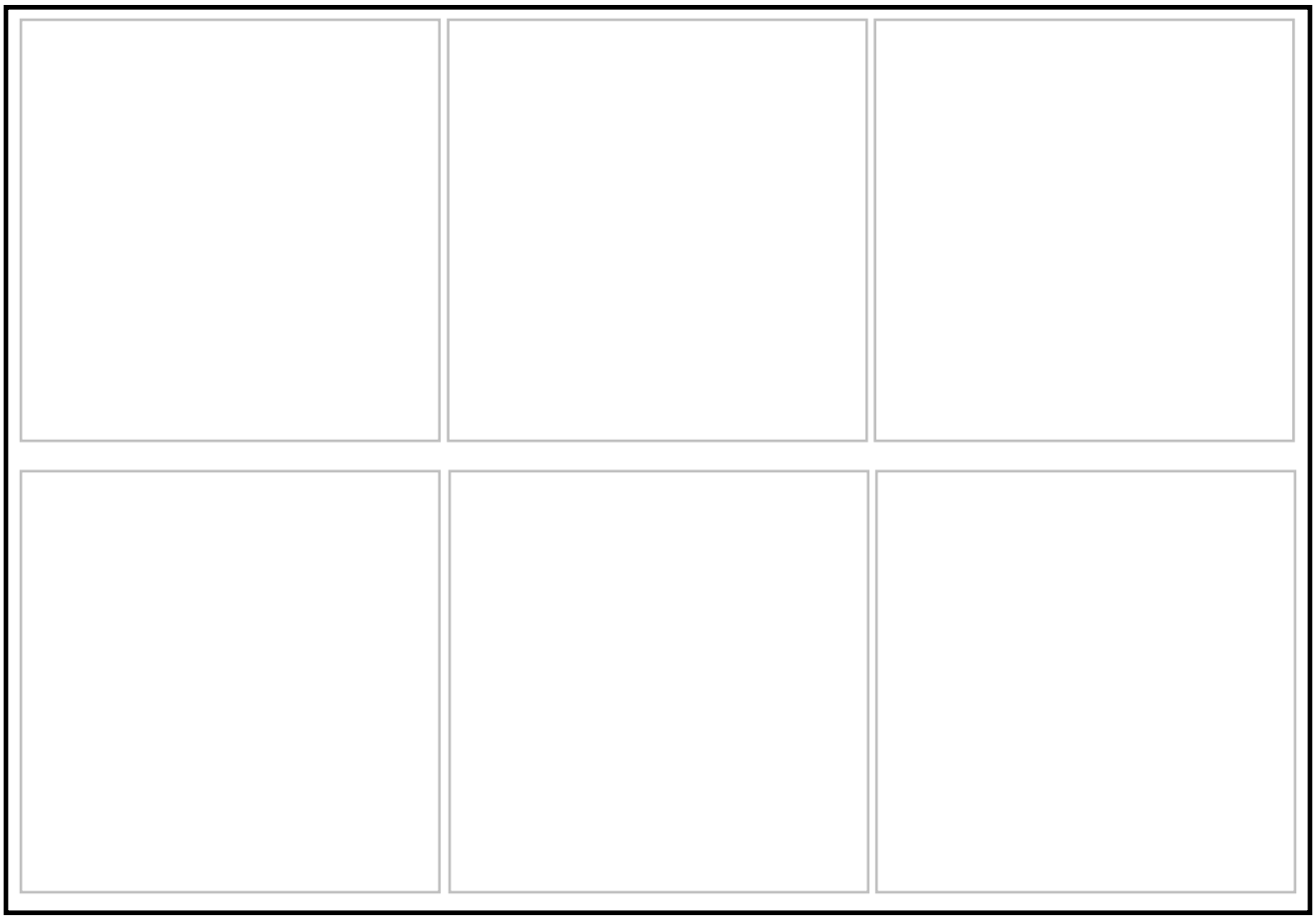
VEHICLE ACCESS CONTROL & PARKING

Vehicle access and control processes can provide an important element in providing the first impression of a facility's security posture. The adequate ordering of vehicle entrances, parking, and egress provides both long-term users and newcomers with a familiarity with structure and order that can be carried throughout a facility's environment. By offering clear site lines, stand-off distances, and orderly vehicle flow and parking control, facilities can limit their exposure to general safety issues such as accidents and pedestrian strikes to more serious criminal activity, as well as reduce response times for emergency personnel should an emergency or security incident occur. In order to adequately review the facility's vehicle access control and parking, the assessor should be present during times of high vehicle and pedestrian traffic to completely observe and answer the following questions.

