Alberta Security Infrastructure Program (ASIP)

Program Guidelines

LAST UPDATED: MARCH 2023

Table of Contents

Alberta Security Infrastructure Program (ASIP)

1. PROGRAM PURPOSE AND OBJECTIVES

1.1 The Alberta Security Infrastructure Program (ASIP) grant provides funding for security assessments, related training, equipment, immediate response and security infrastructure improvements to facilities that serve communities or identifiable groups at risk of hate or bias-motivated crimes or incidents.

2. PROGRAM OVERVIEW

ASIP has two funding streams: Cost Recovery stream and Regular Grant Funding stream:

2.1 ASIP COST RECOVERY GRANT PROGRAM

Stream	**ASIP COST RECOVERY GRANT**			
Category	**A**	**B**		**C**
Overview	Professional Security Risk Assessment	Implementation of Security Risk Management Plan		Immediate Security Response
Funding Limit (see section 2.3)	$10,000 Max.	**B1**: Security Equipment and Infrastructure – $25,000 max.	**B2**: Training- $10,000 max	$10,000 Max.
		TOTAL (**B1**+**B2**): $35,000 Max.		
Reimbursement Time Frame	As of: June 1, 2021	As of: June 1, 2021		As of: June 1, 2021
Grant Agreement	Embedded in Application	Embedded in Application		Embedded in Application
Required Documentation	• Copy of Security Risk Assessment • Receipts/paid invoices	• Copy of Security Risk Assessment • Receipts/paid Invoices related to training and/or security infrastructure and equipment purchases		• Police Report **OR** Police File Number **OR** Letter of Support from Police Member • Receipts/paid invoices

2.2 ASIP REGULAR GRANT PROGRAM

<table>
<tr><td>Stream</td><td colspan="2">ASIP REGULAR GRANT PROGRAM</td></tr>
<tr><td>Category</td><td>A</td><td>B</td></tr>
<tr><td>Overview</td><td>Professional Security Risk Assessment</td><td>Implementation of Security Risk Management Plan</td></tr>
<tr><td rowspan="2">Funding Limit
(see section 2.3)</td><td rowspan="2">$10,000 max.</td><td>B1: Security Equipment and Infrastructure – $25,000 max.</td><td>B2: Training- $10,000 max</td></tr>
<tr><td colspan="2">TOTAL (B1+B2): $35,000 max.</td></tr>
<tr><td>Project Completion</td><td>12 months</td><td>12 months</td></tr>
<tr><td>Grant Agreement</td><td>Embedded in Application</td><td>Embedded in Application</td></tr>
<tr><td>Required Documentation</td><td>• Quote(s)</td><td>• Copy of Security Risk Assessment
• Quote(s) related to training and/or security infrastructure and equipment purchases</td></tr>
<tr><td>Required Final Reporting</td><td>• Final Report
• Copies of receipts/invoices</td><td>• Final Report
• Copies of receipts/invoices</td></tr>
</table>

2.3 FUNDING LIMITS

The following funding limits apply:

- Organizations are eligible to apply for a maximum of $10,000 per organization under Category A, through either the Cost Recovery Grant Program or the Regular Grant Program.
- Organizations are eligible to apply for a maximum of $35,000 per organization under Category B, through either the Cost Recovery Grant Program or the Regular Grant Program.

3. DEFINITION OF HATE CRIME AND INCIDENTS

3.1 Hate Crime and Hate Incidents

For the purpose of the ASIP grant, the following guiding definitions of hate crimes and hate incidents will be considered:

Hatred – a sentiment of intense animosity or hostility that, if exercised against members of an identifiable group, implies that those individuals are to be despised, scorned, denied respect, and made subject to ill-treatment on the basis of group affiliation.

Bias – an inclination of temperament or outlook, especially a personal and sometimes unreasoned judgment.

Prejudice – an antipathy (or enmity) based upon a faulty and inflexible generalization. It may be felt or expressed. It may be directed toward a group as a whole or toward an individual because they are a member of that group.

Hate/Bias crime – a criminal offence committed against a person or property that is perceived to be motivated and/or is motivated in whole or in part by the suspect's hate, bias or prejudice based on the victim's real or perceived ancestry, race, national or ethnic origin, language, colour, religion/creed, sex, age, mental or physical disability, gender identity, sexual orientation or any other similar factor.

