



Risk Management *Tips*

Fight Bullying and Abuse with a Security Vulnerability Assessment

When bullying or abuse occurs, it can have an adverse impact on your organization's core belief of providing a safe place to learn and grow. Assessing your security and supervision policies will help identify areas that may need additional resources, such as increased supervision or monitoring to control unacceptable behaviors that lead to bullying and abuse allegations.

The National Fire Prevention Agency's *NFPA 730 – Guide to Premise Security* offers guidelines for a security vulnerability assessment (SVA). An SVA assesses the current status of an organization's vulnerabilities, including threat exposures, security features, and preparedness.



An SVA should include, but not be limited to, the following steps:

1. **Formation of a team.** Form a team of personnel from pertinent organizational areas and other stakeholders. This can include local staff, key members of related organizations, representatives from your community, and your insurance carrier, for example.
2. **Organization/facility characterization.** This includes identification of assets, operations, policies, environment, crime statistics, current site safety measures, and more. Simply put, you are protecting your organization and potentially your reputation.
3. **Threat assessment.** Classify threats using an assessment process that includes, but is not limited to, the following:
 - a. *Classification of critical assets.* What resources do you have to support an anti-bullying and -abuse program?
 - b. *Identification of potential targets.* Are there any children who might be potential targets for bullying and abuse due to the age, size, gender, sexual orientation, or athletic ability?
 - c. *Consequence analysis.* What impact will an event have on your organization?
 - d. *Definition of potential threats.* What might a potential bully or abuser look like in your community?

(continued)

4. Threat vulnerability analysis. Review prior allegations of abuse and consult with other organizations about what they have experienced. Do potential scenarios exist that make your organization vulnerable to an event, and what actions are in place to prevent them from occurring?
5. Define specific security countermeasures. Define proactive actions you can take using the information from the previous four steps to support your bullying and abuse prevention policies.
6. Assess risk reduction. Review your policies to determine what is working and what is not. Implement additional security risk reduction measures, as appropriate.
7. Document findings and track implementation. As with any quality process, document findings and recommendations, and track the implementation of accepted recommendations.

If you have a safety or risk management question or a suggestion for a topic, please contact Markel's Risk Management Department at safety1st@markelcorp.com.