Guide to the Facility Security Assessment and Authorization Process

GCPSG-016 (2022)

Prepared By:
Royal Canadian Mounted Police
Lead Security Agency for Physical Security
Departmental Security
NHQ 73 Leikin Drive Ottawa Ontario, K1A 0R2

Publication Issued: 2022-12-06
Updated:

Foreword

The Guide to the Facility Security Assessment and Authorization Process is an UNCLASSIFIED publication, issued under the authority of the Royal Canadian Mounted Police Lead Security Agency for Physical Security (RCMP LSA).

This is a Government of Canada publication to serve as a guideline on considerations specific to Facility Security Assessment and Authorizations for departments, agencies and employees of the Government of Canada.

Suggestions for amendments can be sent to the RCMP Lead Security Agency RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

Effective Date

The effective date of the Guide to the Facility Security Assessment and Authorization Process is 2022-12-06.

Record of Amendments

Amendment No.	Date	Entered By	Summary of Amendment

Note: Authority for modifications or variances is Royal Canadian Mounted Police Lead Security Agency for Physical Security (RCMP LSA).

Contents

Foreword i
Effective Date i
Record of Amendments i
1. Introduction 1
1.1. Purpose 1
1.2. Applicability 2
1.3. Information Technology Considerations 2
2. Contact Information 3
3. Glossary 3
4. Overview 5
5. FSA&A and the Facility Project Management Process 5
6. FSA&A Phases 6
6.1. Phase I - Initiation 6
6.2. Phase II - Planning 7
6.3. Phase III - Risk and Analysis 7
6.4. Phase IV – Implementation, Authorization, and Ongoing Security Assessments 8
6.5. Phase V – Decommissioning 10
7. References 11
Promulgation 12

1. Introduction

The RCMP, as the Lead Security Agency (LSA) for physical security for the Government of Canada (GC), is responsible for providing advice and guidance on matters relating to physical security. This includes security measures that are to be taken into consideration during an acquisition, fit-up, or decommissioning of a GC facility.

The Policy on Government Security (PGS) identifies eight security controls, with physical security being one of them. The PGS indicates:

> *Physical security requirements, practices and controls are defined, documented, implemented, assessed, monitored and maintained throughout all stages of the real property and materiel management life cycles to provide reasonable assurance that individuals, information and assets are adequately protected, thereby supporting the delivery of government programs, services and activities.*

The Directive on Security Management (DSM) identifies the mandatory procedures for the physical security control (Appendix C). According to the DSM, GC departments are responsible for implementing facility security assessment and authorizations processes to establish and maintain confidence in the security of facilities that are used, occupied or managed by the department, while considering stakeholder requirements.

1.1. Purpose

The purpose of this Guide is to assist GC departments to establish a Facility Security Assessment and Authorization (FSA&A) process to meet the mandatory procedures specified within the DSM.

> ***This guide is meant to be used in conjunction with the FSA&A Tool Kit created and maintained by the Security Centre of Excellence (SCoE) at Privy Council Office (PCO). The tool kit can be found on the SCoE GCCollab site. The link is here – FSA&A Tool Kit and in the references section of this guide.***

This Guide describes the structured approach for tenant departments to ensure effective security in the acquisition, fit-up, and decommissioning of facilities throughout the GC. Using a consistent risk-management approach for assessing security requirements for a tenant occupied facility ensures that GC organizations have established minimum security baselines and allows for the implementation of additional security controls when/if required. It promotes a workplace that is designed following security principles, standards, and concepts that allows security to evolve with a changing threat environment over time.

The following three considerations outline the expected results of the FSA&A process:

- Establish a structured approach across the GC for FSA&A – to ensure that the end result of an FSA&A is not a temporary stop-gap due to a lack of formal security assessments and authorizations on GC facilities, but a lasting security solution that meets the needs of most organizations regardless of size or capability;

- Allocate resources and invest in the proper technologies – in order for an FSA&A to be conducted accurately and the resultant recommendations implemented, sufficient financial and personnel resources need to be allocated to meet the demands of the project. Part of allocating sufficient resources is doing so in an efficient manner that includes investing in technology that not only meets current demand but future requirements as well; and
- Promote compliance – establishing a well-structured FSA&A process allows organizations to meet the requirements of the Policy on Government Security (PGS) effectively, efficiently, and completely.

1.2. Applicability

This Guide is to be used during the acquisition, fit-up and decommissioning of facilities ensuring that security is considered during all stages of a facility project.