Hate incident – an incident involving behaviours that are perceived to be motivated and/or are motivated by hate, bias or prejudice against a victim's real or perceived ancestry, race, national or ethnic origin, language, colour, religion/creed, sex, age, mental or physical disability, gender identity or sexual orientation and are not criminal acts.

4. DEFINITION OF SECURITY RISK ASSESSMENT

A security risk is the possibility of harm resulting from a threat, incident, or event. Although the main objective of this grant program is to mitigate security risks associated with hate/bias motivated crime and incidents, these specific risks need to be assessed and mitigated within the broader context of the holistic security risks to a facility.

*See **Appendix A** for more details*

5. SECURITY RISK MANAGEMENT PLAN

Security planning considers how security risk management practices are designed, implemented, monitored, reviewed and continually improved.

*See **Appendix B** for more details*

6. ELIGIBILITY CRITERIA

6.1 Eligible Applicants:

Applicants to the ASIP grant must be located in Alberta and be one of the following:

- Registered not-for-profit organization and/or registered charity (and in good standing);
- Places of worship such as a temple, mosque, synagogue, Gurdwara or church, where a group of people can gather to perform acts of religious praise, meditation, honour or devotion;
- Provincially/territorially recognized private educational institutions, including primary and secondary schools serving diverse student bodies;
- School that is linked to an affiliated facility where the facility itself and/or its regular users are affiliated with an identifiable group;
- Community centers, such as a community drop-in center or Indigenous Friendship Centre, where members of any identifiable group gather for social or cultural activities;
- Cemeteries or burial facilities with a primary focus on members of an identifiable group;
- Shelters serving individuals of an identifiable group;
- Ceremonial facilities or monuments used by individuals of an identifiable group; and/or
- Store front organizations serving identifiable groups.

6.2 Ineligible Applicants include:

- Residential dwellings
- Daycares
- For-profit organizations
- Municipalities
- Police Services
- Crown corporations
- Publicly funded institutions
- Individuals
- Property still under construction/development

7. PROGRAM ELIGIBILITY TIME FRAME

Organizations can apply to one or both funding streams available.

7.1 Application Eligibility Time Frame:

	Cost Recovery Grant Stream	Regular Grant Stream
Eligibility Time Frame	June 1, 2021 onward	N/A

7.2 The ASIP program will remain open dependent on availability of funds. Notice of program closure will be posted on the Alberta government ASIP website at https://www.alberta.ca/alberta-security-infrastructure-program-grant.aspx

Note: Due to a predetermined program budget, not all requests that meet the established criteria will be approved and/or guaranteed for funding or reimbursement.

8. FUNDING CATEGORIES (A, B AND C)

Applicants may apply for funding under one or more of funding categories.

If applying to more than one funding category, the application will be assessed based on the criteria of each category. Therefore, funding may be approved wholly, in part, or not at all.

Please review the conditions of funding and eligible expenses carefully for each funding category as they vary between categories.

8.1 CATEGORY A: SECURITY RISK ASSESSMENT

8.1.1 Funding or cost reimbursement for a completed Professional Security Risk Assessment (example: Crime Prevention Through Environmental Design (CPTED))

8.1.2 Funding Maximum: up to $10,000 per organization.

8.1.3 Security Risk Assessments that qualify for reimbursement included:

- Security Risk Assessment conducted by a qualified service provider in accordance with ASIS International General Security Risk Assessment Guidelines.
- Security Risk Assessment conducted by a qualified service provider in accordance with the SAFE Design Standard.
- Crime Prevention through Environmental Design (CPTED) assessment conducted by an accredited service provider in accordance with ISO 22341 guidelines.
- Security Risk Assessment conducted by a qualified service provider in accordance with ISO 31000 Risk Management Guidelines.

8.1.4 For this program, a qualified service provider is defined as a registered corporate entity providing security services under direct supervision of an individual holding verifiable credentials as a security professional. Acceptable professional credentials include:

- Current ASIS International designation as a Certified Protection Professional (CPP).
- Current ASIS International designation as a Physical Security Professional (PSP).
- Current National Institute of Crime Prevention's Crime Prevention Through Environmental Design Professional Designation (CPD).
- Current International Crime Prevention Through Environmental Design Association designation as an ICCP Certified CPTED Practitioner (ICCP- Practitioner).
- Current International Crime Prevention Through Environmental Design
- Association as an ICCP Certified CPTED Professional (ICCP-Professional).
- A recognized subject matter expert in security risk assessment competencies based on demonstrated education, training and/or experience:
    - Minimum of five (5) years experience as a sworn police officer in combination with training certificate(s) in conduct of security risk assessments;
    - Earned graduate level degree (Masters or PhD) in Security and Risk Management in combination with a minimum of five (5) years experience in conducting security risk assessments; or
    - Court qualified expert on matters relating to crime prevention and crime reduction.

