



FAITH-BASED COMMUNITY SELF-ASSESSMENT USER GUIDE



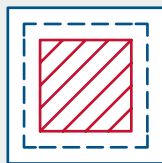
INTRODUCTION

This user guide provides a step-by-step sequence for navigating the Cybersecurity and Infrastructure Security Agency (CISA) Houses of Worship (HOW) Security Self-Assessment.

The Assessment, when completed, will provide an easy-to-follow road map for implementing suggested voluntary options for consideration. These options are based on current best practices designed to improve facility security and preparedness:



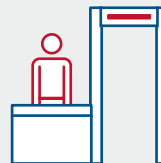
Security and
Safety/Emergency
Management



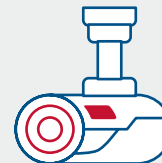
Perimeter Security/
Delineation



Parking and
Barriers



Access
Control/Entry
Control



Video Surveillance
Systems (VSS)

ASSESSMENT BASICS

Each question has either three or five answers. The answers and options for consideration are arranged from the lowest level of security that offers a very low level of protection (red) to a very high level of security that provides a greatly enhanced level of protection (green). None of this infers priority of actions to implement.

For each relevant question, identify the answer that most accurately represents your facility. Directly below the applicable answer is a corresponding option for consideration. It may be helpful to copy and paste the applicable option for consideration into a separate document or spreadsheet.

USE OF THE RESULTS

The tables in the self-assessment are designed to show a range of security and protection, from the lowest level of security that offers minimal protection (red) to a very high level of security that provides a greatly enhanced level of protection (green). None of these designations is meant to infer priority of actions to implement.

Each facility will be able to use the results of this security self-assessment to evaluate the most impactful, cost-effective options to improve their overall risk profile.

USING THE SELF-ASSESSMENT

Before starting, have a self-assessment available to easily move through the question sets. Afterwards, use the methodology depicted on the following page to evaluate your current security level and identify corresponding actions for improvement.

**STEP
1**

Use a **step-by-step process** to go through each question and identify your current posture.

**STEP
2**

After identifying your current posture, drop down to the corresponding option for consideration.

Consider the elements on the sliding scale to modify your security or preparedness level today or in the future.

**STEP
3**

Review and use the provided background, references for the self-assessment question, and additional resources to build and improve your security and lower your risk.

Example: You have identified the lack of a security plan. Gauge the level that you would like to achieve, and then use the resources referenced in the question to build a security plan

THE SELF-ASSESSMENT IN ACTION

Question	Very Low	Low	Medium	High	Very High
Does the house of worship have a security manager or security committee to make security management decisions?	The house of worship does not have a security manager or committee.	The house of worship has a security manager or committee, but security management activities are sporadic.	The house of worship has a security manager or committee. Security management activities are regularly scheduled, but not coordinated with other committees, departments, or groups (e.g., special events planning, childcare).	The house of worship has a security manager or committee. Security management activities are regularly scheduled and coordinated with other committees, departments, and groups, but additional personnel are needed to support the facility's security mission.	The house of worship has a security manager or committee. Security management activities are regularly scheduled and coordinated with other committees, departments, and groups, and staffing levels fully support the facility's security mission.
Option for Consideration	Designate an individual as a security manager or a group of individuals as a security committee, and ensure that person or group is responsible for developing implementing, and coordinating all security related activities. If the manager or committee members have no security or law enforcement background, make sure they reach out to local law enforcement to become acquainted. Provide security management training and/or access to training materials and resources.	Schedule regular meetings to review security procedures and incidents.	Coordinate safety and security planning with other committees, departments, and groups.	Hire or appoint additional personnel to support the facility's security mission.	Regularly assess the facility's security management program. Conduct security surveys, risk assessments, and threat assessments of the facility and neighboring areas. Implement best practices based on collaborative relationships and new or updated resources.

Your self-identified level of security

Your starting point for improving security

Continual Improvement Approach

EASY-TO-USE REFERENCES AND RESOURCES FOR EACH QUESTION**References:**

- ASIS, Securing Houses of Worship, asisonline.org/security-news/security-topics/securing-houses-of-worship/
- Interagency Security Committee (ISC), Facility Security Plan: An Interagency Security Committee Guide, cisa.gov/resources-tools/resources/isc-facility-security-plan-guide
- CISA, Security Planning Workbook, cisa.gov/security-planning-workbook

For more information:

- Protecting Houses of Worship resources and tools, cisa.gov/protecting-houses-worship.