Assessment Section

Indicate the answer that best applies	Yes=1	Some=2	No=3	N/A
1. Are roadways through the site serpentine or otherwise indirect?				
2. Can vehicle entry beyond checkpoints be controlled, permitting entry by only one vehicle at a time?				
3. Are there perimeter barriers capable of stopping vehicles?				
4. Are there clear, traffic-calmed pick-up/drop-off points?				
5. Do curb lanes adjacent to the building prohibit parking?				
6. Is parking allowed adjacent to the facility or gathering areas limited to authorized/ vetted vehicles and personnel?				
7. Are visitor parking areas specifically marked to better identify visitors to the facility?				
8. Are vehicles parked at the facility monitored or checked?				
9. Does the facility have a policy to address vehicles parked for an extended period (e.g., reporting to security, local law enforcement, or tow company)?				
10. Are designated parking spaces non-descriptive. For example, does not identify positions such as Rabbi, Principle, Fed Executive, etc.				
11. Are exterior mechanical, electrical, or other utility equipment areas that are reachable by vehicles protected with bollards or other devices?				
Totals	0	0	0	0
Risk Level:	Low 1-11	Med 12-22	High 22-33	

Photographs (upload photographs of key issues here – JPEG format)



Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

Additional Comments/ Recommendations

ASSESSMENT FINDINGS

BUILDING FACADE, EXTERIOR DOORS, & WINDOWS

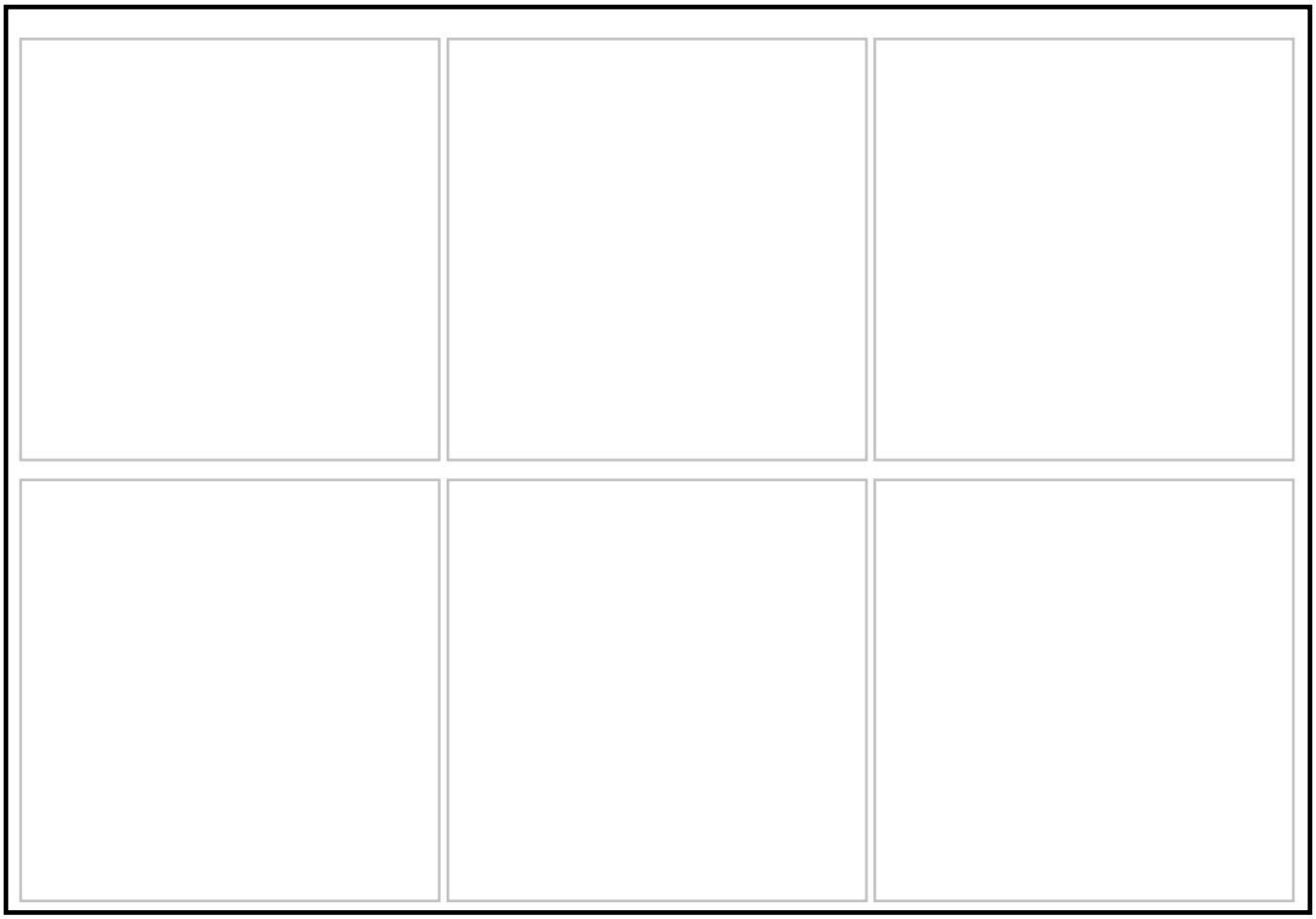
A building's façade including the exterior windows and doors is a key component to a defense-in-depth security approach and is a mainstay of any adequate physical security program. Properly secured systems and utilities help to ensure the security of a facility. Secure exterior windows and doors provide for both the deterrence and delay of any criminal activity or attack. Identifying and securing/hardening exterior windows and doors should be a priority in any physical security program. Additionally, exterior windows and doors must provide not just adequate protection, but also adequate, identifiable, and safe access for first responders, as well as egress for individuals in case of an emergency. In order to assess the security of the facility's exterior doors and windows, the assessor must physically observe, approach, and attempt to enter/exit the individual doors and windows to adequately answer the following questions.