The FSA&A process in this Guide is focused primarily for use by tenants although the key principles can also be adapted by custodian departments. A custodian department is usually responsible for the complete life-cycle of a building from the acquisition of the site, management and maintenance of the facility and eventual disposal. Custodians primary concern is for the building structure and supporting infrastructure. A tenant department occupies space within a building for a period of time (see diagram) and is concerned with the security requirements of the space they occupy. With this in mind, a custodian department will be involved in multiple FSA&A processes throughout the lifetime of the building as tenants change and the security environment evolves.

Tenant departments will often work closely with custodian departments when conducting the FSA&A process for the period of their occupancy of a building. The custodian will be responsible for the base building and common areas, whereas the tenant will be focused on their own space. Working collaboratively, the security requirements for all interested parties can be achieved. The tools provided in this Guide are focused primarily on the tenant needs of small, medium and large departments in the space they occupy.

*Please Note: This FSA&A process does not support authorization of a SIGINT secure area (SSA) or sensitive compartmented information facility (SCIF). Departments seeking to set up an SSA or SCIF must refer to CSE's Canadian SIGINT Security Standards.

1.3. Information Technology Considerations

With the constantly evolving threat landscape, and the convergence of physical and information technology (IT), the performance of security risk assessments are a critical component to the safety and security of GC information/assets/systems and people. A risk assessment should be conducted prior to connecting any application or software that operates a GC building control system to a network. Examples of these control systems are security lighting, perimeter gates, doors, HVAC, etc.

Before implementing any application or software that will control or automate building functions, your departmental security requires it to undergo the completion of an IT Security Assessment and Authorization (SA&A). This will ensure that the integrity and availability of the

components, the applications, or software controls are maintained and that any identified risks will be mitigated. Starting the IT SA&A process early is highly recommended to ensure project delivery schedules are not affected. For more information on the SA&A process, please consult your departmental security.

2. Contact Information

For more information, please contact:

Royal Canadian Mounted Police
Lead Security Agency for Physical Security
73 Leikin Drive, Mailstop #165
Ottawa, ON
K1A 0R2
Email: RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

3. Glossary

Acronym/Term	Meaning
FSA&A	**Facility Security Assessment and Authorization** – a process by which organizations ensure that security assessments are performed on new and existing GC facilities and fit-up projects. Appropriate security controls are identified and implemented before authorization is given to allow the facility to be occupied.
Facility	A physical setting used to serve a specific purpose. A facility may be part of a building, a whole building, or a building plus its site; or it may be construction that is not a building. The term encompasses both the physical object and its use (i.e., weapons' ranges, agriculture fields)
Security Assessment	The process of evaluating security practices and controls to establish the extent to which they are implemented correctly, operating as intended, and achieving the desired outcome with respect to meeting defined security requirements.
Assets	Tangible or intangible assets of the Government of Canada. Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation.
TRA	**Threat and Risk Assessment** – An assessment process evaluating the assets within a facility, the threats against them and the performance of safeguards against these threats in order to define the risks.
FSA&A Project Plan	A Project Plan details the scope of the project, including building address and applicable floor(s) affected, the budget for all aspects of the project from a security perspective such as travel, security hardware and services, the timeline allowed for the project (when the organization takes possession vs. when the space must be operational), and what deliverables are expected. The plan must be

	approved by management in order to confirm that the financial requirements of the project will be met.
FPI - Functional Program Identification	**Functional Program Identification** – Is the identification and description of business/operations.
Ongoing Security Assessments	Assessments conducted to evaluate and maintain authorization throughout the use, occupancy and maintenance of a facility.
SDB	**Security Design Brief** - A document that describes the physical protection philosophy and concepts as well as physical safeguards for a facility taking into account its operations. The approved SDB will inform the recommendations for the Authority To Occupy Facility.
BIA	**Business Impact Analysis** - Defines departmental business continuity management requirements for all departmental services and activities supporting continued availability of services and associated assets that are critical to the health, safety, security or economic well-being of Canadians or to the effective functioning of government, based on an analysis of the potential impacts of disruption.
ATOF	**Authority to Occupy Facility** – a formal declaration by the designated authority that authorizes the occupancy of a facility using a particular set of physical security safeguards within an acceptable level of residual risk as summarized in the Security Design Brief
Risk Mitigation	Activities taken to reduce risks that may be identified through the TRA process.
Risk authority	Person designated at the appropriate level in the organization to accept or mitigate risks
FPMP	**Facility Project Management Process** - The process defines key principles and provides the directives, roadmaps, deliverables and tools needed to successfully deliver facility projects on scope, on time and on budget. **Note: PSPC Real Property refers to this process as "National Project Management System (NPMS)" and this process is similar in nature to non-GC processes where the private sector is the facility owner.*
Delegated Authority	This is the individual with delegated signing authority for entering into lease agreements, construction, and fit-up contracts.
Recommending Authority	The recommending authority will typically be the Chief Security Officer. It is their responsibility to ensure all applicable security assessments have been completed and based on those results, provide a recommendation regarding the occupancy of the facility.
SA&A	**Security Assessment and Authorization** - The security assessment component of SA&A is to verify that the security requirements established for a particular system or service are met and that the controls and safeguards work as intended. The authorization component of SA&A is to signify that management has accepted the residual risk of operating the system or service and authorized the system or service to operate based on the evidence.