8.1.5 Conditions of Funding

- The Security Risk Assessment must be for facilities belonging to or primarily used by the applicant organization.
- The Security Risk Assessment must be conducted by an accredited/certified service provider.
- Other security assessments must meet the described minimum standards above.
- There must not be any real or perceived conflict of interest regarding the individual or company providing the security assessment (refer to Section 9).
- A copy of the quotes or receipt/paid invoice for the Security Risk Assessment, as well as a copy of the assessment (if applicable) must be provided.

NOTE: The request total must be equal to, or less than, the value of the receipts provided. If the request cannot be validated the grant application will be declined.

8.1.6 General Resources for identifying qualified service providers:

- Edmonton Police Service CPTED information
- Calgary Police Service CPTED information
- Alberta Provincial Rural Crime Watch Association CPTED information
- Central Alberta Crime Prevention Centre
- http://www.canasa.org/CANASA
- ASIS Calgary / Southern Alberta Chapter 162
- ASIS Chapter 156 Edmonton/Northern Alberta

8.2 CATEGORY B: IMPLEMENTATION OF SECURITY RISK ASSESSMENT PLAN

8.2.1 Cost reimbursement or funding request to implement mitigation/ countermeasures identified through the Professional Security Risk Assessment (example: CPTED)

8.2.2 Category B is subdivided into two (2) sub-categories:

B1: Security Planning, Infrastructure and Equipment Purchases
B2: Education and Training

8.2.3 Funding Maximums:

B1: up to $25,000 per organization
B2: up to $10,000 per organization

Total request cannot exceed $35,000 per organization.

8.2.4 B1: Security Planning, Infrastructure and Equipment Purchases ($25,000 max. per organization)

Eligible mitigation measures and/or countermeasures include:

- Security Planning:
  - Contract expenses relating to the implementation of Security Risk Assessment recommendation, such as:
    - The development of a Facility Security Risk Management Plan;
    - The development of Facility Security Policies and Procedures**.**
- Security equipment and security related infrastructure changes articulated within the Facility Security Risk Management Plan:
  - Purchase, installation and/or upgrade of security equipment (examples: cameras, gates, etc.).

8.2.5 B2: Education and Training ($10,000 max. per organization)

Education and training expenses relating to security risk management and community resilience:

- Tuition expenses relating to skills development for current organization staff or regular volunteers members, such as:

- Alberta basic security guard training course;
- First Aid Training courses;
- Mental Health Awareness and De-Escalation courses;
- Conflict Avoidance and Violence Prevention courses; and
- Incident Command System (ICS) courses.

- Tuition, venue, and/or contract expenses relating to education initiatives for community members, such as:
  - Upstander Training; Legal Awareness (a.k.a. know your rights training);
  - Cyber Security Awareness;
  - Hate Crime Awareness seminars/information workshops;
  - Victim Services seminars/information workshops; and
  - Newcomer/refugee integration workshops.
- Expenses relating to translation and production of security-related awareness and education materials for community members.

8.2.6 Conditions of Funding

- A Security Risk Assessment must be conducted and dated prior to the purchase/installation of equipment.
- Rationale and security objectives for all equipment must be identified within a Security Risk Management Plan.
- There must not be any real or perceived conflict of interest regarding the individual or company providing the security assessment (refer to Section 9).
- Two quotes or receipts/paid invoices for equipment and installation must be dated at the same time or after the Security Risk Assessment.
- A copy of the floor plan where the equipment will be installed must be submitted with the regular grant application.
- A copy of the Security Risk Assessment and receipts for training, purchases and installation must be submitted with the cost recovery application.
- Consent from the facility/site owner must be obtained if the applicant does not own the facility/site.

NOTE: The request total must be equal to, or less than, the value of the receipts/paid invoices provided. If the request cannot be validated the grant application will be declined.