Assessment Section

Indicate the answer that best applies	Yes=1	Some=2	No=3	N/A
1. Other than the main entrance, are doors to the facility closed and locked to prevent unauthorized access and limit the possibility of an intruder?	☐	☐	☐	☐
2. Are exterior doors referenced above equipped with propped open alarms?	☐	☐	☐	☐
3. Are all entrances marked in a uniform numbering system (e.g., the main entrance is #1 and numbered clockwise from there; doors should include the markings on both the interior and exterior of the door)?	☐	☐	☐	☐
4. Are door hinges concealed and thus not exposed and vulnerable to tampering? (Exposed hinge pins can be quickly "popped," allowing the door to be breached.)	☐	☐	☐	☐
5. Are perimeter entryways equipped with full flush metal or solid core doors at least 1 3⁄4" thick and secured with deadbolt locking devices?	☐	☐	☐	☐
6. Are the locks on all building entry points functional and in a good state of repair?	☐	☐	☐	☐
7. Are exterior doors equipped with high-quality cylindrical locks with a deadbolt at least 1" in length?	☐	☐	☐	☐
8. Are exit doors equipped with push bars allowing for a quick exit?	☐	☐	☐	☐
9. Are Emergency egress doors equipped with an alarm that sounds at a central location (such as security, reception, or administration) and in the immediate area of the door when the doors are opened?	☐	☐	☐	☐
10. Do exterior doors have narrow windows, sidelights, fish-eye viewers, or cameras to permit seeing who is on the exterior side?	☐	☐	☐	☐
11. Are doors periodically checked for proper operation, ensuring that locks actually latch when the door is closed?	☐	☐	☐	☐

12. Do you designate staff to check that all doors are closed and locked at the end of the business day?				
13. Are exterior door systems designed to resist the effects of blast and forced entry through security film, laminate, wire mesh, steel shutter, security drapes, or other applications that offer enhanced protection from debris and enhanced security?				
14. Is the glass in a door or within a door frame 3 feet from the door lock, resistant to breaking?				
15. Are windows and sidelights sized and located so that if they are broken, persons cannot reach through and open a door from the inside?				
16. Are all exterior windows easily locked?				
17. Are window hardware and frames in good condition or reinforced with slide bolts or other security devices?				
18. Are windows designed to serve as a secondary means of escape not blocked by security bars/grills, louvers, awnings, or other devices that would prevent escape?				
19. Are windows designed and located to resist the effects of gunfire and forced entry?				
20. Do windows have security film, laminate, wire mesh, steel shutters, security drapes, or other application that offers enhanced protection from debris and enhanced security?				
21. Is the exterior of the building void of any recesses or alcoves that can serve as hiding places or places of concealment for intruders?				
22. Are building utilities (electric, gas, water, communication) connections protected/ secured against tampering?				
23. Are HVAC air intakes located along the building façade 16 feet above the ground?				
24. Are dumpsters, trash containers, mailboxes, vending machines, and other fixtures and features that could conceal devices secured and situated away from building entrances and entry points?				
25. Does the facility have a backup generator?				
Totals	0	0	0	0
Risk Level:	Low 1-25	Med 26-50	High 51-75	

Photographs (upload photographs of key issues here – JPEG format)



Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

Additional Comments/ Recommendations

ASSESSMENT FINDINGS

ACCESS CONTROL & VISITOR MANAGEMENT

Access control and visitor management refers to the efficient identification of individuals authorized to enter a facility, as well as the understanding of where they are, how long they are authorized to be there, and when they are scheduled to leave. An efficient access control and visitor management program can also serve as a barrier to entry for those individuals who are not authorized to be on the premises. In order to assess the facility's access control & visitor management system, the assessor must be onsite to observe the facility and visitor access process or have significant up-to-date knowledge to answer the following questions.

Assessment Section

Indicate the answer that best applies	Yes=1	Some=2	No=3	N/A
1. Does the facility maintain a presence of security personnel, such as off-duty police or a uniformed professional security agency?	☐	☐	☐	☐
2. Do all staff wear facility-issued identification credentials while on the premises?	☐	☐	☐	☐
3. Are separate wings, buildings, doors, and windows externally marked for emergency responders?	☐	☐	☐	☐
4. Have external markings been coordinated with local first responders?	☐	☐	☐	☐
5. Does the facility have a "Knox" box or other means to provide first responders with access to facility keys or access media?	☐	☐	☐	☐
6. Have steps been taken to restrict unauthorized access to the roof, such as ladders and other items that could be used to access the facility's upper floors and/or rooftops secured?	☐	☐	☐	☐
7. Is roof access from inside the building only and locked?	☐	☐	☐	☐
8. Are mechanical equipment enclosures on the roof protected from unauthorized access or vandalism?	☐	☐	☐	☐
9. Is entry granted by supervising staff, greeters, ushers, or through the use of proximity cards, keys, coded entries, or other devices?	☐	☐	☐	☐
10. Is the designated visitor entry point under the visual supervision of a receptionist or administrative office?	☐	☐	☐	☐
11. Does the facility utilize a Visitor Management System?	☐	☐	☐	☐
12. Are visitors required to have an appointment?	☐	☐	☐	☐
13. Does visitor access allow for stand-off/remote identification?	☐	☐	☐	☐
14. Are visitors asked to provide proof of identification (govt. issued) and sign in/out?	☐	☐	☐	☐