4. Overview

The FSA&A process involves conducting security assessments of a facility, in which the core of the process revolves around the acquisition or fit-up of a facility. As such, the FSA&A should be integrated into a Facility Project Management Process (FPMP) at the outset.

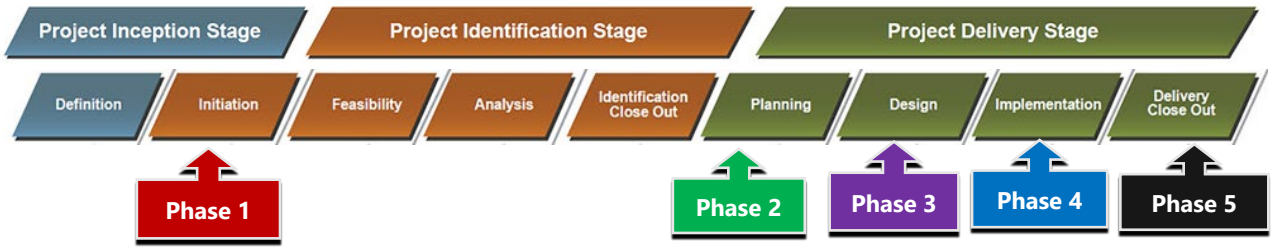
FPMP is designed to work through the process of identifying the need, determining how the investment will be carried out, the type of acquisition (traditional procurement, design-build, lease, design-build-operate, etc.), the design, implementation, and close-out of the project.

The FPMP can be divided into three stages: project inception, project identification, and project delivery. While the FPMP is ongoing, the FSA&A is introduced in five stages: Initiation, Planning, Risk & Analysis, Implementation/Authorization/Ongoing Security Assessment, and Decommissioning.

5. FSA&A and the Facility Project Management Process

Given that the FPMP is already well established, it is crucial that the FSA&A process fit into it seamlessly. Note that the final phase of the FSA&A (Decommissioning), takes place outside of the FPMP after Delivery Close-out.

FSA&A phases and where they fit in the Facility Project Management Process



Phase 1: Initiation	• Formal request for engagement of Security SMEs by Facilities SMEs • Joint review of identified space requirement by Security and Facilities SMEs • Stakeholder engagement phase (identify and engage appropriate stakeholders)
Phase 2: Planning	• Functional Program Identification (FPI) (to include business/operations description, security considerations, and space/facility description conducted by Facilities SMEs) • FSA&A Project Plan (Plan includes timeline and deliverables taking into account the elements identified in the FPI)
Phase 3: Risk & Analysis	• Business Impact Analysis (BIA completed and/or analyzed to have situational awareness of priority business operations) • Threat and Risk Assessment (Base Building) • Facility physical Threat and Risk Assessment (Operations) • Conduct and/or review of IT Threat and Risk Assessment completed by IT Security
Phase 4: Implementation, Authorization, & Ongoing Security Assessments	• Security Design Brief (final space design plan taking into account the TRAs, BIA) • Authority to Occupy Facility (plan outlining business operations, use of space, and security features to be approved) • On a cyclical basis, ongoing security assessments will be conducted to review and maintain the authorization to ensure the facility continues to comply with security requirements as identified throughout the FSA&A process
Phase 5: Decommissioning	• Facility post-occupancy procedure (procedures to be followed once space is vacated to ensure no assets or information have been left behind) • Post occupancy completion approval (signoff confirming the space has been properly vacated and all assets and information have been collected)

6. FSA&A Phases

6.1. Phase I - Initiation

Phase Description

Prior to the significant involvement of security in a facility project, it is important for Subject Matter Experts (SMEs) from the offices of security and facilities to engage in preliminary discussions. This ensures that there is a solid understanding from each stakeholder on what is expected and required from each other.

When a business requirement for a facility is identified, facilities SMEs will engage with the Chief Security Officer (CSO) or an authorized delegate, to inform them of the upcoming project. At this point a formal arrangement is prepared between the CSO or their delegate and facilities SMEs to fully define the scope of the space and project and outline specific responsibilities based on the resources (human and financial) available to them.