8.3 CATEGORY C: IMMEDIATE SECURITY RESPONSE

8.3.1 Cost reimbursement for immediate, short-term, security response needs related to a high-risk (potentially violent) hate or bias-motivated incident that was reported to police, or perceived threat thereof.

8.3.2 Funding Maximum: up to $10,000 per application.

8.3.3 Eligible expenses include:

- Security Personnel for 30 days or less;
- Immediate repairs (directly related to an incident) to the facility to

prevent access or to address a concern that could cause further trauma (examples: lock replacement, door repair, etc.); and
- Graffiti removal.

8.3.4 Conditions of Funding

- A police report **OR** police file number **OR** letter(s) of support from a police service member.
- Proof of payment (receipts/paid invoices) for equipment, repairs, services, etc. must be provided at the time of application.
- Expenses that have already been covered by insurance are not eligible for reimbursement.
- There must not be any real or perceived conflict of interest regarding the individual or company providing the security assessment (refer to Section 9).

NOTE: The request total must be equal to, or less than, the value of the receipts provided. If the request cannot be validated the grant application will be declined.

8.4 INELIGIBLE EXPENSES (ALL CATEGORIES: A, B and C):

Ineligible expenses include, but are not limited to the following:

- Costs incurred prior to the eligibility time frame (prior to June 1, 2021)
- Capital costs that include land or vehicle purchases and the construction of buildings
- Salaries/wages for applicant organization staff
- Permanent or long-term (over 30 days) security staff (security guards, etc.)
- Legal costs
- Insurance costs (premiums, deductibles, etc.)
- Unrelated debt repayment
- Ongoing subscription or service fees (example: monthly alarm service/monitoring fees)
- Time and labour provided towards preparation of funding applications
- Financing charges and interest payments on loans
- Costs covered under an insurance policy
- Costs for electrical upgrades, or general facility upgrades
- Security service worker licencing fees
- Internet service fees
- Security Professional Certification Program Fees (i.e., CPP, PCI, PSP, APP, CPD, ICCP-Practitioner, ICCP-Professional)
- Post-secondary education tuition for diploma, certification or academic degree programs

NOTE: this grant program will not provide reimbursement in cases where expenses have been paid for by another entity other than the organization making the application

9. CONFLICT OF INTEREST

9.1 In addition to complying with the ASIP guidelines and the terms in the grant application, an individual affiliated with an ASIP grant application or recipient(s)

should not place themselves in an apparent or actual conflict of interest related to the grant funds.

9.2 A conflict of interest arises when a conflict between an individual's personal interests (what they could gain financially or otherwise) and their duty to apply for or administer the grant funds in an accountable and transparent manner are in question.

9.3 A conflict of interest may be actual or perceived. Actual conflict exists where an individual's personal interests could improperly influence the recipient's duty to utilize the grant funds in a responsible and accountable manner. For example, an individual employed by the recipient wants to use the grant funds to rent space from a private company owned by the individual. An actual conflict of interest exists because the individual personally benefits from this decision.

9.4 Perceived conflict of interest exists when there is the appearance that an individual has a private interest that could improperly influence the individual's duty to act in the best interests of the grant recipient.

9.5 Whether a conflict of interest is categorized as actual or perceived, the individuals affiliated with the grant recipient should avoid placing themselves in a situation where their personal interest could interfere with their duty to be transparent and accountable with the use of the grant funds. For example, the individual should ensure that their family members or the businesses they have an interest in have no involvement with the project and in no way personally benefit from the Government of Alberta funding that was provided.

9.6 As soon as reasonably possible after becoming aware of a personal interest that causes or is likely to cause a conflict of interest in relation to a grant application, the grant applicant or recipient must give notice of the conflict to the Ministry of Alberta Public Safety and Emergency Services , Community Initiatives Support staff by contacting them via asip@gov.ab.ca. After giving notice of a conflict, the grant applicant may not commence nor continue until instructed to do so by the Community Initiatives Support staff and may not be allowed to proceed.

9.7 There must not be any real or perceived conflict of interest regarding the individual or company who has conducted or provided a security risk assessment for the applicant organization.

10. FINANCIAL REPORTING REQUIREMENTS

10.1 ASIP COST RECOVERY GRANT

10.1.1 In order to be considered for reimbursement under any of the funding categories, you must provide proof of payment for goods and/or services at the time of application.

