

# Security Assessment Dashboard

Facility Name:

Enter facility name

Date of Report:

Report Number:

Enter report number

## Security Management and Planning

Does the facility have a designated security manager or security committee?

**Very Low**

The facility does not have a security manager or committee, or

**Low**

The facility has a security manager or committee, but security

**Medium**

Security management activities are regularly scheduled,

**High**

Security activities are coordinated, but additional personnel

**Very High**

Security activities are fully coordinated and staffing

## Recommendation

Maintain current practices and continue to evaluate and update security management processes regularly. Stay informed about emerging threats and best practices. Consider sharing your successful security management model with other facilities to foster a culture of security excellence across the industry.

## Background

Continuous review and updates to security management processes ensure that the facility remains prepared for emerging threats and can adopt best practices as they evolve.

### + References

## Relevant Sources

CISA: Cybersecurity and Physical Security Convergence - Advanced concepts

ASIS International: Organizational Resilience Standard

## Does the facility have a comprehensive written security and emergency operations plan?

### Very Low

The facility does not have a written security and emergency operations plan.

### Low

The facility has a written plan, but it is incomplete or outdated.

### Medium

The facility has a complete plan, but it is not regularly reviewed or updated.

### High

The facility has a complete and regularly updated plan.

### Very High

The facility has a complete, regularly updated plan.

## Recommendation

Continue regular reviews and updates to the security and emergency operations plan. Ensure it is fully integrated with local and regional emergency plans. Develop collaborative exercises with local emergency services to test and refine the plan.

## Background

Integration with local and regional plans ensures coordinated response efforts during an emergency. Collaborative exercises help identify and address gaps in the plan, enhancing overall preparedness.

### [+ References](#)

## Relevant Sources

CISA: Risk Management Process - Interagency Security Committee

NIST: Security and Privacy Controls for Information Systems and Organizations

## Are employees and volunteers trained on the security and emergency operations plan?

### Very Low

Employees and volunteers are not trained on the

### Low

Some employees and volunteers are trained, but not all.

### Medium

Most employees and volunteers are trained, but the training

### High

All employees and volunteers are regularly trained on the

### Very High

All employees and volunteers are regularly trained

## Recommendation

Ensure regular training sessions for all employees and volunteers. Update training materials regularly to reflect changes in the security and emergency operations plan. Incorporate practical exercises to enhance learning and retention.

## Background

Regular training ensures that staff remain familiar with the plan and are able to respond effectively to any changes or updates. Practical exercises help reinforce theoretical knowledge and improve overall preparedness.

## [+ References](#)

### Relevant Sources

CISA: Planning and Response to an Active Shooter

FEMA: Guide for Developing High-Quality Emergency Operations Plans

CISA: Cybersecurity and Physical Security Convergence

### Are visitors or clients informed about relevant elements of the security and emergency operations plan?

#### Very Low

Visitors or clients are not informed about the ..

#### Low

Some visitors or clients are informed, but not all.

#### Medium

Most visitors or clients are informed, but the information is ..

#### High

All visitors or clients are informed about relevant ele ..

#### Very High

All visitors or clients are comprehensively informed about ..

### Recommendation

Regularly review and update the methods used to inform visitors and clients about the security and emergency operations plan. Incorporate feedback from visitors to improve the effectiveness of communication.

### Background

Regular updates and feedback integration help ensure that the information provided remains relevant and effective in enhancing visitor safety.

## [+ References](#)

### Relevant Sources

## RELEVANT SOURCES

CISA: Planning and Response to an Active Shooter

FEMA: Guide for Developing High-Quality Emergency Operations Plans

OSHA: Safety and Health Management Systems eTool

### Has the facility coordinated its security and emergency operations plan with local first responders?

#### Very Low

The facility has not coordinated its plan with local first responders.

#### Low

Some coordination has been attempted, but it is incomplete.

#### Medium

The facility has coordinated its plan, but not all aspects are complete.

#### High

The facility has coordinated its plan comprehensively with local first responders.

#### Very High

The facility has thoroughly coordinated its plan with local first responders.

### + References

### Does the facility conduct regular exercises of the security and emergency operations plan?

#### Very Low

The facility does not conduct regular exercises of the plan.

#### Low

Exercises are conducted sporadically and do not cover the entire plan.

#### Medium

Regular exercises are conducted, but not all elements of the plan are covered.

#### High

Regular exercises are conducted covering most elements of the plan.

#### Very High

Comprehensive regular exercises are conducted covering all elements of the plan.

### Recommendation

Continue regular and comprehensive exercises. Share best practices and

lessons learned from exercises with similar facilities. Consider participating in regional or national exercise initiatives to further enhance preparedness.