Guidelines

This entire process is dependent on a **pre-existing strong partnership** between security and facilities SMEs. This partnership will ensure that open communication takes place and security SMEs are aware of the facility project as soon as possible. In addition to a strong partnership

between security and facilities SMEs, the security SMEs must keep communications open between various stakeholders who might potentially be involved with the project. Efficiency and respect of timelines must be a priority for all involved, as any one group can cause delays for the entire project. In order to facilitate this communication, **early buy-in and cooperation from the stakeholders** is key. This can be achieved through:

- Issuing a communiqué informing stakeholders of a new project; and
- Preparing a formal notice, message, agreement or arrangement at the outset of a project with stakeholders outlining the expected deliverables in order to provide clarity and avert any uncertainty.

6.2. Phase II - Planning

Phase Description

Once a partnership has been established and stakeholders are on board, the next step is to plan the project itself. During this phase, an FSA&A Project Plan is drafted by security SMEs. It requires review and approval by the CSO or identified delegate. The FSA&A Project Plan identifies the funds specific to the FSA&A project and establishes the timeline and deliverables within the set Facility Project Management Plan. Early planning sets the stage and expected results of the FSA&A project.

After clearly defining the scope of the FSA&A, funding, level of effort, deliverables, and timeline, the natural progression is to identify the operations that will take place within the facility. Knowing the type of business that will be taking place in the facility is crucial. A full description of the operations of the facility as well as how the facility construction/ fit-up will occur is captured in a separate Functional Program Identification (FPI) document. Once the business is identified, the FSA&A Project Plan is finalized, ensuring that the construction/fit-up and security elements are integrated in a manner that supports operations with the necessary human and financial support.

Guidelines

At this point, a draft **Facility Planning Identification document will be completed, outlining how the space will be used** (offices including ministerial/executive/management/etc., storage, public vs. operations areas). This is primarily a facilities responsibility; however, security must be available for consultation. Once facilities have selected operations in terms of floorplans, security SMEs can then best decide what security controls are required.

6.3. Phase III - Risk and Analysis

Phase Description

Existing organizational Business Impact Analysis (BIA) is integrated into the process to ensure critical services have been identified. This will prioritize the operations in terms of level of security and protection required. A new BIA is not required provided that one was previously conducted as part of the Business Continuity Management (BCM) process in the last five years. Following the BIA, physical and IT Threat and Risk Assessments (TRAs) will be conducted with a focus on the base building, Operations, and IT requirements/assets.

Guidelines
Provided there is an existing facility, the analysis and subsequent phases are straightforward; however, if, the facility has not yet been built, or there is significant retrofitting scheduled, the process becomes a paper-based exercise.

Once the operations have been identified, they must be prioritized. This will ensure that increased levels of security can be applied to those operations that require it.

BIAs are not new concepts and form part of a GC organization's Business Continuity Management. Existing BIAs capture the critical functions that may be inherent in the mandate of the operations.

A Base Building Physical **Threat and Risk Assessment is crucial to the security of a facility**. Knowing the security of a facility in terms of its structural integrity and capability of withstanding certain types of threats, in addition to power capabilities, will assist in the planning of where operations will be situated within the building.

The completion of this step is an excellent time to conduct a physical threat and risk assessment considering the specific layout of the facility and the operations within as well as a time to conduct an IT Threat and Risk assessment.

It is important to conduct the security assessments one at a time in order to ensure there is no wasted effort and all considerations, such as business activities, layout/floorplan, and critical functions, are factored into the security design of the facility.

6.4. Phase IV – Implementation, Authorization, and Ongoing Security Assessments

Phase Description

Implementation

The Security SMEs will review the Facility Design Plan to determine which security features will be added, in line with the completed TRAs. At the conclusion of this step, the facility security assessment portion of the FSA&A is completed. This will generate a Security Design Brief completed by the Security SMEs summarizing the TRAs that have been conducted with input from the BIA. Also in this phase, it is time to implement the security controls that have been identified to ensure the safety and security of all occupants and important GC sensitive information/assets.

Authorization

The completion of the implementation phase, specifically the Security Design Brief, allows the **Authority To Occupy Facility (ATOF)** to be given due consideration and potential approval from a security perspective. This will meet the requirements for the authorization portion of a FSA&A. This concludes the primary function of the FSA&A; however, the decommissioning phase will take place at the end of the facility's life-cycle and is required as part of the termination of ongoing use and occupancy of the facility.

Should the situation arise where the security recommendations are only partially or are not attainable, this must be noted by the recommending authority (CSO) as requiring follow-up for full approval.