10.1.2 Proof of Payment (Receipts/Paid Invoices)

10.1.2.1. Itemized receipts and/or invoices related to the funding request must be submitted with grant application.

10.1.3 An Itemized Expenses/Budget Template must be submitted with the grant application.

10.1.4 All expenses that are included in the funding request for reimbursement should be listed individually with the associated dollar value.

10.1.5 The total amount indicated in the Itemized Expenses/Budget Template should match the funding request.

10.1.6 The funding request and Itemized Expenses/Budget Template can be used to validate receipts/invoices submitted with the grant application.

10.1.7 The **Itemized Expenses/Budget Template** will be included as Appendix A of the Grant Agreement.

10.2 ASIP REGULAR GRANT

10.2.1 In order to be considered for funding under any of the funding categories, you must provide valid quotes dated within a reasonable timeframe of application

10.2.2 A copy of the floorplan must be submitted with the grant application.

10.2.3 An Itemized Expenses/Budget Template must be submitted with the grant application.

10.2.4 All requested expenses should be listed individually with the associated dollar value

10.2.5 The total amount indicated in the Itemized Expenses/Budget Template should match the funding request.

10.2.6 Grant recipients must complete their financial accounting for the project using the **Itemized Expenses/Budget Template** and include receipts/invoices that support the expenditures.

10.2.7 The final reporting must be properly completed and signed by an authorized representative having legal and/or financial signing authority for the organization. The final report must include all supporting documentation (i.e. receipts/invoices).

10.2.8 Expenses not able to be validated by proper documentation will be considered ineligible and funds must be returned.

10.2.9 Any recipient that does not comply with the reporting requirements may be

ineligible to receive additional funding from other Alberta Public Safety and Emergency Services grant programs until acceptable reporting is provided.

IMPORTANT NOTE: The requested amount in each category, and the total request, should be equal to or less than the cost to the organization as indicated by the documentation. If the request total is not equal to, or less than, the value of the receipts or quote provided, the grant application will be declined.

11. APPLICATION PROCEDURES

The following specifies procedures for submitting an application to ASIP:

11.1 Each funding category has specific criteria including documents that must be submitted at the time of application, for example, itemized receipts or Security Risk Assessment, etc.

11.2 Applicants should ensure they are applying to the funding category or categories, that best suit their need. Applicants are encouraged to contact the Community Initiatives Support (CIS) program office for assistance with completing the application.

11.3 In order to process applications, the information requested from applicants needs to be fully completed and all questions on the forms must be answered. Applications that are incomplete and/or are submitted without the required documentation will not be considered.

11.4 Check boxes are included on the application to ensure the application package is complete and all supporting documentation and mandatory attachments are
included. Applicants should be sure to submit all required and supporting documents, when applying.

11.5 It is important that applicants keep a complete copy of their application, as you may need to refer to this copy if CIS staff has questions about the application.

11.6 Organizations can submit their application package by email: asip@gov.ab.ca.

12. FUNDING CONDITIONS

Applicants that are successful in receiving grant funding must be aware of and observe the following funding conditions:

12.1 After the review, approval and payment of a grant relative to an application to the ASIP Cost Recovery Grant and/or the ASIP Regular Grant:

- The applicant is bound by the terms and conditions of the grant agreement that forms part of the Cost Recovery Grant and/or the ASIP Regular Grant application;

12.2 Grant funds must be spent according to approved eligible costs as outlined in the ASIP Guidelines and determined by Alberta Public Safety and Emergency Services /CIS staff.

12.3 Grant funding not used or accounted for in accordance with the approved eligible costs shall be repayable by the grant recipient to the Government of Alberta. CIS staff should be contacted for instructions.

12.4 If the expenses approved in the original application change or the applicant wishes to change the scope of the project, a written request must be made to CIS staff requesting approval. Expenses must fall within the mandate and intention of the ASIP grant program.

12.5 Financial reporting must be completed and submitted to CIS staff within the following time frames:

- ASIP Cost Recovery Grant: at the time of application
- ASIP Regular Grant: within 30 days of term end date

Note: the ASIP Regular Grant term ends 12 month following payment

13. AUDIT

13.1 Your organization may be randomly selected for Audit related to your application. By participating in the ASIP program, you are agreeing to provide the requested material, such as receipts, documents, etc. in order to allow for a fair adjudication of your grant application in accordance with the Conditional Grant Agreement imbedded in section 1 of the grant application.