15. Are visitors provided with visitor passes?				
16. Are passes dated and designed to look different from staff identification?				
17. Are visitor passes collected from visitors when they sign out?				
18. Does staff challenge or offer to assist people not wearing a visitor's pass or identification credential?				
19. Do visitors have to check in at an administrative office or desk before they can access other parts of the building?				
20. Can doors be electronically locked to block visitors' entry into the building?				
21. Are there established procedures and/or signage to prevent visitors from accessing unauthorized areas such as utility rooms and sensitive areas?				
22. Are there exit signs in all relevant languages and with simple maps or diagrams where needed to direct visitors to designated building exits?				
23. Are all incoming deliveries inspected before being delivered to the designated recipient?				
Totals	0	0	0	0
Risk Level:	Low 1-23	Med 24-46	High 47-69	

Photographs (upload photographs of key issues here – JPEG format)

Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

Additional Comments/ Recommendations

ASSESSMENT FINDINGS

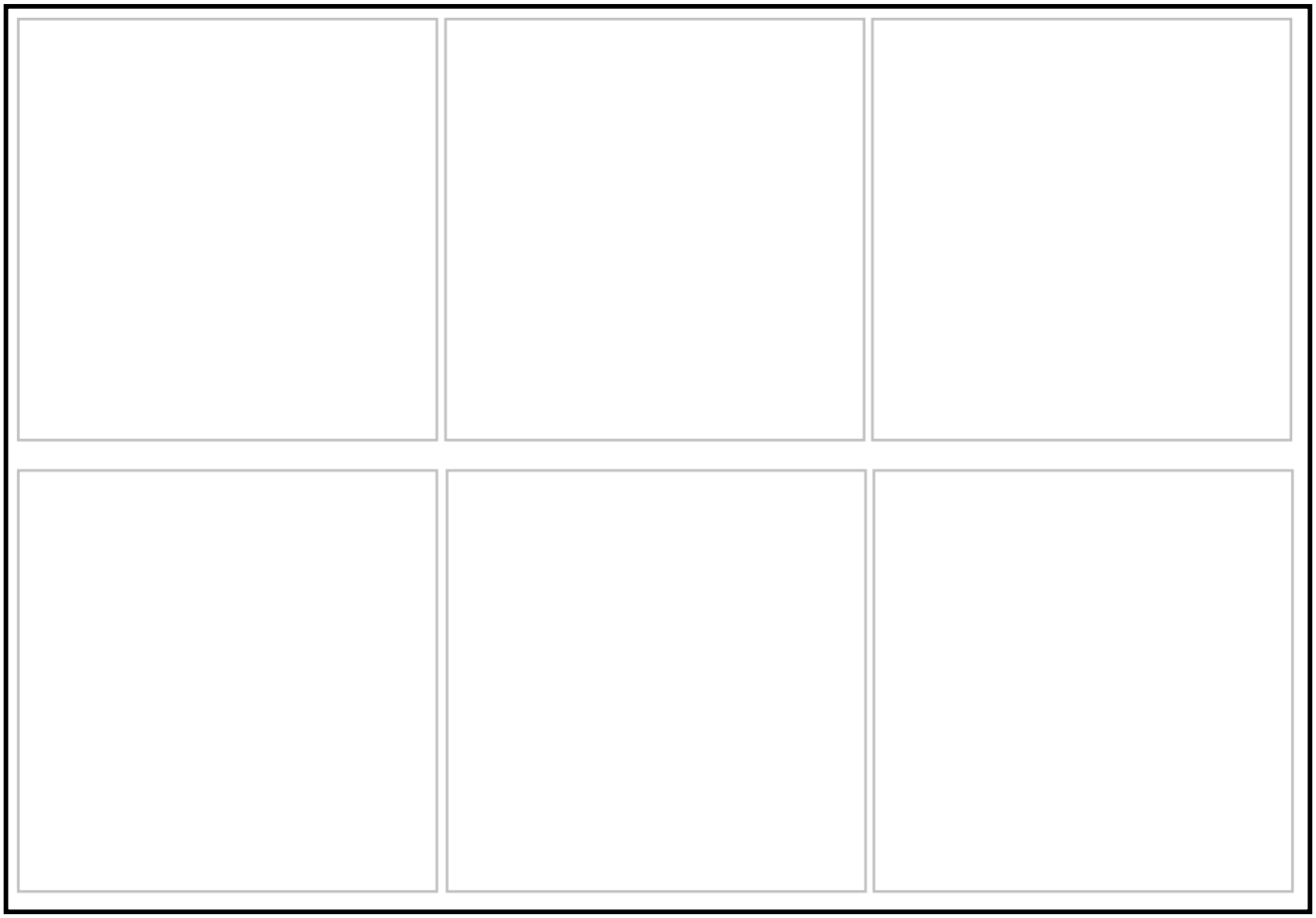
VIDEO SURVEILLANCE SYSTEMS

Video surveillance systems provide a method for detecting, identifying, and potentially initiating responses to emergency situations. Video systems also provide a means for evidence collection and storage in the event of criminal or suspicious activity. Video systems should be both internal and external to provide efficient coverage of areas of concern to a facility including building perimeter, building access and egress points, secure areas within the building, and other sensitive areas as identified by the facility such as meeting rooms, server rooms and areas with expensive property. In order to assess the facility's video surveillance system (if applicable), the assessor must physically observe each camera and camera location, as well as the remote video images at monitoring locations in order to answer the following questions.