## Background

Sharing best practices and participating in broader exercise initiatives help improve overall preparedness within the community and beyond. This also helps the facility stay informed about emerging threats and best practices.

### + References

## Relevant Sources

CISA: Cybersecurity and Physical Security Convergence - Advanced concepts

ASIS International: Organizational Resilience Standard

## Does the facility have lockdown, lockout, and shelter-in-place procedures?

### Very Low

The facility does not have these procedures.

### Low

The facility has some procedures, but they are incomplete

### Medium

The facility has complete procedures, but they are not regularly updated

### High

The facility has complete and regularly updated procedures

### Very High

The facility has complete, regularly updated procedures

## Recommendation

Maintain current practices of regularly updating and reviewing procedures. Consider sharing your procedures and best practices with similar facilities to promote a culture of preparedness. Participate in broader initiatives to enhance overall preparedness.

## Background

Sharing best practices and participating in broader initiatives help improve overall preparedness within the community and beyond. This also helps the facility stay informed about emerging threats and best practices.

### + References

## Relevant Sources

CISA: Cybersecurity and Physical Security Convergence - Advanced concepts

ASIS International: Organizational Resilience Standard

## Does the facility have mass notification capabilities?

### Very Low

The facility does not have mass notification capabilities.

### Low

The facility has some notification capabilities, but they are limited.

### Medium

The facility has reliable mass notification capabilities, but they are not fully integrated.

### High

The facility has reliable and integrated mass notification capabilities.

### Very High

The facility has reliable, integrated, and regularly updated mass notification capabilities.

## Recommendation

Maintain regular testing and updates of mass notification capabilities.

Ensure that all staff are trained on the system and that any feedback is used to make continuous improvements. Consider expanding the system to include additional communication tools and technologies.

## Background

Regular testing and updates help ensure that the mass notification system remains effective. Expanding the system to include additional

communication tools and technologies can enhance overall preparedness and response capabilities.

## [+ References](#)

## Relevant Sources

CISA: Risk Management Process - Interagency Security Committee

NIST: Security and Privacy Controls for Information Systems and Organizations

## Does the facility have crisis communications plans and procedures?

### Very Low

The facility does not have crisis communications

### Low

The facility has some plans and procedures, but they are in

### Medium

The facility has complete plans and procedures, but they are

### High

The facility has complete and regularly updated plans and

### Very High

The facility has complete, regularly updated plans

## Recommendation

Maintain current practices of regularly updating and reviewing plans.

Consider sharing your plans and best practices with similar facilities to promote a culture of preparedness. Participate in broader initiatives to enhance overall preparedness.

## Background

Sharing best practices and participating in broader initiatives help improve overall preparedness within the community and beyond. This also helps the facility stay informed about emerging threats and best practices.

## [+ References](#)

## Relevant Sources

CISA: Cybersecurity and Physical Security Convergence - Advanced concepts

ASIS International: Organizational Resilience Standard

### Does the facility receive threat information or security-related bulletins from external sources?

#### Very Low

The facility does not receive any external threat infor

#### Low

The facility receives some infor mation, but it is not compre

#### Medium

The facility receives regular threat infor mation and bulletins,

#### High

The facility receives comprehensive and timely threat infor

#### Very High

The facility receives comprehensive, timely, and

## Recommendation

Maintain regular receipt and review of comprehensive and timely threat information. Ensure that this information is shared with all relevant staff and used to inform security planning and decision-making. Gather feedback to continuously improve the process.

## Background

Regular receipt and review of comprehensive threat information help ensure that the facility remains informed and prepared for potential threats. Continuous feedback and improvement help maintain a high standard of preparedness.

### + References

### Relevant Sources

## RELEVANT SOURCES

CISA: Risk Management Process - Interagency Security Committee

NIST: Security and Privacy Controls for Information Systems and Organizations

### Does the facility participate in any external security or emergency preparedness working groups?

#### Very Low

The facility does not participate in any external

#### Low

The facility participates in some groups, but involvement is

#### Medium

The facility participates regularly in some groups, but does not

#### High

The facility actively participates and contributes to multiple

#### Very High

The facility is a leading participant in multiple groups,

## Recommendation

Continue to lead in participation in external working groups. Share best practices and lessons learned with similar facilities to promote a culture of preparedness. Participate in broader initiatives to enhance overall preparedness.

## Background

Leading participation and sharing best practices help improve overall preparedness within the community and beyond. This also helps the facility stay informed about emerging threats and best practices.

### + References

## Relevant Sources

CISA: Cybersecurity and Physical Security Convergence - Advanced concepts

Generate PDF Report

Generate Detailed PDF Report

Toggle Detailed Elements