14. NOTIFICATION

14.1 Applicants will receive written notification/email of the decision regarding their application.

14.2 All decisions on grant applications are final, and no appeals will be considered.

15. *FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT*

15.1 The personal information that is provided on the grant application form will be used for the purpose of administering the ASIP and advising the applicant of grant program updates and relevant Ministry initiatives. It is collected under the authority of section 33(c) of the *Freedom of Information and Protection of Privacy Act* (*FOIP Act*) and is protected by the privacy provisions of the *FOIP Act*.

15.2 The *FOIP Act* applies to any information that is provided to Alberta Justice/Public Safety and Emergency Services . This information may be disclosed in response to an access request under the *FOIP Act*, subject to any applicable exceptions to disclosure under the *FOIP Act.*

15.3 Please note, once an application has been approved and funding issued to an organization, the community/city, grant recipient, project, amount funded and fiscal year become a matter of public record.

15.4 Occasionally, Alberta Public Safety and Emergency Services may contact

applicant organizations to provide information about Ministry initiatives or announcements related to the following topics:

- Grant program changes, funding announcements and opportunities to provide input/opinion on programs; and
- Awareness of Ministry resources or events available to organizations

15.5 Only authorized contact representatives noted in the grant application may request specific information about grant applicants from the CIS office.

15.6 For questions about the collection and use of this information, please contact the CIS staff at asip@gov.ab.ca.

16. OFFICE CONTACT INFORMATION

Email: asip@gov.ab.ca

Main line: 780-415-1819
Toll-free: 780-310-0000 (780-415-1819)

Website:
https://www.alberta.ca/alberta-security-infrastructure-program-grant.aspx

17. FREQUENTLY ASKED QUESTIONS

Q: Can my organization apply to both the ASIP Cost Recovery Program and the ASIP Regular Grant Program at the same time?

A: Yes, if you meet the requirements outlined in the ASIP Program Guidelines you can apply to both programs at the same time.

Q. We would like to apply for both Cost Recovery Grant and the Regular Grant, do I need to fill out both applications.

A. Yes, when applying for both grants, you must complete both applications

Q: My organization paid for a security risk assessment on their own and now we are ready to implement the recommendations, which grant should we apply for?

A: If you have not previously received grant funding for the security risk assessment, you may apply for reimbursement under the ASIP Cost Recovery grant.

To apply for funding to implement the security measures (i.e. purchase/install equipment), you may apply under the ASIP Regular Grant.

Q: Our quote is 6 months old, do I need to get a new one?

A: Quotes are only valid for the period of time indicated on the quote (example:

90 days). If your quote is invalid at the time of application, please get a new quote as part of your submission. Invalid or stale dated quotes may impact the outcome of your application.

Q: We received an ASIP Regular Grant, can we purchase different equipment then what was included in our application?

A. Expenses must fall within the mandate and intention of the ASIP grant program. If the expenses approved in the original application change or the applicant wishes to change the scope of the project, a written request must be made to CIS staff requesting approval.

Q: Do I have to return unspent funds?

A: Yes, Grant funding not used or accounted for in accordance with the approved eligible costs must be repayable by the grant recipient to the Government of Alberta.

Q: When can I expect to hear back on the outcome of my application?

A: Applications will be reviewed and adjudicated as they are received, you will be given notice via email of the outcome of your application.

Q: I applied to the former ASIP grant program and was not approved/ partially approved, can I apply again?

A: Yes

Q. Should I print and sign my application or budget page?

A. Please fill out the attestation statement at the end of the documents electronically; a hand-written signature is not necessary**.**

Q. How should I submit my receipts/quotes, or other supporting documents?

A. If possible, attach electronic files/scan and email all supporting documents to asip@gov.ab.ca

APPENDIX A – SECURITY RISK ASSESSMENT

The first step in the process of managing security risks is to identify and analyze the threats and vulnerabilities facing a facility by conducting a Security Risk Assessment (SRA). SRA is a tool to assist organizations in making decisions on the need for countermeasures to address threats and vulnerabilities.