Assessment Section

Indicate the answer that best applies	Yes=1	Some=2	No=3	N/A
1. Does the facility have a video camera/surveillance system installed?				
2. Does the facility have signs displayed informing the public/warning offenders they are being monitored and recorded?				
3. Does the video surveillance system cover all entrances, exits, loading docks, lobbies, facility perimeter, parking areas, stairwells, vehicle entrances, and other potential access points to the facility?				
4. Is there video surveillance of areas adjacent to the facility?				
5. Are the cameras actively monitored?				
6. Does the video surveillance system provide the intended coverage such that there are no blind spots/ zones in the camera coverage or areas where the view is blocked by vegetation or other obstructions?				
7. Do you have cameras covering critical areas in your business, such as server rooms or other sensitive areas?				
8. Is the video surveillance system nighttime capable?				
9. Is the video surveillance system regularly inspected and maintained?				
10. Are all of the cameras and recording devices in proper working order?				
11. Are images recorded offsite via web-base, retained for future use as needed, and stored in a secure area?				
12. Does local law enforcement have the ability to remotely access the video feed?				
Totals	0	0	0	0
Risk Level:	Low 1-12	Med 13-24	High 25-26	

Photographs (upload photographs of key issues here – JPEG format)



Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

Additional Comments/ Recommendations

ASSESSMENT FINDINGS

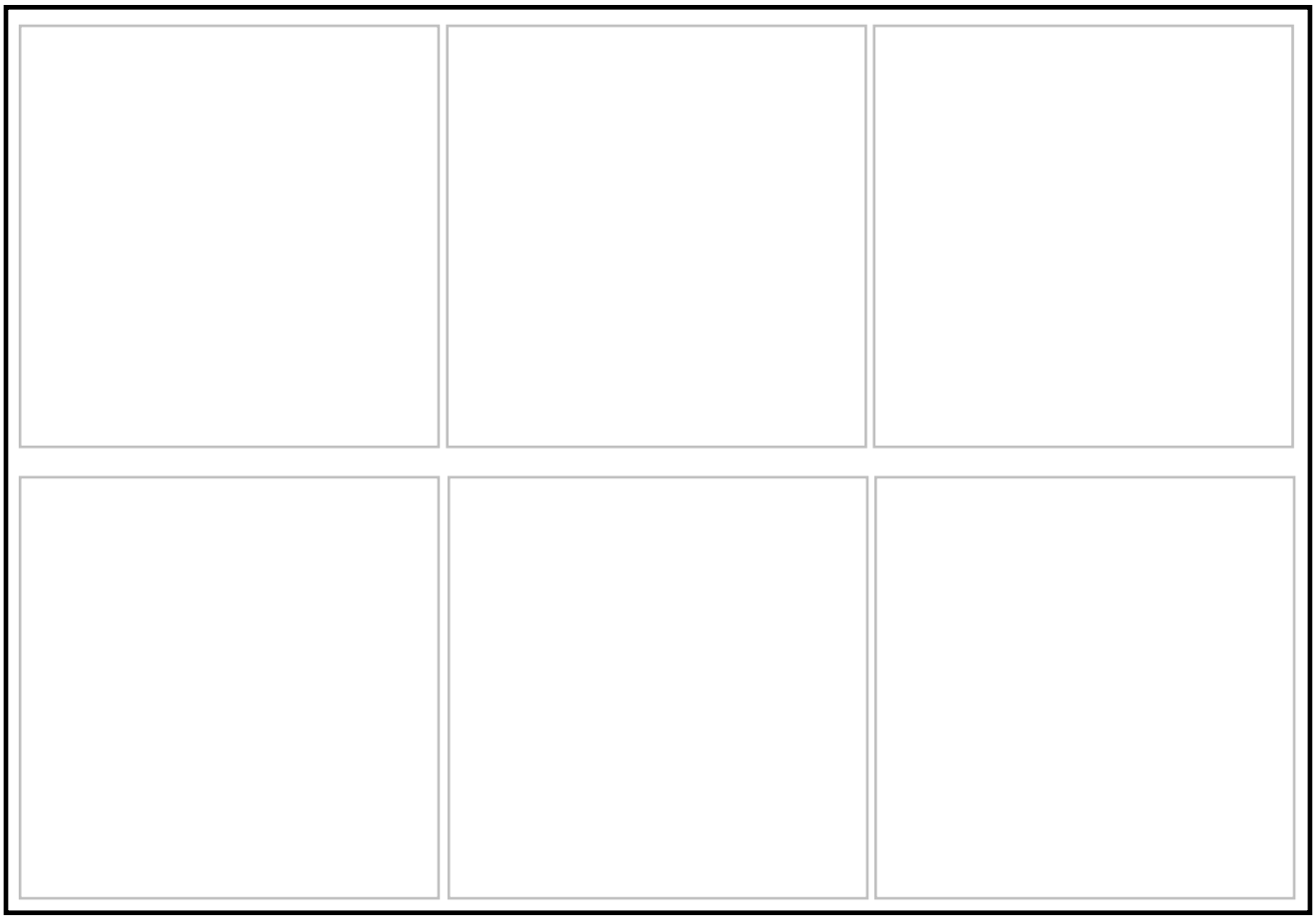
BUILDING INTERIOR

Interior security measures provide protection from insider threats, protect critical interior systems, and, for facilities with an "open door" policy, are the only line of defense between you and the public. Interior security should be an additional layer of control working in concert with exterior security measures as part of the overall layered levels of protection. Interior security is best implemented by creating interior layers of control, restricting access to critical areas of operation and personnel (offices, executive staff, school/classrooms, etc.) public versus private spaces and critical equipment. In order to review the facility's interior security posture, the assessor must physically walk the facility's interior in order to answer the following questions.