Note: If at any point there is disagreement between the recommending authority (CSO), the delegated authority for facilities projects, and any stakeholders, they should be noted in the final report; however, the process must continue in order to complete the ATOF. Disagreements between stakeholders are to be defined in a dispute resolution document, outlining any concerns and the proposed means to address them.

Ongoing Security Assessments

Once a FSA&A has been conducted on a new facility or during the fit-up of an existing facility, and the facility has received the ATOF, this authority is to be maintained throughout the use, occupancy and maintenance of a facility's lifecycle. Ongoing security assessments are an important aspect of a FSA&A to ensure that the authorization remains current and valid. This is particularly important where security recommendations outlined in the FSA&A have been identified but that certain security controls may not have been able to be implemented prior to the proposed date of occupancy. Therefore, the ongoing security assessments aid in addressing any outstanding FSA&A security recommendations and therefore will increase the security posture of the facility.

Generally, ongoing security assessments are performed on a predetermined cyclical basis (depending upon the organization's mandate, critical functions, etc.). The cyclical ongoing security assessments of the Authorization to Occupy Facility provides sufficient time for the recommendations to be implemented over the course of the identified timeline.

Security assessments such as a threat and risk assessments can identify antiquated physical security and electronic security controls that may require replacement or be upgraded with newer technology as the facility ages. TRAs, or other security assessments, are also necessary when a significant change in the threat level has changed or when a mandate for the organization has changed and physical and IT security requirements need to be reevaluated.

Note: Should the mandate of the organization located in the facility change, requiring the area to be constructed into segregated security zones, this would then trigger a FPMP that requires construction of walls etc. A new FSA&A will be required as it is considered a fit-up project and subject to the requirements of a formal FSA&A).

Guidelines

Leading up to this point, in-depth analyses has been conducted on the facilities and operations. With the completion of the Facility Planning Document in the previous phase, the security team can now complete a Security Design Brief to indicate the placement of the security features and products within and outside (if applicable) the facility. Once the Security Design Brief is complete, it will accompany the TRA reports, and Business Impact Analysis that are submitted to the Chief Security Officer for review and approval.

The approval will take into account:

- The operations that will take place;
- The identified levels of risk;
- The layout of the space as designed by facilities/infrastructure personnel;
- The layout of security features; and
- Financial and time constraints;

Ongoing security assessments will be performed on a cyclical basis.

6.5. Phase V – Decommissioning

Phase Description

The final phase of the FSA&A is the decommissioning phase. It occurs at the end of the lifecycle of the facility when it is to be either razed, ownership transferred, divested, or it is the end of a lease. Although staff will no longer have access to the facility, it is imperative that no assets or information, especially that of a sensitive nature, be left behind. This will require a planned disconnection and removal of security assets such as closed circuit video equipment (CCVE), card readers, motion detectors, locks, all furniture and cabinets (which must be empty), etc. This also includes the planning of how information, such as paper files, will be transferred to a new location. Once everything has been removed from the facility, a security inspection must take place as a final confirmation and approval must be obtained by the CSO or identified delegate that the space has been cleared. Should anything be left behind, it must be tagged and the responsible manager must be informed before custody of the facility is transferred.

Guidelines

This final phase is one of the most crucial because it **is often overlooked as a formal step** in the FSA&A. It is essential that the space is properly verified to ensure that all sensitive information and assets have been removed and that identified security hardware has been disconnected and relocated where required. This requires careful planning and must be done in such a way that access control measures and intrusion alarms are not disconnected before information and assets have been moved. Additionally, given that security cabinets must be empty to be moved, **careful planning and timing must be adhered to** between the time when cabinets are emptied, to the time when the sensitive information/assets are relocated. Consideration should be taken for proper storage before the move as well as secure transportation during the move. Coordination of movers, contractors, and adhering to deadlines for turning over the space will generally be under the control of the facilities personnel.

7. References

Policy on Government Security
IT Security Risk Management
Directive on Security Management
Guide to the Management of Real Property
National Project Management System (PSPC)
RCMP Guide on Transport and Transmittal
SCoE FSA&A Toolkit (Tools)

Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-016 - (2022) Guide to the Facility Security and Assessment and Authorization Process for approval.

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2022.12.07 14:04:20 -05'00'

Shawn Nattress,
Manager
RCMP Lead Security Agency

Date

Approved

I hereby approve GCPSG-016 - (2022) Guide to the Facility Security and Assessment and Authorization Process.

St-Pierre,Andre Vincent,000171484

Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2022.12.08 11:36:06 -05'00'

Andre St-Pierre,
Director, Physical Security
Royal Canadian Mounted Police

Date