A Security Risk Assessment is a systematic process that evaluates the likelihood that a threat against a facility – such as a hate/bias motivated crime or incident – will be successful and considers the potential severity of consequences to the facility, its occupants, the organizations operations, and the surrounding community. The objective of conducting a SRA is to identify security hazards, threats, and vulnerabilities facing a facility, and to evaluate the countermeasures to provide for the protection of the facility, its occupants, and the organization's operations. Security risks can be assessed and strategies can be formed to reduce vulnerabilities as required.

A basic premise is that not all security risks can be completely prevented. The security objectives generally employ four basic strategies to help minimize the risk:

1) Deter
2) Detect
3) Delay
4) Respond

Appropriate strategies for managing security can vary widely depending on the individual circumstances of a facility, including the type of facility, its usage(s), its occupants, and the threats facing the facility. Risk assessments can be either qualitative or semi-quantitative depending on the level of risk, the amount of data available to the assessor and the methodology used.

There are numerous security risk assessment techniques and methods available to organizations:

- CPTED - Crime Prevention through Environmental Design,
- SAFE Design Standard®,
- ASIS International General Security Risk Assessment,
- Security Vulnerability Assessment,
- RCMP Harmonized Threat Risk Assessment,
- THIRA - Threat and Hazard Identification and Risk Assessment,
- US Homeland Security Risk Management Doctrine.

All share common risk assessment principles. The SRA method and depth of analysis should be chosen relative to the nature of the facility. Differences in geographic location, type of operations, and occupants all play a role in determining the scope of SRA and the approach taken.

Regardless of the method used, all security risk assessment techniques should include the following activities:

- **Identify Elements at Risk**. Understand the organization and identify the people, assets (i.e., property), and operations at potential risk.
- **Identify Threat Sources**. Security threats are deliberate actions intended to cause harm to people and/or damage to the facility. A threat (inclusive of, but not limited to those relating to hate/bias motivated crime and incidents) is characterized as the combination of both intent and capability of a threat actor or threat source to realize a threat or attack against an asset. General threat categories may include crimes against people, crimes against property, and quality of life/harmful societal behaviours impacting facility operations.
- **Identify Vulnerabilities**. A vulnerability is any susceptibility, flaw or condition that can be exploited for the successful realization of a potential threat against the facility and its users. Vulnerability conditions can be classified into two types: physical and procedural. A physical vulnerability condition is an actual physical deficiency, flaw or absence of physical measures designed to deter, detect, delay and/or respond to a security breach. A procedural vulnerability condition relates to the existence, implementation, and oversight of policies and procedures, which are designed to deter, detect, delay, respond or recover against a security breach.
- **Assess the Likelihood of an incident**. The combination of threat and vulnerability relates to the likelihood (i.e., probability and frequency) of a threat being realized through exploitation of a vulnerability. Probability may be based upon considerations of such issues as prior incidents, trends, warnings, or threats, and such events occurring at the facility. Frequency of events relates to the regularity of event.
- **Identify the Consequences of an incident**. Determine the impact of a threat being realized. The physical, psychological, financial, and related costs associated with the probable incident.
- **Prioritize Security Risks**. Security risk is the combination of likelihood and consequence, generally articulated as credible scenarios of threats applied against the elements at risk (i.e., people, property, services). A risk severity rating is evaluated for each scenario to support considerations of mitigation actions required.
- **Identify potential mitigation measures/countermeasures**. Identify options available to prevent or mitigate risk scenarios through physical, procedural, logical, or related security processes. Study the feasibility of implementation of options, and the practicality of implementing the options without substantially interfering with the facilities operation**.**
- **Determine residual risk acceptability**. Perform a cost/benefit analysis – a systematic attempt to measure or analyze the value of all the benefits that accrue from particular mitigation options.

APPENDIX B – SECURITY RISK MANAGEMENT PLAN

Organizations should develop a security plan that sets out how they will manage their identified security risks and how security aligns with their priorities and objectives. The plan should describe how policies, procedures, and controls (i.e., security equipment) are to be implemented to minimize or eliminate identified security risks identified by the security risk assessment process. Where feasible, the plan should include scalable control measures to respond to increases or decreases in risk when a threat to the entity changes.

Education and training can be an important aspect of a successful security management plan. This may include training for management and security personnel to better monitor, respond, evaluate, and report security incidents. It may also include education and training for facility occupants and users to build understanding and resilience against identified security risks.

Security risk management is a cycle, not a linear path. Given continual evolution of the threat environment and inherent uncertainties, a security risk management plan should be a living document.