Assessment Section

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. Do interior doors lock on the inside of the room, office, etc.?				
4. 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?				
5. Are doors to utility, mechanical, electrical, and telecom rooms secured?				
6. Are recesses, niches, or blind corners visible with surveillance cameras?				
7. Are clear and precise emergency evacuation maps posted at critical locations, do they match their positions in the building, and include the building's address?				
8. Does the facility have a mass communication system for security and emergency announcements?				
9. Have local first responders toured the facility to gain a greater understanding of the physical layout?				
10. Do classrooms and other frequently used rooms have exterior window markings for easy identification by first responders?				
11. Do responding law enforcement agencies have copies of the building's floor plans?				
Totals	0	0	0	0
Risk Level:	Low 1-11	Med 12-22	High 23-33	

Photographs (upload photographs of key issues here – JPEG format)



Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

Additional Comments/ Recommendations

ASSESSMENT FINDINGS

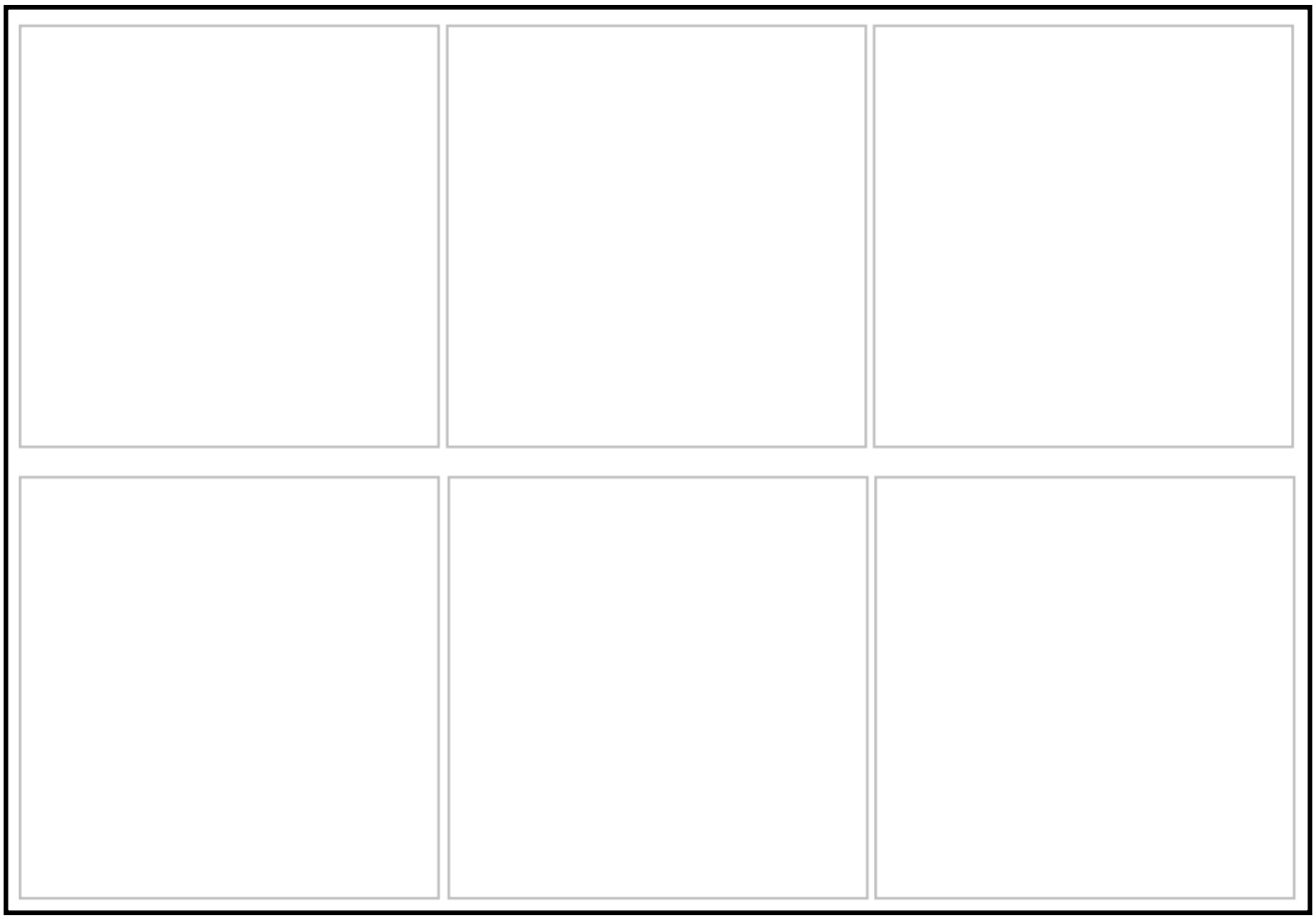
INTRUSION DETECTION SYSTEMS

This section reviews the selection, application, and performance of Intrusion Detection Systems. This includes lighting, access control systems, intrusion detection systems, security camera systems, duress/panic systems, emergency phones and communications, intercom systems, and applicable detection and screening systems. Reliable systems can offer front-line and immediate deterrence, detection, notification, and response capabilities to any sound physical security program. In order to assess the facility's security systems (if applicable), the assessor needs to have knowledge of the system(s). This can be accomplished by physically inspecting and testing the system where applicable, as well as interacting with the company that installed and maintains the system(s).

Assessment Section

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. 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?				
3. Does the intrusion detection system cover all exterior entry/exit points?				
4. Is the intrusion detection system armed (activated) every night and other times when the facility is not in use?				
5. Are the arm/disarm codes for an intrusion detection system changed and reissued at least annually?				
6. Does the intrusion detection system have a cellular or backup power supply?				
7. Is there a preventive maintenance program for the intrusion detection alarm system?				
8. Are panic or duress alarm buttons installed at the reception desk and other critical areas, and are remote fobs used?				
9. Are panic alarms linked to the entire facility and EMS and routinely tested?				
Totals	0	0	0	0
Risk Level:	Low 1-9	Med 10-18	High 19-27	

Photographs (upload photographs of key issues here – JPEG format)



Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

Additional Comments/ Recommendations

ASSESSMENT FINDINGS

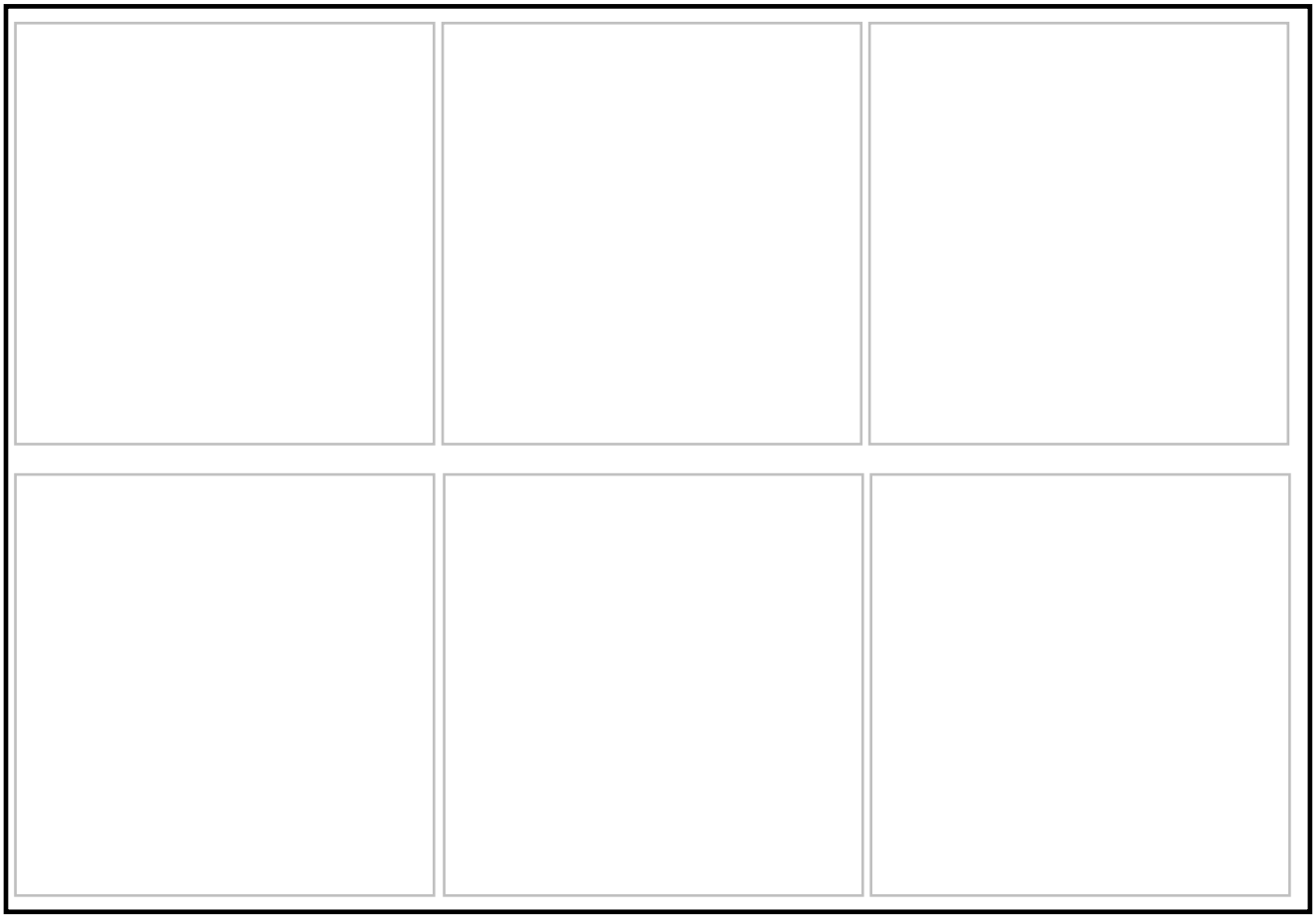
TRAINING & EXERCISES

Training and exercises are among the most cost-effective measures organizations can utilize to increase their overall security posture. Examples of training are SCN's Countering Active Threat Training (CATT), Stop the Bleed, and Be Aware training. Adequate and recurrent training and certification in base-level security techniques and procedures is a foundational physical security posture. In order to assess the training & exercises section, the assessor should have knowledge of the facility's emergency management and training programs. These functions often reside with the facility's emergency management committee, security committee, or specifically designated individual(s). The assessor should either have direct knowledge of these categories or contact the appropriate persons in order to answer the following questions.

Assessment Section

Indicate the answer that best applies	Yes=1	Some=2	No=3	N/A
1. Have all employees been provided with annual security awareness training?	☐	☐	☐	☐
2. Are ushers, greeters, and volunteers trained in security awareness and threat detection?	☐	☐	☐	☐
3. Are your telephones pre-programmed with emergency contact numbers?	☐	☐	☐	☐
4. Are staff trained, and have they practiced/ exercised their responsibility to handle emergencies in the last twelve months?	☐	☐	☐	☐
5. Are staff trained and have they practiced their response to handle the following emergencies?				
a) Nuisance phone calls	☐	☐	☐	☐
b) Active shooter/Active assailant threat	☐	☐	☐	☐
c) Evacuation	☐	☐	☐	☐
d) Severe weather	☐	☐	☐	☐
e) Suspicious bags/packages/bomb threat	☐	☐	☐	☐
f) Fire	☐	☐	☐	☐
g) Workplace violence	☐	☐	☐	☐
h) Vehicle-Borne Improvised Explosive Device (VBIED)	☐	☐	☐	☐
Totals	0	0	0	0
Risk Level:	Low 1-12	Med 13-24	High 25-36	

Photographs (upload photographs of key issues here – JPEG format)



Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

Additional Comments/ Recommendations

ASSESSMENT FINDINGS

POLICIES & PROCEDURES

Policies and procedures describe the methods and techniques an organization uses to maintain its security posture and are unique to each security category. Policies and procedures help to establish the process, method, order, and accountability of security programs that have been established by an organization. In order to assess the security policies and procedures section, the assessor should have knowledge of the facility's security policies and procedures program. These functions often reside with the facility's emergency management committee, security committee, or specifically designated individual(s). The assessor should either have direct knowledge of these categories or contact the appropriate persons in order to answer the following questions.

Assessment Section

Indicate the answer that best applies	Yes=1	Some=2	No=3	N/A
1. Does the facility have a security manager or security committee to make security management decisions?	☐	☐	☐	☐
2. Are there regular meetings with the staff to discuss security issues?	☐	☐	☐	☐
3. Does the facility receive threat information, security-related bulletins, advisories, or alerts from an external source?	☐	☐	☐	☐
4. Are mechanisms in place for employees, volunteers, and congregants to report behaviors that raise safety concerns to the security force and/or the facility leadership?	☐	☐	☐	☐
5. Does the facility interact with law enforcement and neighboring businesses/facilities on issues of security and crime trends that might affect everyone?	☐	☐	☐	☐
6. Does the facility have written security policies and procedures, and crisis response plans?	☐	☐	☐	☐
7. Does the facility have a lockdown, lockout, and shelter-in-place procedures?	☐	☐	☐	☐
8. Does the facility regularly conduct training to exercise security and crisis response policies and procedures?	☐	☐	☐	☐
9. Does the facility assign personnel to provide a security presence during times of critical vulnerability (i.e., during congregant arrival/departure, special events)?	☐	☐	☐	☐
10. Does the facility increase security for large events or mass gatherings?	☐	☐	☐	☐
11. Is there a policy that requires a background check of staff and volunteers?	☐	☐	☐	☐
12. Is there a single person responsible for access control media (cards/ fobs) and key issuance and record keeping?	☐	☐	☐	☐
13. Are access control media and keys stored in a locked cabinet with limited, auditable access?	☐	☐	☐	☐

14. Are lost access control media and keys investigated?				
15. Is there a written, up-to-date child and student safety and protection policy, to include a security training program for employees and volunteers?				
16. Is there a policy that requires that two or more adults be present during facility-sponsored programs involving children and youth?				
17. Is there a child-tag system or other child check-in and drop-off procedure?				
18. Is the facility exclusively used by the parent organization and not rented or leased to other organizations on a daily or regular basis?				
19. Does the organization prohibit or discourage the use of the facility for special events that would draw large crowds or pose iconic significance?				
20. Are these groups or organizations required to follow the established facility security and emergency plans?				
21. Are local first responders made aware of an increase in population due to special events and/or potential threats?				
Totals	0	0	0	0
Risk Level:	Low 1-21	Med 22-42	High 43-63	

Photographs (upload photographs of key issues here – JPEG format)

Recommendations Section Below should be completed in consultation with a Security Professional

Recommendations (Select from drop-down arrows)

Additional Comments/ Recommendations
